

THE YALE LAW JOURNAL

ZINA MAKAR

The Datafication of Incarceration

ABSTRACT. Courts today stand at a doctrinal inflection point: it is unclear whether the spatial logic that has long defined prison law can, or should, govern the digital technologies rapidly evolving behind bars. As tablets and other technologies increasingly structure the daily lives of incarcerated people – and extend outward to those who communicate with them – courts are beginning to confront the limits of existing prison-law doctrine. Some continue to apply traditional deference frameworks, relying on *Turner v. Safley* or *Hudson v. Palmer* to uphold sweeping powers allowing prisons to extract data and surveil communication under vague security rationales. Others – in growing numbers – express unease and hesitation in applying old frameworks, noting that digital surveillance is different in scale and kind. Like the privacy concerns at issue in *Riley v. California*, the surveillance made possible by digital tools, both inside and beyond prison walls, far surpasses the conventional practices that gave rise to foundational prison-law precedents. This emergent divide reflects a more fundamental question – if the spatial logic undergirding prison law no longer functions, what should replace it?

This Article offers the first comprehensive analysis of digital privacy rights in prisons, using as its basis the First and Fourth Amendments’ intersecting constitutional privacy principles. The Article makes three novel contributions to the privacy and prison-law fields. First, it tackles the growing issue of unchecked carceral deference in a digital era, where the law has yet to establish limits on the prison’s ability to collect and surveil prisoner and carceral-adjacent data. As such, this Article reconceptualizes the existing standards of review in light of digital privacy-based harms, likening the collection and surveillance of information data to compelled speech, or “compelled data.” To resolve these unique harms, the Article proposes an alternative privacy test to distinguish between just and unjust interferences with private information within or arising from a carceral space. Second, this Article supplements existing scholarship on dispositional favoritism in prison law to reveal how courts frequently mask data-compulsion concerns by minimizing the nature of privacy harms claimed by incarcerated and nonincarcerated individuals. And finally, this Article engages with information-privacy scholarship to shape courts’ understanding of privacy trade-offs for carceral-adjacent individuals, who now more than ever fall within the carceral sphere. By foregrounding the intersection of prison law and information-privacy scholarship, this Article demonstrates how carceral technology has antidemocratic, subordinating effects at the population level and raises questions about our commitment to data privacy for all members of our society.

AUTHOR. Assistant Professor of Law, University of Baltimore School of Law. For their generous time and insightful conversations, thanks to Alice Abrokwa, Chaz Arnett, Paulina Arnold, Ryan Calo, Bennett Capers, Devon Carbado, Ángel Díaz, Sharon Dolovich, Jessica Eaglin, Yan Fang,



Andrew Ferguson, Brandon Figg, Thomas Frampton, Michele Gilman, Aya Gruber, Danielle Jefferis, Nia Johnson, Orin Kerr, Rachel Kincaid, Cynthia Lee, Grace Li, Aaron Littman, Emmanuel Mauleón, Jamelia Morgan, Alexandra Natapoff, Melanie Newport, Keramet Reiter, Laura Rovner, Ryan Sakoda, Margo Schlanger, Heather Schoenfeld, Ji Seon Song, Anna VanCleave, Elizabeth Daniel Vasquez, Kate Weisburd, and Jonathan Zittrain. Thanks also to the participants of the 2025 UCLA-Michigan Incarceration Law and Policy Roundtable, 2025 Privacy Law Scholars Conference, and 2025 Culp Colloquium for their engagement with this piece. Finally, a special thanks to the brilliant editorial team of the *Yale Law Journal*, especially Avital Fried and Anthony Cosentino for their critical insights and precise editing.



ARTICLE CONTENTS

INTRODUCTION	2455
I. CARCERAL SURVEILLANCE AS COMPELLED DATA	2464
A. Conditions of Compulsion	2464
B. Reconceptualizing Carceral Privacy for Digital Surveillance	2470
II. LIMITATIONS AND EVOLUTIONS OF CARCERAL-PRIVACY LAW	2475
A. Limitations of Prison Law's First Amendment Doctrine	2476
1. Spatial Limitations of Relational Rights	2476
2. The Illusion of Alternative Modalities	2480
B. The Evolution of Fourth Amendment Carceral-Privacy Precedent	2482
1. Spatial Logics of Carceral Searches	2482
2. The Erosion of Spatial Limitations and Expansion of Carceral Searches	2485
C. Intersections Between Carceral Technologies and Free-World Law	2487
D. The Normative Implications of Carceral Technologies	2490
1. The Fiction of Carceral Consent	2490
2. Expanding the Carceral Sphere	2496
III. CARCERAL PRIVACY THROUGH THE LENS OF DATA-SURVEILLANCE TECHNOLOGIES	2498
A. Limitations of Prison-Law Precedent: Lower-Court Applications and Loopholes	2498
1. Evaluating Digital Prison Policies Under <i>Turner v. Safley</i>	2499
2. Evaluating Digital Prison Policies Under <i>Hudson v. Palmer</i>	2502
B. Drawing a Line Between the Need for Security and Obscurity	2505
1. Passive Interference	2507
2. Active Interference	2508
3. Justified Interference	2510
IV. RECONCEPTUALIZING THE BOUNDARIES OF CARCERAL INTERFERENCE	2512
A. Unjust Interference	2513



B. Carceral Privacy and Broader Digital-Rights Movements	2521
CONCLUSION	2524

INTRODUCTION

The government's most coercive power lies in its ability to incarcerate. As a consequence of incarceration, detainees become a distinct population of society subject to intense and intrusive forms of surveillance, ostensibly to ensure safety and security within a carceral facility.¹ But carceral surveillance today is more than it once was. Conventional forms of visual, physical, and auditory observation—like cell searches, CCTV footage, searches of physical mail, and eavesdropping on phone calls—are just part of the prison's toolkit.² Modern carceral-surveillance technologies can turn anything into an identifiable, analyzable data point, extracting metadata from e-messages, scanning photographs using facial recognition, and developing voiceprints from recorded phone calls.³

All this surveillance is made possible through a single device: the digital prison tablet.⁴ Like a Trojan horse, prison tablets embed surveillance technologies in incarcerated people's everyday lives, as prison officials and administrators funnel most forms of social connection—communication, education, and entertainment—through their digital architecture.⁵ With few ways to opt out, the prison makes digitizing one's life less an option borne of convenience and more of a compulsion met by necessity.⁶ And the harms of this compulsion are pervasive: tablet surveillance targets not only incarcerated people's outer expressions but also their interior lives—and those of their loved ones.⁷

-
1. See *Turner v. Safley*, 482 U.S. 78, 83, 90, 93 (1987) (recognizing security, order, and rehabilitation as legitimate penological interests which may serve as a basis for burdening individual rights).
 2. For a discussion on traditional applications of carceral surveillance, see *infra* Part II.
 3. See Zina Makar, *The Digital Prison Panopticon*, 38 HARV. J.L. & TECH. 961, 1023-25 (2025). *The Digital Prison Panopticon* is the first piece in a series that provides a comprehensive overview on the use of digital tablets in prisons. The paper shares qualitative stories from currently and formerly incarcerated individuals who have used tablets and briefly touches on the various legal issues potentially raised by these devices. Among the several issues raised in this first piece was a concern about data privacy. This Article is the second in the series and specifically analyzes digital tablets from a privacy-oriented lens. Future works will address the property and due-process issues implicated by carceral technologies in prisons.
 4. *Id.* at 965.
 5. Despite hosting sophisticated surveillance software, tablets themselves have fairly limited user capabilities and many restrictions that limit potential security breaches. *Id.* at 965, 988-89.
 6. Cf. *Carpenter v. United States*, 585 U.S. 296, 315 (2018) (rejecting the argument that “voluntary exposure” supersedes an individual’s legitimate expectation of privacy in physical movements captured through a cell phone and reasoning that “[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data”).
 7. See, e.g., *Schmidt v. City of Norfolk*, No. 24-cv-621, 2025 WL 410080, at *1 (E.D. Va. Feb. 5, 2025) (denying a motion to dismiss plaintiffs’ Fourth Amendment claims that the Norfolk

Before focusing on the carceral context, it is useful to ground ourselves in the broader literature on digital privacy harms. While some aspects of digital surveillance in prisons are unique, digitization can generally be understood as an intensified version of the same data practices that structure digital life outside prison walls. Across society, digital technologies blur the boundary between private and public life, enabling employers,⁸ landlords,⁹ law enforcement,¹⁰ and even neighbors¹¹ to collect and exploit personal data with limited consent or oversight. The difference in prisons is that the recipients and users of this data are state actors—correctional officers and administrators, as well as third-party private contractors—who exercise direct coercive authority over the people whose information they obtain. Whatever diffused risk exists in the “free world” becomes a concentrated form of control behind prison walls.¹² And because courts routinely defer to prison officials under the banner of “internal security,”¹³ incarcerated individuals face particularly steep obstacles in asserting their privacy rights within prison walls.

Police Department used street surveillance cameras to track individuals’ daily movements throughout the city); Ángel Díaz, *The Public Harms of Private Surveillance*, 72 UCLA L. REV. 904, 960 (2025) (“[P]rivate surveillance networks that capture more of our thoughts and movements . . . ha[ve] a serious impact on all manner of public life, including how we seek knowledge, how we use public spaces, and how we build community.”).

8. See, e.g., Ifeoma Ajunwa, *Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law*, 63 ST. LOUIS U. L.J. 21, 25 (2018).
9. See, e.g., M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1133 (2011) (citing the privacy harms of a landlord secretly listening to tenants in *Hamberger v. Eastman*, 206 A.2d 239, 241 (N.H. 1964)).
10. See *infra* note 17.
11. See, e.g., Díaz, *supra* note 7, at 13–15.
12. This Article uses the term “free world” as a descriptive shorthand to distinguish constitutional doctrines applied outside the carceral space from those deployed within it. The term is intended to reflect the doctrinal distinction that courts often draw when assessing how constitutional standards—originally articulated for noncarceral spaces—are modified or diminished in prisons, a process that frequently exposes the artificial and difficult-to-apply nature of this dichotomy. Further, this Article also recognizes this term as one that incarcerated individuals may use to describe those on the outside. See Aaron Littman, *Free-World Law Behind Bars*, 131 YALE L.J. 1385, 1390 n.9, 1482 (2022).
13. Although there may be several penological interests animating prison policies, this Article identifies the security rationale as the primary driver behind the majority of facility-wide policies and the most commonly accepted penological interest by courts in justifying rights deprivations. See, e.g., *United States v. Cohen*, 796 F.2d 20, 23 (2d Cir. 1986) (“Prior to *Hudson*, decisions upholding cell searches had done so only in cases where prison officials had grounded the reason for the search on security.”).

Modern carceral facilities have access to sophisticated, ever-evolving digital-surveillance tools through partnerships with tablet service providers (TSPs).¹⁴ These agreements include not only physical technology—the tablets and their infrastructure—but also access to centralized databases of communications records, billing names and addresses, scanned mail, and stored phone and video calls with searchable text transcripts.¹⁵ These databases are not just accessible to correctional officers at the facility where the data is collected.¹⁶ To the contrary, TSPs promote their ability to collect the originating facility’s data and pool it with other facilities, making data available to any carceral facility or law-enforcement office that pays for the TSP’s services.¹⁷

Tablets are available to incarcerated individuals under several schemes. Facilities that permit tablet usage sell, rent, or provide “free” digital tablets to incarcerated individuals, thereby streamlining library and e-book access, entertainment services, and all communications inside and outside of the facility.¹⁸ The tablets are highly regulated for end users, with limited content, apps, and capabilities and no free access to the internet.¹⁹ Once a facility introduces digital tablets, the administration will often phase out paper-based information-

-
14. Mack Finkel & Wanda Bertram, *More States Are Signing Harmful “Free Prison Tablet” Contracts*, PRISON POL’Y INITIATIVE (Mar. 7, 2019), <https://www.prisonpolicy.org/blog/2019/03/07/free-tablets> [<https://perma.cc/9EQB-87PF>].
 15. See, e.g., *Discover THREADS*, SECURUS TECHS. (2026), <https://securustechnologies.tech/investigative/investigation/threads> [<https://perma.cc/RU45-7N22>]; Class Action Complaint for Injunctive Relief and Damages at 76, *M.M. v. King*, No. 24-000546-CZ (Mich. Cir. Ct. Mar. 15, 2024), https://static1.squarespace.com/static/65c3d5f6ce15413362d4f477/t/66328edb18bdb9352d9bd026/1714589404097/MM+v+King_St+Clair+County_Complaint.pdf [<https://perma.cc/LD2W-46DB>].
 16. See Class Action Complaint for Injunctive Relief and Damages, *supra* note 15, at 75-76 (discussing Securus’s shared database with law enforcement and corrections facilities).
 17. Law enforcement also has access to these shared data pools. See Affirmation by Attorney Elizabeth Daniel Vasquez in Support of Verified Article 78 Petition at 23-25, *Reid v. N.Y.C. Dep’t of Corr.*, No. 806245/2024E (N.Y. Sup. Ct. Apr. 14, 2024), <https://bds.org/assets/files/Affirmation-by-Attorney-Elizabeth-Daniel-Vasquez.pdf> [<https://perma.cc/F37K-SC5R>] (identifying how tablet service provider (TSP) Securus actively surveils community members); *Fusion Centers*, U.S. DEP’T HOMELAND SEC. (Oct. 17, 2022), <https://www.dhs.gov/fusion-centers> [<https://perma.cc/J5L7-M2Y3>] (discussing the Department of Homeland Security’s national network of “fusion centers” that allow state and local agencies to aggregate and share data).
 18. Alissa Johnson, “Free” Prison Tablets: *In Promise and in Practice*, ELEC. PRIV. INFO. CTR. (Aug. 29, 2024), <https://epic.org/free-prison-tablets-in-promise-and-in-practice> [<https://perma.cc/Y3A7-U5Y7>] (discussing the hidden costs of “free” tablets on families and friends).
 19. See Makar, *supra* note 3, at 969-75.

sharing models, arguing that reduced access to paper will prevent contraband from entering the facility.²⁰

But security concerns are not the only motivation for the digitization of prison life. Profit figures prominently in these ostensibly administrative decisions.²¹ There are five main TSPs, two of which—Securus and Global Tel*Link Corporation—dominate (and essentially monopolize) the digital market in corrections.²² The contracts that corrections agencies sign are often commission-based, providing the agency a portion of the profits when prisoners purchase digital services like telecommunications, e-books, and e-entertainment.²³ This arrangement encourages prison administrators to reduce or remove access to nondigital alternatives.²⁴ Some have gone as far as replacing in-person visitation with video calls or transitioning paper-based law libraries to online resources.²⁵

The benefits of free-world competitive markets—namely, the power of choice that gives consumers leverage, supplied through competitive pricing policies and privacy protections—are absent for the captive population within prisons.²⁶ In many cases, the conditions under which prison tablets are administered make traditional modes of communication, entertainment, or education—those that would not necessarily leave a digital trail—inaccessible or impracticable.

20. See *infra* Section III.A.1.

21. By contracting with TSPs, prison administrators outsource their own security protocols to private companies whose networks and products lack established efficacy standards and consumer protections. See, e.g., Stephen Rahe, *The Wireless Prison: How Colorado's Tablet Computer Program Misses Opportunities and Monetizes the Poor*, PRISON POL'Y INITIATIVE (July 6, 2017), <https://www.prisonpolicy.org/blog/2017/07/06/tablets> [<https://perma.cc/8W8B-GJEH>] (discussing TSP contracts that allow the provider to excuse themselves of liability in the event that a tablet breaks or malfunctions).

22. See, e.g., U.S. Dep't of Just., Antitrust Div., *Ex parte* Submission on Proposed Rule on Incarcerated People's Communication Services; Implementation of the Martha Wright-Reed Act; Rates for Interstate Inmate Calling Services, WC Docket Nos. 23-62, 12-375, at 3 (F.C.C. Apr. 29, 2024), <https://www.justice.gov/archives/opa/media/1349941> [<https://perma.cc/6CGU-MAYV>].

23. *Pay-for-Play Tablets: The New Costly Prison Paradigm*, PRISON LEGAL NEWS (Mar. 1, 2025), <https://www.prisonlegalnews.org/news/2025/mar/1/pay-play-tablets-costly-new-prison-paradigm> [<https://perma.cc/Q63R-GLNH>] (reporting that in 2015, “74% of jails banned in person visits when they implemented video visitation” in order to maximize telecommunications revenue). For sample contracts from state departments of corrections, see *infra* note 83.

24. See *Pay-for-Play Tablets*, *supra* note 23.

25. *Id.*

26. See, e.g., Cecil v. Keller, No. 23-cv-00310, 2025 WL 918165, at *6 (W.D. Va. Mar. 25, 2025) (detailing the plaintiff's allegations that he had no alternative but to join “smartjailmail.com” in order to access incoming digitized mail); cf. Littman, *supra* note 12, at 1417-20 (discussing the gap in the Federal Communications Commission's regulation of prison telecommunications rates).

Further, this forced migration to digital platforms is particularly consequential where different modes of communication are not experientially interchangeable—that is, where each conveys distinct layers of expressive and relational information, and the substitution of letters or in-person visits with phone or video communications strips away forms of emotional nuance, nonverbal expression, and presence essential for meaningful connection.²⁷

It should not be ignored, however, that digital tablets help break down the traditional barriers of “carceral spaces”²⁸ by allowing incarcerated persons to feel connected with their communities.²⁹ Through daily tablet use, incarcerated people participate in their communities, and nonincarcerated people can engage with those on the inside in more meaningful ways.³⁰ Incarcerated persons benefit via tablets from many of the same technological conveniences the nonincarcerated enjoy when using a cell phone or computer.³¹ This digital revolution has fundamentally changed the experience of incarceration. But change has been uneven.

The old spatial divide between prison walls and the free world remains the foundational scaffolding for much of prison law’s treatment of individual rights.³² These traditional conceptions of carceral space have insulated prison officials from heightened scrutiny in antidemocratic ways, allowing them nearly

27. See *infra* Section II.A.2.

28. I use the term “carceral space” to position the prison as the focal point of government intrusion. Other, more ancillary intrusions upon the privacy of incarcerated people may extend beyond the prison walls, resulting in the expansion from traditional, brick-and-mortar prisons to include those within the circle of individuals under government surveillance. This term is also used to break away from the false dichotomy between free-world law and prison law to underscore the porous nature of the prison walls. See *infra* Section II.D.2.

29. There are a number of benefits that digital tablets provide. In prior work, I detailed these varying benefits by compiling qualitative stories and narratives reported by journalists such as Mia Armstrong-López and Charlotte West, as well as articles written by incarcerated and formerly incarcerated individuals. For a more detailed overview on the benefits that digital tablets provide incarcerated individuals and adjacent communities, see Makar, *supra* note 3, at 969–75. See also, e.g., Kwaneta Harris, Sara Kielly & Heather C. Jarvis, *What 24 Hours Looks Like in Three Prisons*, SLATE (Dec. 14, 2023, 5:45 AM), <https://slate.com/technology/2023/12/prison-tech-diaries-texas-ohio-new-york.html> [<https://perma.cc/86FB-9Y3S>] (detailing the diaries of three women incarcerated in three different states over the course of one twenty-four-hour period).

30. Makar, *supra* note 3, at 970–72.

31. *Id.*

32. See *id.* at 979 (arguing that standard prison-law applications stemmed from the spatial limitations of a traditional physical carceral facility).

unchecked deference when acting under the capacious guise of maintaining order and security within the prison walls.³³

Courts today stand at a doctrinal inflection point: it is unclear whether the spatial logic that has long defined prison law can, or should, govern the digital technologies rapidly evolving behind bars.³⁴ As digital tablets and surveillance infrastructures increasingly structure the daily lives of incarcerated people – and extend outward to those who communicate with them – courts are beginning to confront the limits of existing prison-law doctrine. Some courts continue to apply traditional deference frameworks, relying on *Turner v. Safley* or *Hudson v. Palmer* to uphold prisons officials’ sweeping authority over digital communication and data extraction.³⁵ Other courts express unease and hesitation in applying old doctrines, noting how digital surveillance differs from its conventional counterpart in both scale and kind.³⁶ Like the data-privacy concerns at issue in *Riley v. California*,³⁷ the extent of surveillance made possible by tablets far surpasses the tools that gave rise to prison law, reaching beyond the prison walls into the lives of the nonincarcerated.³⁸

33. See *id.*; *Turner v. Safley*, 482 U.S. 78, 89–91 (1987) (articulating the reasonable-restriction test); *Turner*, 482 U.S. at 100–01 (Stevens, J., concurring in part and dissenting in part) (critiquing the low bar articulated by the reasonable-restriction test).

34. For a detailed discussion on current prison-tablet litigation and applications, see *infra* Part III. See also Mike Wessler & Juliana Luna, *Prison Banned Books Week: Books Give Incarcerated People Access to the World, but Tablets Are Often Used to Wall Them Off*, PRISON POL’Y INITIATIVE (Sep. 16, 2024), https://www.prisonpolicy.org/blog/2024/09/16/prison_banned_book_week [<https://perma.cc/P5HE-UMAV>] (noting that in 2019, only twelve states contracted to provide access to prison tablets, but by 2024, forty-eight states permitted their use).

35. See, e.g., *Smith v. Wolf*, No. 19-cv-0711, 2020 WL 4551229, at *1, *6–9 (M.D. Pa. Aug. 6, 2020).

36. See, e.g., *Diez v. Texas Dep’t of Crim. Just.*, No. 23-CV-00269, 2024 WL 2867806, at *6 (S.D. Tex. Mar. 25, 2024), *report and recommendation adopted in part, rejected in part*, No. 23-CV-00269, 2024 WL 1959293 (S.D. Tex. May 3, 2024), *appeal dismissed*, No. 24-40350, 2024 WL 3912951 (5th Cir. Aug. 23, 2024).

37. 573 U.S. 373, 381 (2014).

38. Drawing on my previous work, this Article uses the term “carceral adjacent” and “prisoner adjacent” to describe individuals who are not incarcerated but are nevertheless impacted by the reach of carceral surveillance through their association with an incarcerated individual. See Makar, *supra* note 3, at 964 n.3. Carceral-adjacent individuals are increasingly bringing Fourth Amendment and state familial-association claims against prisons that force them to communicate with their incarcerated loved ones exclusively through data-collecting channels. See, e.g., Verified Petition at 68–69, *Reid v. N.Y.C. Dep’t of Corr.*, No. 806245/2024E (N.Y. Sup. Ct. Apr. 15, 2024), <https://bds.org/assets/files/Verified-Petition-Marcus-Reid-v-Department-of-Correction.pdf> [<https://perma.cc/A3PL-SRC7>]; *S.L. v. Swanson*, No. 24-120601-CZ, slip op. at 3–4 (Mich. Cir. Ct. Dec. 30, 2024), <https://www.publicjustice.net/wp-content/uploads/2024/03/2024.12.30-Opinion-granting-MSD.pdf> [<https://perma.cc/HE78-9L2W>]; Class Action Complaint and Jury Demand at 3–5, *E.L. v. Claps*, No. 2025-CV-31717

Critics may argue that denying incarcerated individuals digital privacy rights is essential to maintaining institutional security and preventing criminal activity. But this logic assumes a spatially bounded prison law, one that aligns poorly with the realities of modern technology. Consider prison law's Fourth Amendment applications. Carceral spaces already subject incarcerated individuals to daily privacy intrusions. From cell searches³⁹ to bodily searches,⁴⁰ to reviewing mail⁴¹ and listening to phone calls,⁴² hardly a moment goes by when an incarcerated individual is not susceptible to possible privacy intrusions. But each of these intrusions aims to prevent prohibited items from physically entering and circulating within a facility.⁴³ Through digital tablets, the nature and quality of information that can be created, collected, accessed, analyzed, and manipulated far exceeds what standard prison-law precedent initially encompassed.

The First Amendment's protections for speech and association also present serious issues.⁴⁴ Prison law's First Amendment has occasionally demanded a higher level of scrutiny when examining policies that burden the relational rights of carceral-adjacent individuals.⁴⁵ For example, attempts to restrict marriage or monitor outgoing mail have sometimes failed rational-basis review or triggered heightened scrutiny.⁴⁶ In contrast, prisons have successfully imposed policies limiting incarcerated persons' access to face-to-face media interviews on security

(Colo. Dist. Ct. Oct. 28, 2025), https://civilrightscorps.org/wp-content/uploads/2025/10/EL-v-Claps_Complaint.pdf [<https://perma.cc/WJA3-9452>].

39. See *Hudson v. Palmer*, 468 U.S. 517, 519 (1984).

40. See *Florence v. Bd. of Chosen Freeholders*, 566 U.S. 318, 323-24 (2012).

41. See, e.g., *Turner v. Safley*, 482 U.S. 78, 81-82 (1987); *Procunier v. Martinez*, 416 U.S. 396, 398 (1974).

42. See *United States v. Amen*, 831 F.2d 373, 378-79 (2d Cir. 1987).

43. See *infra* Section II.B.2. Under the traditional carceral-surveillance regime, some information may be maintained beyond an individual's period of incarceration. For example, jails and prisons keep records of current and prior prisoners. The Bureau of Prisons (BOP) records and publishes the information of federally incarcerated individuals, including their name, register number, age, sex, race, dates of incarceration, and location. See *Inmate Locator Information*, FED. BUREAU PRISONS, https://www.bop.gov/inmateloc/about_records.jsp [<https://perma.cc/475J-62MR>]. BOP also retains an "inmate central file," including information about any relevant disciplinary actions. See U.S. DEP'T OF JUST., FED. BUREAU OF PRISONS, PROGRAM STATEMENT 5270.09: INMATE DISCIPLINE PROGRAM 20 (July 8, 2011), https://www.bop.gov/policy/progstat/5270_009.pdf [<https://perma.cc/ET5L-JQS8>]. Although BOP's retention policies for these files are unclear, the content in the files is limited to what occurred within the prison walls. Such records are individualized and typically used for discrete identification purposes if an individual becomes reincarcerated.

44. U.S. CONST. amend. I.

45. See *Martinez*, 416 U.S. at 413-14.

46. See *infra* Section II.A.

grounds.⁴⁷ One reason for this divergence may be that the former implicates relational rights on the outside that have traditionally demanded greater protection, whereas the latter involves the right to access information on the inside.⁴⁸ Yet in the digital space, where physical, contraband-based security concerns are less relevant, distinctions between relational rights and information access become largely arbitrary, rendering this bifurcated scrutiny framework difficult to apply and misaligned with the realities of legitimate penological interests.

Digital carceral surveillance presents an issue of first impression for courts today, given the overlap between First and Fourth Amendment rights and their varying applications.⁴⁹ Information-privacy scholarship has long debated the security-privacy trade-off, but this domain has always been undertheorized in the prison-law context. These gaps have only grown with the rise of digital privacy regimes, where standard prison-security rationales no longer map onto existing doctrinal frameworks. The security interests at stake in searching physical mail, for example, may not easily justify the growing practice of digitizing and retaining letters and photographs sent between incarcerated and carceral-adjacent individuals. And the reasoning behind monitored phone calls may not support maintaining a database of biometric voiceprints for call participants.⁵⁰ Tablets and other digital technologies therefore urge us to rethink what carceral space means and how notions of privacy should apply within it.

This Article argues that digital tablets in prisons should not be regulated by the security-minded deference of standard prison law. Instead, they should be regulated by their own body of doctrine sensitive to First and Fourth Amendment privacy, consent, and community values, treated wholly differently than doctrines applied to physical carceral spaces. Unlike traditional carceral surveillance, where constitutional scrutiny might be triggered by a discrete act—a search of a cell, the reading of a letter, or the monitoring of a specific phone call—digital surveillance via tablets collapses the spatial-temporal boundaries that have historically structured constitutional law. Because data collection is constant and consent is preemptively bundled into tablet-usage agreements, it is

47. See *infra* note 219.

48. See *infra* Section II.A.1.

49. As a note, analyzing digital tablets, particularly in carceral spaces, presents many problems due to the lack of publicly available information on how data is created, collected, analyzed, shared, and ultimately used. This lack of transparency, coupled with the rapid evolution of technology, requires this Article to make certain speculations regarding the future uses and capabilities of carceral technology and how those potential risks may interact with current doctrinal applications. As such, this Article serves as the first doctrinally articulated rationale to guide courts and legislatures through analyzing the multifaceted aspects of digital-technology and privacy issues in carceral spaces.

50. For a discussion of recent lower-court decisions and litigation surrounding digital tablets, see *infra* Section III.A.

difficult to pinpoint when a “search” occurs or when a chilling effect takes root.⁵¹ The mere fact that a government actor has ongoing access to an expanding data archive renders the constitutional intrusion ambient rather than event-based.⁵² The structure of digital surveillance, then, makes it harder to distinguish between lawful institutional monitoring and constitutionally suspect data exploitation. Courts are left without a clear analytic foothold, unable to determine when passive collection of data crosses into actionable government overreach.

This Article offers the first comprehensive analysis of digital privacy rights in prisons based on the First and Fourth Amendments’ intersecting constitutional privacy principles. It makes three novel contributions to the privacy and prison-law fields. First, this Article tackles the growing issue of unchecked carceral deference in the digital era. The law has yet to establish limits on the prison’s ability to collect and surveil prisoners and carceral-adjacent data. As such, this Article reconceptualizes the existing standard of review in light of digital privacy-based harms, likening the collection of information data to compelled speech.⁵³ In developing the concept of “compelled data,” the Article offers an alternative test to distinguish between just and unjust interferences with information in carceral spaces. Second, this Article builds upon existing scholarship on dispositional favoritism⁵⁴ in prison law to reveal how the federal courts mask data-compulsion concerns by minimizing the privacy harms claimed by incarcerated and carceral-adjacent individuals.⁵⁵ And finally, this Article contributes to understandings of privacy trade-offs for society more broadly. By

51. This Article does not dispute the ways in which the First and Fourth Amendments have been applied to the prison context by the Supreme Court. Rather, it takes issue with the broad extension of these frameworks by lower courts. See *infra* Section III.A. In this vein, just as data-privacy scholars have identified the difficulties in placing limits on the government through existing free-world First and Fourth Amendment applications in the face of evolving technologies, this Article argues that the very foundations of the First and Fourth Amendments’ prison-law frameworks are ill-suited to addressing digital-privacy issues. The haphazard applications of standard prison-law doctrine by lower courts only underscore these concerns. See *infra* Section III.A. The constant, unparticularized, and state-initiated nature of this data-driven form of surveillance adds an additional layer of complexity that current constitutional tests—free world or prison-based—have yet to address, presenting the need for a new and integrated constitutional approach to these issues.

52. For a discussion of the various forms of government interference that accompany constant data collection, see *infra* Section III.B.

53. See *infra* Part I.

54. See Sharon Dolovich, *The Coherence of Prison Law*, 135 HARV. L. REV. F. 302, 317 (2022) (defining dispositional favoritism as “an orientation that can best be described as a readiness to look upon prison officials and their evidence and arguments with favor and sympathy, while regarding incarcerated litigants and *their* evidence and arguments with skepticism and even hostility”).

55. See *infra* Section III.B.

analyzing the intersection of prison-law and information-privacy scholarship, this Article illustrates how carceral technology can have antidemocratic and subordinating effects for incarcerated individuals, their loved ones, and all members of our society.⁵⁶

This Article proceeds in four Parts. Drawing on the First Amendment’s compelled-speech doctrine, Part I reframes the issue of carceral surveillance as one of data compulsion. Part II lays out the Supreme Court’s First and Fourth Amendment prison-law precedent to demonstrate how the core principles protected by these rights – namely privacy, consent, and community – play out in the context of digital technologies in carceral spaces. Turning to lower courts and the current litigation on digital tablets, Part III critiques how traditional penological justifications – predominantly notions of “security-based” surveillance – materialize as critical privacy-rights interferences when applied to digital technologies. Although digital-tablet litigation is in its nascent stages, early cases reveal the incongruity between traditional applications of prison law and the digital space. Finally, Part IV theorizes a new test that reconciles the overlap and tensions between First and Fourth Amendment carceral precedent, offering an alloyed approach to promote coherency across these doctrinal domains.

I. CARCERAL SURVEILLANCE AS COMPELLED DATA

Carceral technologies enable government actors to surveil incarcerated individuals continuously and comprehensively. The deference embedded in prison-law doctrine further permits officials to condition and mediate access to everyday functions through those technologies.⁵⁷ This Part introduces a novel framework for reconceptualizing surveillance through compelled data collection. Section I.A examines the conditions that create an environment of compulsion, while Section I.B grounds the conception of “compelled data” in First and Fourth Amendment doctrine.

A. *Conditions of Compulsion*

When digital technology functions simultaneously as a rights-accessing platform and a surveillance apparatus, it compels incarcerated individuals to generate a persistent data trail—one that collapses the boundary between their

56. Here, I use the terms “antidemocratic” and “subordinating” to signify general dignitary harms along with the specific chilling effect that surveillance has on individual communications, associations, and behaviors. See Mary Anne Franks, *Democratic Surveillance*, 30 HARV. J.L. & TECH. 425, 430 (2017).

57. For a discussion of current prison-law doctrine, see *infra* Sections II.A-B.

external interactions and inner life into quantifiable, modular data points.⁵⁸ For purposes of this Article, the term “data” is intended to encompass biometric data, including facial depictions and voice prints; behavioral biometrics such as speech, typing, and language patterns; and information data, including medical records or geolocations of associates.

To provide a simple example, the following reflects how the raw data points might appear:

inmate ID: 1265789
 login data: 2025-03-21 08:30:45
 duration: 45 minutes
 activity log: accessed educational material on legal studies
 searches: vocational training
 device performance: connection error: 2025-03-21 09:15:00⁵⁹

These are all typical data points collected from a single instance of tablet usage.⁶⁰ Once this raw data is processed, it can reveal seemingly benign yet nevertheless expressive informational trends. For example, John Doe logged in five times over the past week, with an average duration of forty minutes per session. He primarily accessed educational content regarding legal studies and vocational training opportunities. These insights may indicate a desire to expand his knowledge or acquire new job skills.⁶¹ This data could then be used to monitor rehabilitation progress or recommend further educational programs.

58. See, e.g., DANIEL J. SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* 6-8 (2004).

59. This is a fictionalized example.

60. See Tianxing Dai et al., *What Mobile Phone Data Reveal About Mobility Patterns of Teleworkers*, 201 TRANS. RSCH. PART A: POL’Y & PRAC. art. no. 104670, at 1 (2025).

61. Most incarcerated individuals will produce the kinds of data specified in this example. This data can be traced back to the relevant individual or analyzed against data produced by other incarcerated people. This example therefore aims to show that even the simplest data points can pose serious harms once compounded and compared against other users, generating usage patterns to predict future behavior. See Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 607 (2021) (describing horizontal data relations). Because only a small number of TSPs dominate the market, this relational analysis is even more valuable in the prison-tablet context, allowing providers to aggregate and pool data across multiple facilities and jurisdictions rather than analyzing it in institutional isolation. For instance, Securus’s services alone account for over fifty percent of the tablets used by incarcerated individuals. See, e.g., *About Us*, SECURUS TECHS., <https://securustech.net/about-us/index.html> [<https://perma.cc/CUU4-XM2L>] (explaining that the company services “over 1.2 million incarcerated individuals across North America”); Wendy Sawyer & Peter Wagner, *Mass Incarceration: The Whole Pie 2025*, PRISON POL’Y INITIATIVE (Mar. 11, 2025), <https://www.prisonpolicy.org/reports/pie2025.html> [<https://perma.cc/Y29H-FZYW>] (approximating that two million individuals are incarcerated at any given time).

Where digital tablets replace traditional modes of communication or information access, incarcerated individuals face a coercive choice: produce a digital data trail or forgo the meaningful exercise of a fundamental right altogether. This Article describes this phenomenon as “compelled data.” In the example provided above, this data would not have been capable of collection under traditional modes of carceral surveillance. Prison officials could not have easily drawn inferences in such a comprehensive manner, let alone at such a large scale. And the incarcerated individual would not have intended to create and share this data with correctional officers.

The stakes of data compulsion become more acute when the information comes from sources presumed to be private. Tweaking the previous example, assume the tablet collected information from a digital notepad (equivalent to a paper journal) where John Doe wrote about his dissatisfaction with the prison’s vocational offerings and his desire to receive training in another field, perhaps one more stereotypically aligned with those offered to women.⁶² John Doe may be reticent to share this information for many reasons – its criticism of the facility’s offerings, its defiance of stereotypical notions of gender, or its potential for retaliation against him.⁶³ Though compulsion in and of itself is not problematic,⁶⁴ it should be suspect where it leads to indiscriminate access to an individual’s data and interference with other rights that rely upon privacy protections.⁶⁵

Privacy rights protect individuals from government overreach in various contexts, but it is unclear which doctrine applies most directly here. Where the First Amendment protects individuals’ right to express themselves and associate without interference or censorship,⁶⁶ the Fourth Amendment restricts government intrusion that might infringe upon spaces in which those private

62. See, e.g., Karen F. Lahm, *Equal or Equitable: An Exploration of Educational and Vocational Program Availability for Male and Female Offenders*, 64 FED. PROB., Dec. 2000, at 39, 40 (finding that vocational programs tend to be gender stereotyped, offering the male incarcerated population access to auto-repair and construction training while providing their female counterparts access to office training).

63. Cf. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013) (“[S]urveillance of people when they are thinking, reading, and communicating with others in order to make up their minds about political and social issues . . . is especially dangerous because it can cause people not to experiment with new, controversial, or deviant ideas.”).

64. See, e.g., Eugene Volokh, *The Law of Compelled Speech*, 97 TEX. L. REV. 355, 358–59 (2018). For a discussion on carceral interference harms, see *infra* Section III.B.

65. See, e.g., *supra* notes 8–11 and accompanying text.

66. See, e.g., *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 466 (1958) (holding that the right of association protects individuals’ interests in keeping their associations private, thereby foreclosing the government from compelling public disclosure of those associations).

expressions or associations occur.⁶⁷ The overlap between the two amendments illustrates the crucial role privacy plays in society, ensuring both personal expression and spatial privacy remain free from undue government interference.⁶⁸

Teasing out privacy harms related to either the First or Fourth Amendments can be challenging due to the nuanced and often overlapping nature of the rights they protect, especially in the digital space.⁶⁹ Take the compelled decryption of electronic devices. When an individual is forced to provide a password to decrypt a device as part of a criminal investigation, encryption can be viewed as an incriminating testimonial act.⁷⁰ Because these legal issues arise in the criminal context, they are formally addressed through the Fourth Amendment's warrant requirement and subsequently through the Fifth Amendment's protection from self-incrimination.⁷¹ As a result, the concept of privacy as a form of First Amendment "speech" in criminal investigations (in this example, the expressive testimonial act) lurks in the background, but its salience is never legally addressed.⁷²

Digital tablets in carceral spaces give rise to a distinct set of privacy concerns at each stage of their use – beginning with their integration into essential prison functions, continuing through the disclosures they compel, and culminating in the indefinite retention of the data they generate. First, these concerns arise from the increasing necessity of tablet use in carceral spaces, where such devices now function as the primary platform for communication, education, and entertain-

67. See, e.g., Alex Abdo, *Why Rely on the Fourth Amendment to Do the Work of the First?*, 127 YALE L.J.F. 444, 455-56 (2017) (arguing that the First Amendment better addresses some of the privacy-related harms currently redressed through the Fourth Amendment); Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 747 (2008) (critiquing the Fourth Amendment's ability to regulate network-based surveillance models like traffic data).

68. See Thomas P. Crocker, *The Political Fourth Amendment*, 88 WASH. U. L. REV. 303, 311, 332-38 (2010) (identifying parallel rationales between the First and Fourth Amendments).

69. As technology develops and data-surveillance harms grow more concerning, scholars continue to question the Fourth Amendment's capacity to regulate privacy harms arising from government reliance on private technology companies, proposing a range of doctrinal reforms and, in some cases, arguing that the First Amendment may provide a better framework for addressing such harms. See Abdo, *supra* note 67, at 445. This Article is the first to identify and theorize the overlapping principles that animate both First and Fourth Amendment protections in this context, offering a doctrinally integrated approach to balance privacy harms against the regulatory needs of the carceral space.

70. See, e.g., Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767, 768-69 (2019).

71. *Id.* at 770.

72. See, e.g., *id.* at 779-81 (arguing that the mere act of decryption is testimonial, regardless of what information is revealed once the door is opened).

ment.⁷³ As in broader society, there are certain benefits provided by handheld devices, which ultimately drive the centralization of communication and access to information within such devices. For example, as compared to potentially infrequent in-person visits or phone calls, tablets offer incarcerated people a more consistent connection with the outside world.⁷⁴ Online technology provides more opportunities for incarcerated students to obtain GED degrees⁷⁵ and often offers a wider selection of reading materials.⁷⁶ But this consolidation of activity creates a comprehensive – and functionally expressive – data trail, capturing not only messages and calls but also behavioral patterns, preferences, and social connections.

The second stage stems from the information data that prisoners are compelled to disclose. Because tablets mediate nearly all meaningful activity, they enable correctional officials to access intimate data, such as personal communications, educational progress, biometric information, and even ideas by way of private notes akin to journals. Tablets are increasingly replacing many traditional paper-based forms of communication and educational materials.⁷⁷ Grievance forms and medical requests are increasingly placed through apps on digital tablets.⁷⁸ And many prisons have begun replacing paper-based law libraries with

-
73. See, e.g., Stephen Raher, *Data Privacy in Carceral Settings: The Digital Panopticon Returns to Its Roots*, 119 NW. U. L. REV. ONLINE 73, 85-89 (2024); Johnson, *supra* note 18.
 74. See, e.g., Phillip Vance Smith II, *My Girlfriend and I Used to Rely on Letters to Communicate. Then, "Texting" Came to My Prison*, SLATE (Dec. 13, 2023, 11:30 AM), <https://slate.com/technology/2023/12/e-messaging-prison-gettingout-romantic-relationships.html> [<https://perma.cc/Y6PW-PRCX>].
 75. See, e.g., Kate Payne, *New Program Will Help Inmates Earn High School Diplomas with Tablets*, ASSOC. PRESS (Sep. 18, 2024, 12:03 AM EST), <https://apnews.com/article/prison-high-school-education-tablets-d8e8f844611383f86ffab6ddod48c16e> [<https://perma.cc/SL6A-9YRC>].
 76. Wessler & Luna, *supra* note 34; Johnson, *supra* note 18.
 77. See, e.g., Sarah Stillman, *Do Children Have a "Right to Hug" Their Parents?*, NEW YORKER (May 13, 2024), <https://www.newyorker.com/magazine/2024/05/20/the-jails-that-forbid-children-from-visiting-their-parents> [<https://perma.cc/RA2H-VVGD>]; Ess Pokornowski, *Technology in Higher Education in Prison Programs: A Report on Survey Findings*, ITHAKA S+R (Sep. 7, 2023), <https://sr.ithaka.org/publications/technology-in-higher-education-in-prison-programs> [<https://perma.cc/82P9-V2GL>] (anticipating user access to online educational materials will increase over the next several years); Payne, *supra* note 75.
 78. See, e.g., L.A. Cnty. Sheriff's Dep't, 8-03/005.00 Inmate Grievances (2024) (requiring that grievance forms be submitted electronically or on paper); N.J. Dep't of Corr., Internal Management Procedure: Inmate Electronic Communication/Information/Visitation System, § IV(5)(A)(4)(a)(iii)-(iv) (2022) (making grievance copies automatically available electronically and requiring affirmative requests for paper copies).

online resources.⁷⁹ As such, prisoners have no alternative but to engage with the tablet, and meaningful access to essential functions is contingent on compliance with the facility's new policies.⁸⁰ Carceral-adjacent individuals face a similar dilemma if they wish to communicate with their loved ones.⁸¹ Therefore, the centralization of these experiences within digital tablets renders data compulsion effectively inescapable.⁸²

The final stage of use—the indefinite storage and institutional exploitation of this data—only compounds these concerns. TSPs incentivize tablet usage through profit-sharing agreements; they market tablets both as a cost-saving measure and as a tool for automating surveillance activities traditionally carried out manually, such as reading mail or listening to phone calls.⁸³ TSPs also emphasize the comprehensive nature of these services, highlighting their ability to monitor incarcerated persons' connections with the outside world through, for example, data on commissary deposits and financial transactions.⁸⁴ Indeed, some TSPs promise that their technology can “use automated systems to

79. See, e.g., Stephen Rahe & Andrea Fenster, *A Tale of Two Technologies: Why “Digital” Doesn’t Always Mean “Better” for Prison Law Libraries*, PRISON POL’Y INITIATIVE (Oct. 28, 2020), <https://www.prisonpolicy.org/blog/2020/10/28/digital-law-libraries> [<https://perma.cc/MY9V-LAT5>].

80. Prisons often designate tablet access as a privilege rather than a right—meaning that access can be revoked as a disciplinary tool (without due process) if incarcerated people fail to comply with institutional expectations. The loss of tablet access entails not just a disruption of communication but also the removal of educational and entertainment resources crucial to incarcerated people’s daily lives. See Makar, *supra* note 3, at 969–75; cf. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 600 (2009) (“Third-party business record holders can recognize the advantages of fighting for the privacy rights of their customers even absent Fourth Amendment protection. The prospect of resistance from the legal teams of third-party record holders often creates a substantial deterrence against government overreaching even when the third-party doctrine does not.”).

81. See, e.g., Class Action Complaint for Injunctive Relief and Damages, *supra* note 15, at 15–16 (recounting the story of Marie Bills, who discussed her reluctance to share private information with her incarcerated father through prison video calls because they are recorded).

82. Cf. Matthew Tokson, *Inescapable Surveillance*, 106 CORN. L. REV. 409, 428 (2021) (challenging the concept of inescapability in applications of the Fourth Amendment to digital searches).

83. Finkel & Bertram, *supra* note 14 (documenting the various contracts between prisons and tablet providers, including the portion of revenue the prison receives from the contract); see *infra* note 248.

84. See, e.g., Neema Singh Guliani & Nathan Freed Wessler, *Company that Handles Prison Phone Calls Is Surveilling People Who Aren’t in Prison*, ACLU (May 11, 2018), <https://www.aclu.org/news/privacy-technology/company-handles-prison-phone-calls-surveilling-people-who> [<https://perma.cc/KTA4-CE5Z>]; *Investigative Technology: Analysis and Insight to Support Active Investigations*, GLOBAL TEL*LINK CORP. (2017), https://www.eff.org/files/2021/09/23/gtl-tech-brief-investigative-technology_tb-iqtech-01_1.pdf [<https://perma.cc/F84C-49SJ>]. See generally Anna VanCleave, *Prison Banking*, 112 CALIF. L. REV. 1699 (2024) (discussing prisons’ banking systems and tracking of transactions).

generate call transcripts, detect keywords, measure the emotion of the call participants, and map a network of associations for incarcerated people” via geolocation data.⁸⁵ Put simply, these agreements convey the following: the more prisons integrate tablet usage, the more money they will save.⁸⁶ This approach results in a data windfall, consolidating an individual’s life into a comprehensive record accessible to a range of facilities and officials within a larger database.⁸⁷

B. Reconceptualizing Carceral Privacy for Digital Surveillance

Compelled data offers the first framework to address the carceral-specific harms left unresolved under traditional First and Fourth Amendment prison-law doctrines. The notion of compelled data draws parallels to the First Amendment doctrine of compelled speech. This doctrine establishes that when speakers are required to disclose personal information they would normally be reticent to disclose — thereby chilling speech — these mandates may trigger heightened scrutiny under the First Amendment.⁸⁸ In the carceral setting, the same dynamic arises when data extraction forces individuals to reveal information that communicates aspects of their identity, associations, or beliefs.⁸⁹ Distinct from the First Amendment’s conception of compelled speech — where the government requires an individual to say or express something they otherwise would not — compelled data concerns the creation of data that an individual intends to generate but not disclose.

The Court has recognized the cost of, yet yielded to, the necessity of heightened scrutiny to limit government overreach in both the First and Fourth Amendment spheres.⁹⁰ In the First Amendment context, the Court has acknowledged

85. See Class Action Complaint and Demand for Jury Trial at 72, *S.L. v. Swanson*, No. 2024-120601-CZ (Mich. Cir. Ct. Dec. 30, 2024), <https://civilrightscorps.org/wp-content/uploads/2024/03/GeneseeCounty-Complaint.pdf> [<https://perma.cc/5855-MTQM>]; Multi-Party Conversation Analyzer and Logger, U.S. Patent No. 10,069,966 (filed Jan. 6, 2015) (issued Sep. 4, 2018) (describing the invention’s ability to develop relational “networks of criminals” by identifying “associations between phone numbers, the names of persons reached at those phone numbers, and voice print data”).

86. See, e.g., Class Action Complaint and Demand for Jury Trial, *supra* note 85, at 57–62 (citing monetary motivations to ban in-person visitation).

87. See Viljoen, *supra* note 61, at 579 (describing population-level interests associated with relational data analysis).

88. Volokh, *supra* note 64, at 359–60.

89. See, e.g., Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 70 (2014) (discussing the expressive qualities of data).

90. See, e.g., *Riley v. California*, 573 U.S. 373, 401 (2014) (“Privacy comes at a cost.”); cf. Franks, *supra* note 56, at 427 (describing how privacy interests uniquely impact people in both vulnerable and privileged positions in society).

that even well-intentioned regulatory regimes must satisfy heightened scrutiny when they risk chilling expression of unpopular viewpoints or restructuring the conditions under which speech and association occur.⁹¹ Similarly, in the Fourth Amendment context, the Court has refused to grant warrant exceptions when novel technological practices threaten to expand the government's access to personal information wholly unrelated to the objective of the search.⁹²

Prison tablets demonstrate an equally compelling need for heightened scrutiny, as their implementation and design simultaneously mediate and condition expressive activity while dramatically expanding the state's capacity to collect, retain, and analyze intimate personal information. By conditioning communication on the knowledge that every message, search query, and digital interaction may be scrutinized, incarcerated individuals and those communicating with them may be deterred from engaging in candid speech, intimate discussions, or criticisms of prison conditions.⁹³ The same conditions chill privacy in the Fourth Amendment context by normalizing pervasive data extraction as a prerequisite to ordinary activities, resulting in continuous disclosures of voiceprints, facial recognition, or geolocation data for carceral-adjacent individuals.⁹⁴

Invoking principles of heightened scrutiny will not necessarily doom a practice. Carceral exceptions have shaped the constitutional protections associated with surveillance in the past,⁹⁵ and although compulsory speech restrictions are presumptively unconstitutional, that presumption can be rebutted.⁹⁶ For instance, courts can restrict speech as part of a criminal sentence for narrowly

91. See, e.g., *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462–63 (1958).

92. See, e.g., *Carpenter v. United States*, 585 U.S. 296, 310–13 (2018); *Riley*, 573 U.S. at 393; *United States v. Jones*, 565 U.S. 400, 415–18 (2012) (Sotomayor, J., concurring); *Jones*, 565 U.S. at 430–31 (Alito, J., concurring).

93. For an example of retaliatory censorship through tablets, see *infra* notes 275–278.

94. See, e.g., James O'Donnell, *An AI Model Trained on Prison Phone Calls Now Looks for Planned Crimes in Those Calls*, MIT TECH. REV. (Dec. 1, 2025), <https://www.technologyreview.com/2025/12/01/1128591/an-ai-model-trained-on-prison-phone-calls-is-now-being-used-to-surveil-inmates> [<https://perma.cc/RD8V-FV9L>] (discussing an interview with the Securus president, who indicated that the telecommunications company utilizes its vast database of recorded prison calls to train large language models to predict the thought processes behind criminal activity).

95. Cf. Jason Mazzone, *The Waiver Paradox*, 97 NW. U. L. REV. 801, 803 (2003) (“The Supreme Court carefully polices governmental efforts to entice individuals to give up rights of free speech in exchange for welfare, grants, or public employment, but the Court encourages criminal defendants to trade their rights in exchange for government benefits.”). See generally Kent Greenawalt, *Criminal Coercion and Freedom of Speech*, 78 NW. U. L. REV. 1081 (1984) (discussing the boundaries of free expression and coercion).

96. Volokh, *supra* note 64, at 359.

defined categories, such as speech related to the criminal conduct at issue.⁹⁷ Courts can also compel speech as part of probation conditions, like requiring an apology or answers to certain questions regarding one's identity.⁹⁸ In these circumstances, scrutiny is not diminished, but the nature of the compelled speech satisfies its demands.

Those same exceptions may also apply to the concept of data compulsion. Although prison officials may, in some instances, be justified in compelling data creation, such mandates may also cross the threshold into constitutional interference.⁹⁹ Consider how digital prison policies impact incarcerated individuals and their families.¹⁰⁰ A prison may institute a policy requiring all incoming and outgoing mail to be scanned and digitized based on concerns of contraband or prison escapes. This policy then results in the creation of a searchable database of text—from both incarcerated and nonincarcerated persons—when these individuals intended the communication to be handwritten on paper. Such a policy conflates security objectives with surveillance writ large, extrapolating the need to thwart contraband entry or escape plans into a database of language patterns unique to certain populations. Viewing such policies through the lens of compelled data establishes a presumption of constitutional sensitivity while still facilitating a structured analysis of that interference's legitimacy for penological purposes.¹⁰¹

First Amendment critics may argue that “data” itself is not a form of “speech” and that data privacy should not gain constitutional status.¹⁰² In the context of compelled speech, First Amendment scholar Eugene Volokh hypothesizes that compulsions to convey facts typically do not violate the Constitution, while compulsions to convey ideas do.¹⁰³ The scholarly debate over whether data constitutes “speech” or “facts” remains open and unsettled.¹⁰⁴ But the debate surr-

97. *Id.* at 359 n.29 (citing *United States v. Clark*, 918 F.2d 843, 848 (9th Cir. 1990)).

98. *Id.* (citing *People v. Corona*, No. D054887, 2010 WL 769150, at *3-4 (Cal. Ct. App. Mar. 8, 2010)).

99. The Supreme Court has not addressed how to treat compulsions that create speech. *See id.* at 382.

100. For additional details, see *infra* Section III.A.

101. *See infra* Part III, Section IV.A.

102. *See, e.g.,* Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1170-71 (2005) (asserting that the predicate question of the First Amendment's “scope” is understudied and that critiques on the level of scrutiny applied to data-privacy issues are therefore incomplete).

103. Volokh, *supra* note 64, at 380.

104. Scholars have taken varying positions on the First Amendment's scope and the strength of scrutiny to be applied. *See, e.g.,* Elena Kagan, *Private Speech, Public Purpose: The Role of*

ounding these binary questions demonstrates yet another instance where existing doctrines assume the conditions under which harm arises, necessitating the conceptualization of a new analytical framework.¹⁰⁵

One individual data point may be nonexpressive or fact-like but, when viewed comprehensively, take on a different form that raises constitutional concern.¹⁰⁶ The constitutional stakes of compelled data emerge not from the expressive content of each discrete data point but from the structural conditions and power dynamics under which that data is produced, as well as its capacity to reveal expressive information via aggregation and analysis. When incarcerated individuals must use digital systems that automatically collect and analyze their personal information, the act of data creation becomes a form of compelled participation — one that may chill expression, reveal intimate associations, or expose personal beliefs or unpopular opinions.¹⁰⁷

Governmental Motive in First Amendment Doctrine, 63 U. CHI. L. REV. 413, 414 (1996) (“[T]he application of First Amendment law is best understood and most readily explained as a kind of motive-hunting.”); Frederick Schauer, *The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience*, 117 HARV. L. REV. 1765, 1768 (2004) (arguing that the First Amendment’s scope is determined by an array of political, cultural, and economic factors rather than a consistent legal doctrine); Richards, *supra* note 102, at 1171 (“Rather than looking at which communications are ‘speech’ and which are ‘not speech,’ it is possible to view the category of ‘unprotected’ speech as something like the rational basis category that exists in other areas of rights jurisprudence [T]he scope question could be viewed as a threshold for invoking heightened scrutiny”).

105. *Free Speech Coalition, Inc. v. Paxton*, 606 U.S. 461 (2025), offers a recent example of this trend. There, petitioners asked the Court to determine whether a Texas law requiring age verification for websites that publish sexual material harmful to minors should be subject to rational-basis review or strict scrutiny. The Court held that such speech is “unprotected to the extent the State seeks only to verify age” and required intermediate scrutiny. *Id.* at 482. Importantly, the majority noted, “Because proof of age performs the same critical function online that it does in person, requiring age verification remains an ordinary and appropriate means of shielding minors in the digital age from material that is obscene to them.” *Id.* at 481. In limiting its inquiry to the First Amendment, the Court failed to consider the Fourth Amendment privacy concerns that differ across mediums and viewed the function of age verification solely as a form of expression rather than a compelled data point.
106. See, e.g., *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010) (describing the “mosaic theory” of surveillance), *aff’d in part sub nom.*, *United States v. Jones*, 565 U.S. 400 (2012); Viljoen, *supra* note 61, at 579 (discussing “population-level interests at stake in data production” and noting the “importance of social causes and social effects of privacy erosion”).
107. This dynamic resembles the principle articulated in *West Virginia State Board of Education v. Barnette*, which held that the state may not compel individuals to affirm a belief or engage in symbolic expression against their will. 319 U.S. 624, 633 (1943). There, the constitutional injury stemmed from a school policy requiring students to participate in the Pledge of Allegiance. *Id.* at 626–29. Just as the school in *Barnette* received significant leeway to infringe upon students’ rights prior to the Court’s intervention, prisons receive similar authority over incarcerated people’s expressive freedoms. See Zina Makar, *The Absence of Dignity in Prison Law*, 84

This form of surveillance also departs from traditional Fourth Amendment searches in physical prison spaces, as it entails the extraction of personal data and has the capacity to extend state control into broader social spheres. Fourth Amendment searches typically require particularized suspicion of a single individual.¹⁰⁸ But legal scholars have begun to argue that blanket collection and surveillance of data from individuals in communication with system-impacted individuals uses the impacted individual's legal status as a proxy for the particularized suspicion required by the Fourth Amendment.¹⁰⁹ These practices create clear tension with "free-world"¹¹⁰ applications of the Fourth Amendment and again illustrate the importance of a more nuanced analytical framework.

But as with compelled speech,¹¹¹ data compulsion alone is not the problem. It is the interference with data *after* compulsion that may require constitutional interventions.¹¹² As Volokh observes, even when speech is not restricted, the mere act of compulsion can implicate a speaker's autonomy interests such that government action becomes unconstitutional.¹¹³ By analogy, the compulsion of use data and its subsequent manipulation in carceral settings interfere with an individual's informational autonomy in ways that warrant constitutional scrutiny.

At the surface level, corrections officers could use data to block access to certain books or movies arbitrarily¹¹⁴ or remove individuals from preapproved call lists because they disagree with or dislike what information is shared.¹¹⁵ At a

MD. L. REV. 387, 392 (2024). In the carceral environment, the harm of compelled data lies in the mandatory production and disclosure of personal information under prison tablet policies. Thus, the question is not whether data is inherently expressive but whether the state's creation and use of such data constitute an impermissible form of compulsion that undermines the values of autonomy and expressive freedom underlying the First Amendment.

108. See Mariam A. Hinds, *The Shadow Defendants*, 113 GEO. L.J. 823, 868 (2025).

109. See *id.* at 868-69; Kate Weisburd, *The Carceral Home*, 103 B.U. L. REV. 1879, 1916 (2023).

110. The binary distinction between free-world law and prison law arises frequently. See Littman, *supra* note 12, at 1388. With technological advancements in communication, the dichotomy between free-world and prison law has grown significantly murkier, with a growing number of instances in which prison-law spillover constrains the rights of carceral-adjacent individuals.

111. See Volokh, *supra* note 64, at 368 (observing that, where sufficiently implicated, a speaker's autonomy rights can render government action compelling the person's speech invalid).

112. For a balancing test that addresses the harms of data compulsion through an interference analysis, see *infra* Section IV.A.

113. Volokh, *supra* note 64, at 369 (citing *W. Va. State Bd. of Educ. v. Barnette*, 319 U.S. 624, 642 (1943)).

114. Cf. *Beard v. Banks*, 538 U.S. 521, 530 (2006) (validating a prison policy that prohibited certain high-security prisoners from accessing magazines and newspapers based on the assumption that the prisoners' desire to access the news would facilitate rehabilitation).

115. See *infra* Section III.A.1.

more invasive level, the same data might subsequently be used to identify voices, generate predictive insights based on communications, keep tabs on a prisoner's associates via facial recognition, or identify locations where carceral-adjacent individuals reside or frequent.¹¹⁶

Drawing on the intersecting constitutional values of privacy, consent, and community, this Article proposes a doctrinal approach that eschews threshold categorical determinations of constitutional “coverage” and uses the concept of compelled data to advance a balancing test that accounts for the state’s interests along with the structural conditions of data production within carceral settings.¹¹⁷ Part II provides an overview of the Supreme Court’s carceral-privacy doctrine, foregrounding the existing analytical framework. Part III then interrogates the applicability of this current doctrine to emergent lower-court decisions involving digital technologies, before laying out the Article’s updated framework in Part IV.

II. LIMITATIONS AND EVOLUTIONS OF CARCERAL-PRIVACY LAW

As carceral institutions move further into the digital era, the tests that once applied to physical carceral spaces offer a limited framework for understanding the security-privacy trade-offs in digital settings. Sections II.A and II.B offer a descriptive overview of the Court’s First and Fourth Amendment carceral-privacy doctrines, respectively. Section II.C explains why contemporary free-world law also fails to provide an immediate fix for these clear doctrinal gaps. And Section II.D raises normative concerns about existing prison-law frameworks, demonstrating how they have been reshaped by data-driven surveillance to erode contemporary understandings of consent and community.¹¹⁸

116. See, e.g., Brandon Epstein, James Emerson & ChatGPT, *Navigating the Future of Policing: Artificial Intelligence (AI) Use, Pitfalls, and Considerations for Executives*, POLICE CHIEF ONLINE (Apr. 3, 2024), <https://www.policechiefmagazine.org/navigating-future-ai-chatgpt> [https://perma.cc/275Z-EWHV] (discussing the applications of AI in law enforcement through an AI-generated article).

117. For examples of this approach, see *infra* Section IV.A.

118. See generally Makar, *supra* note 3 (arguing that digital tablets challenge prison law by bridging the gap between the carceral setting and broader society).

A. Limitations of Prison Law's First Amendment Doctrine

Today, *Turner v. Safley*¹¹⁹ stands as the seminal case governing constitutional claims arising within carceral institutions.¹²⁰ But the deferential *Safley* test faces two key limitations that, when taken together, highlight its shortcomings in the digital space.¹²¹ First, *Safley* is spatially limited; it is designed only to assess the burden that prison policies place on incarcerated persons, making it ill-suited to address policies that infringe on free-world and relational rights. Second, though the test does not require that alternatives to these rights be ideal, it fails to consider whether the alternatives require the prisoner or carceral-adjacent individual to waive another right. Through a discussion of these limitations, this Section critiques *Safley*'s adequacy as a framework for evaluating prison policies in the digital era and underscores the urgency of future reform.

1. Spatial Limitations of Relational Rights

First Amendment rights can be relational, meaning that two or more parties require protection to meaningfully exercise the right.¹²² For example, the right to communicate may only be effectuated if the communicator can share information and the intended recipient is able to access it.¹²³ If the government prevents the intended recipient from receiving the message, the government will have interfered with both the sender and the recipient's right to communicate. Long before the advent of digital technology, prison policies have incidentally burdened these relational rights by, for example, opening and inspecting mail for contraband. What has changed, however, is how surveillance infrastructures mediate and monitor the exercise of relational rights across both ends of the communicative exchange.¹²⁴ Whereas contemporary prison-law doctrine confined burdens on the communicative exchange to the physical boundaries of the

119. 482 U.S. 78 (1987).

120. *Safley*'s test has since transcended its original scope. Prison-law scholars argue that the test has now become transsubstantive in lower courts' hands. See, e.g., Justin Driver & Emma Kaufman, *The Incoherence of Prison Law*, 135 HARV. L. REV. 515, 537-39 (2021) (describing the majority's test as one that "purported to govern all constitutional challenges to prison policy").

121. For an overview of the *Safley* test, see *infra* Section II.A.1.

122. See *Bd. of Educ. v. Pico*, 457 U.S. 853, 866-67 (1982); *Griswold v. Connecticut*, 381 U.S. 479, 482-83 (1965).

123. See *Pico*, 457 U.S. at 867.

124. For a discussion on the nature of expressive information collected through data-surveillance practices, see *supra* Part I.

prison, digital mediation collapses those spatial limits, extending surveillance to the substance of the communication itself.

In developing its prison-law doctrine, the Supreme Court has struggled to apply a consistent test to prison policies that infringe on relational rights traversing both the carceral space and the free world. Prior to *Safley*, the Court first applied intermediate scrutiny in *Procunier v. Martinez*.¹²⁵ There, the prison censored incoming and outgoing mail and prohibited incarcerated individuals from writing about prison grievances or expressing political, racial, or religious viewpoints.¹²⁶ The *Martinez* Court applied intermediate scrutiny and found that the policy placed an impermissible burden on speech protected under the First Amendment.¹²⁷ The prison argued that preventing incarcerated people from sharing information about prison grievances with those on the outside formed a necessary “precaution” to maintaining security and order within the facility.¹²⁸ In response, the *Martinez* Court specifically noted that outgoing mail poses less of a security risk than incoming mail, making the penological interest in screening these materials more attenuated.¹²⁹ In this way, the Court’s reasoning appeared to limit the scope of prison deference to the spatial confines of the carceral space by reviewing the policy under heightened scrutiny.¹³⁰

Following *Martinez*’s use of intermediate scrutiny, the *Safley* Court articulated a lower threshold, providing greater deference to prison policies regulating the constitutional rights of those on the inside. In *Safley*, prisoners and nonincarcerated individuals brought a class-action suit challenging Missouri prison regulations that prevented prisoners from marrying without warden permission and limited prisoner-to-prisoner correspondence to immediate family members.¹³¹ In analyzing these regulations, the Court drew on precedent¹³² to estab-

125. 416 U.S. 396, 413 (1974), *overruled in part by*, *Thornburgh v. Abbott*, 490 U.S. 401 (1989). *Abbott* overruled *Martinez* to the extent it created a distinction between the legal status of individuals sending mailing into a prison, but *Abbott* did not disturb the *Martinez* Court’s holding that outgoing mail fails to present the same internal security concerns that can occur with incoming mail. *Abbott*, 490 U.S. at 413-14.

126. *Martinez*, 416 U.S. at 399-400.

127. *Id.* at 413-14.

128. *Id.* at 416.

129. *Id.* (“[T]he Department’s regulations authorized censorship of prisoner mail far broader than any legitimate interest of penal administration demands and were properly found invalid by the District Court.”).

130. See Makar, *supra* note 3, at 983-84.

131. *Turner v. Safley*, 482 U.S. 78, 81-82 (1987).

132. *Id.* at 86-91 (first citing *Pell v. Procunier*, 417 U.S. 817 (1974); then citing *Jones v. N.C. Prisoners’ Lab. Union, Inc.*, 433 U.S. 119 (1977); then citing *Bell v. Wolfish*, 441 U.S. 520 (1979); and then citing *Block v. Rutherford*, 468 U.S. 576 (1984)); see also Makar, *supra* note 107, at 396-400 (contextualizing the precedent that gave rise to the *Safley* test).

lish a four-factor test: (1) whether there is a valid, rational connection between the prison regulation and the legitimate governmental interest; (2) whether alternative means are available for the prisoner to exercise the right being restricted; (3) the extent of the burden any accommodation will have on the correctional institution; and (4) whether there is an absence of ready alternatives to the prison regulation.¹³³

The marriage restriction ultimately failed *Safley*'s rational-basis-like test, as it substantially burdened the relational rights of incarcerated and nonincarcerated individuals.¹³⁴ The Court emphasized the inherent value in the right to marry and the extent to which this right flows beyond the prison walls.¹³⁵ Yet the Court upheld the ban on prisoner-to-prisoner mail correspondence.¹³⁶ The simplest way to reconcile these two holdings—the former applying more pressing scrutiny and the latter accepting the prison's judgment—involves the role of spatial limitations. Specifically, the marriage rule implicated the rights of nonincarcerated individuals to access a fundamental right that can only be realized if shared with a prisoner.¹³⁷ When the consequences of the prison policy impacted the space outside of prisons, the Court required that the penological interest be precise and individualized. Alternatively, when the prisoner-to-prisoner mail restriction only burdened the communicative right within carceral spaces, the Court yielded to the prison's judgment on how best to maintain institutional security.¹³⁸

Notably, *Safley* never repudiated *Martinez*. Instead, two years after *Safley*, the Court used *Thornburgh v. Abbott*¹³⁹ as an opportunity to reconcile the use of intermediate scrutiny in *Martinez* (regulating outgoing mail) and the reasonable-restriction test in *Safley* (regulating incoming mail).¹⁴⁰ *Abbott* involved a prison

133. *Safley*, 482 U.S. at 89-91.

134. *Id.* at 81.

135. *Id.* at 95-96 ("These incidents of marriage, like the religious and personal aspects of the marriage commitment, are unaffected by the fact of confinement or the pursuit of legitimate corrections goals.").

136. *Id.* at 81.

137. See Makar, *supra* note 3, at 983-84 (articulating a spatial-limitations theory of prison law).

138. Legal scholar Sharon Dolovich has argued that *Safley*'s deference regime often leads to dispositional favoritism, allowing courts to find in favor of prison without scrutinizing the incarcerated individual's complaint. See Dolovich, *supra* note 54, at 311. Understanding *Safley*'s spatial limitations explains the distinct outcomes that arise within this foundational case.

139. 490 U.S. 401 (1989).

140. One might presume that *Abbott* overturned *Martinez* in full, leaving courts with only the *Safley* test. That does not seem to be the intent of the Court. The Court explicitly states, "[W]e acknowledge today that the logic of our analyses in *Martinez* and [*Safley*] requires that

policy allowing the prison to censor incoming publications that created an institutional security risk.¹⁴¹ Of note in *Abbott* are two footnotes where the Court theorizes the types of First Amendment rights that can be burdened by the carceral space. In footnote nine, the Court emphasized the status of the rights claimants at issue – publishers and journalists were different than prisoners.¹⁴² But footnote ten clarified that spatial nature of status, noting that “the parties in *Martinez* stressed that the regulation as enforced dealt ‘with thoughts expressed in prisoner mail to relatives or friends – *mainly outgoing letters, not matters circulated within the walls.*’”¹⁴³

The distinction between prisoners and outsiders drawn in *Martinez* and its progeny underscores a crucial limitation in the Supreme Court’s doctrine: the classification of parties as “incarcerated” or “nonincarcerated” may be less legally relevant than the space where the substantive right is exercised.¹⁴⁴ And in cases involving relational rights – such as the right to associate or communicate – constitutional protection must acknowledge that such rights do not singularly reside in prisons or society. Where a protected right involves both incarcerated individuals and those outside prison walls, courts must employ a more exacting level of scrutiny, ensuring that the challenged regulation bears a substantially closer fit to the governmental interest asserted. The mere fact of one party’s incarceration does not diminish the other party’s constitutional interest in receiving or participating in the communication.

The proliferation of carceral technologies only widens this doctrinal gap. Digital infrastructure comes with an expanded capacity for surveillance, data retention, and behavioral profiling. Unlike conventional correspondence, digital communications are not only faster but also more revealing – capturing metadata, patterns of interaction, and often biometric identifiers.¹⁴⁵ In this digital landscape, the bifurcated scrutiny framework developed in *Martinez* and *Safley*, which historically permitted courts to treat outgoing and incoming communications differently, becomes increasingly untenable. As real-time exchanges

Martinez be limited to regulations concerning outgoing correspondence.” *Id.* at 413. The Court ties this limitation to the recognition that implications on prison security are of a “categorically lesser magnitude” than incoming mail. *Id.* Further, lower courts today continue to apply the *Martinez* test to outgoing mail, recognizing the spatial considerations that *Abbott* left intact. See, e.g., *infra* note 279 and accompanying text.

¹⁴¹ *Abbott*, 490 U.S. at 403.

¹⁴² *Id.* at 410 n.9 (quoting *Procunier v. Martinez*, 416 U.S. 396, 409 (1974)).

¹⁴³ *Id.* at 411 n.10.

¹⁴⁴ *Id.* at 411-12; cf. Driver & Kaufman, *supra* note 120, at 522 (observing that *Safley* “produces a body of law that is less focused on the particular right at issue than the peculiarities of the prison setting”).

¹⁴⁵ See Makar, *supra* note 3, at 976-79.

collapse the spatial distinctions upon which the Supreme Court's doctrines rely, the constitutional stakes of government interference become more acute for carceral and carceral-adjacent parties.

2. *The Illusion of Alternative Modalities*

Communication is a textured, multimodal practice through which individuals express identity, emotion, and relational intent. Though courts have historically treated different modes of communication—letters, phone calls, and video visits—as interchangeable for constitutional purposes, this equivalence obscures critical distinctions.¹⁴⁶ Each modality conveys different layers of expressive information: a handwritten letter may reflect literacy, emotional nuance, or cultural expression through syntax and spelling; a phone call reveals tone, dialect, and affective cues; and a video call adds facial expression, nonverbal gestures, and visual presence.¹⁴⁷ In-person visitation, particularly for familial relationships, enables embodied communication, full-range nonverbal engagement, and a sense of copresence that no digital format fully replicates.¹⁴⁸ The significance of these distinctions is magnified for certain populations—such as children, individuals with disabilities, and elderly caregivers—for whom specific modalities of communication are not merely preferable but necessary for meaningful relational contact.¹⁴⁹

In recent years, correctional facilities across the country have begun phasing out in-person visitation and physical mail in favor of digitized alternatives, often justified by appeals to efficiency, contraband control, or resource allocation.¹⁵⁰ Digital tablets now serve as conduits for video visits, scanned mail, and electronic messaging.¹⁵¹ These are hardly neutral changes. These policies generate profit through user fees and data extraction while imposing serious burdens on incarcerated individuals and their families, who must pay for access to what was

146. See, e.g., Amicus Curiae Brief of the American Civil Liberties Union of Michigan et al. at 11–14, *M.M. v. King*, No. 372342 (Mich. Ct. App. Sep. 4, 2024), https://civilrightscorps.org/wp-content/uploads/2024/03/MM-v-King_ACLU-AmicusBrief.pdf [<https://perma.cc/A5TS-32EQ>].

147. See *id.*

148. See *id.*

149. See, e.g., Margo Schlanger, *Keynote: Promoting Disability Equality Behind Bars*, 25 *NEV. L.J.* 537, 545–50 (2025) (arguing that equality requires individualization, particularly for individuals with disabilities in carceral spaces).

150. For a discussion of lower courts reviewing digital prison policies, see *infra* Section III.A.

151. See *infra* Section III.A.

once freely available.¹⁵² And digital platforms introduce asymmetric surveillance risks: communication through proprietary systems compels both parties – not just the incarcerated individual – to surrender metadata, biometric cues, and other personally revealing information. The old-fashioned physical visit or mailed letter left little to no digital trace and involved far less third-party mediation.

Despite these critical differences, courts evaluating First Amendment claims under *Safley* routinely reduce questions of communication to matters of substitution: whether some form of communication remains available, regardless of its qualitative nature.¹⁵³ The second prong of the *Safley* framework asks whether alternative means of exercising the right remain open to the incarcerated individual.¹⁵⁴ But when applied in the digital context, this inquiry falls short. Where physical visitation is eliminated or severely curtailed in favor of centralized digital platforms – often controlled by private TSPs – *Safley*’s logic fails to account for the fundamental transformation in both the nature of access and the conditions under which communication occurs.

Safley and its progeny¹⁵⁵ indicate to lower courts that they need only search for nominally “alternative means” without ever interrogating the coercive structure through which a substantive right is offered.¹⁵⁶ But in the case of digital technologies, the inquiry should include whether the alternative (1) preserves the reciprocal character of the right at issue and (2) compels disclosure of information that would not otherwise be created by threatening incarcerated persons with the waiver of another right.¹⁵⁷ When the only avenue for communication is one that requires both parties to interact via a surveillance-suffused platform, the prison’s regulation is not merely substituting one method for another – it is conditioning a materially different experience on participation in an information-generating system.

152. See Mike Wessler, *Incarcerated People Must Be at the Forefront of Biden Administration and Federal Trade Commission Efforts to End “Junk Fees,”* PRISON POL’Y INITIATIVE (Feb. 8, 2023), <https://www.prisonpolicy.org/blog/2023/02/08/junk-fees> [<https://perma.cc/FKY9-PEBZ>].

153. See, e.g., *S.L. v. Swanson*, No. 24-120601-CZ, slip op. at 5 (Mich. Cir. Ct. Dec. 30, 2024), <https://www.publicjustice.net/wp-content/uploads/2024/03/2024.12.30-Opinion-granting-MSD.pdf> [<https://perma.cc/HE78-9L2W>] (holding that plaintiffs do not have a substantive right to in-person visitation where other alternatives to communication exist).

154. *Turner v. Safley*, 482 U.S. 78, 90 (1987).

155. See, e.g., *Overton v. Bazzetta*, 539 U.S. 126, 135 (2003) (applying *Safley* to uphold a policy banning no-contact visitations for nonimmediate family, including children with whom the prisoner’s parental rights were legally terminated, and citing the incarcerated person’s ability to call the individuals prohibited from visiting).

156. For a discussion on lower courts’ application of *Safley* to cases challenging digital prison policies, see *infra* Section III.A.

157. For a discussion on Fourth Amendment consent waivers, see *infra* Section II.D.

Return to the distinction between video calls and in-person visitation. While both offer visual contact, they are not equivalent. A video visit mediated by a TSP allows the government – and its private contractors – to compel the creation of facial-recognition data, movement patterns, timestamps, and location meta-data from the nonincarcerated participant.¹⁵⁸ None of this would occur during an in-person visit conducted across plexiglass or monitored by CCTV. *Safley*'s framework contains no mechanism to evaluate these qualitative changes in access or their constitutional implications. It collapses the platform and the practice, treating the mere availability of any communication as sufficient to satisfy constitutional demands.

Thus, while there may be diversity in the *type* of communication available, there is often no meaningful choice in the *platform* of communication. That distinction – between content and infrastructure – is constitutionally salient but doctrinally invisible under *Safley*. Treating the digital sphere as merely an extension of the physical prison environment obscures its unique constitutional stakes. The doctrine must evolve to account for the structural burdens imposed not only on incarcerated people but also on the nonincarcerated individuals with whom they seek to communicate.

B. The Evolution of Fourth Amendment Carceral-Privacy Precedent

Although prison policies invoke a range of state interests – security, order, and rehabilitation – the Supreme Court has consistently privileged security as the dominant justification for Fourth Amendment privacy intrusions.¹⁵⁹ *Hudson v. Palmer*¹⁶⁰ remains the seminal case on this issue. This Section first traces a chronological narrative of doctrinal development, outlining how the Supreme Court has applied the reasonable-expectation-of-privacy test to incarcerated individuals. It then examines how *Palmer* entrenches a spatial logic incapable of accounting for the distinct characteristics of digital carceral technologies.

1. Spatial Logics of Carceral Searches

The Supreme Court has held that, under certain circumstances, incarcerated individuals do not retain any reasonable expectation of privacy and therefore do not benefit from the protections of the Fourth Amendment. Outside of the carceral context, it is well understood that a constitutionally protected expectation

¹⁵⁸. See *supra* note 85 and accompanying text.

¹⁵⁹. For an example of a court prioritizing a prison's penological interest in security, see *supra* note 13.

¹⁶⁰. 468 U.S. 517, 530 (1984).

of privacy exists if (1) the individual has a subjective expectation of privacy in the place searched and (2) society is objectively prepared to recognize that expectation as reasonable.¹⁶¹ A closer look, however, reveals two limitations in *Hudson v. Palmer*'s test for carceral searches. First, *Palmer*'s holding extended only to individuals admitted to a carceral space. And second, it established that while carceral spaces, such as a prison cell, may not be protected by the Fourth Amendment, expectations of privacy may still attach in certain circumstances.

As the first case in the Court's carceral-privacy jurisprudence, *Palmer* addressed whether a prisoner had a reasonable expectation of privacy in his cell.¹⁶² The *Palmer* Court validated a prison policy that permitted suspicionless, randomized searches of prisoners' cells, holding that the policy was rationally related to the penological interest of ensuring security within the prison environment.¹⁶³ The Court wrote:

A right of privacy in traditional Fourth Amendment terms is fundamentally incompatible with the close and continual surveillance of inmates and their cells required to ensure institutional security and internal order. We are satisfied that society would insist that the prisoner's expectation of privacy always yield to what must be considered the paramount interest in institutional security.¹⁶⁴

The prison's security rationales ultimately carried the day, with the Court reiterating the importance of these randomized searches as "the most effective weapon of the prison administrator in the constant fight against the proliferation of knives and guns, illicit drugs, and other contraband."¹⁶⁵ These considerations led the Court to hold that despite an incarcerated individual's subjective expectation of privacy, society was not prepared to recognize an objective one, such that the scenario fell outside the protection of the Fourth Amendment.¹⁶⁶ The Court therefore concluded that cell searches were not considered protected "searches" for the purposes of the Fourth Amendment.¹⁶⁷

161. The Court's predominant Fourth Amendment "reasonable expectation of privacy" test was first articulated by Justice Harlan in *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring). The two-part test was formally adopted by the Court in *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

162. *Palmer*, 468 U.S. at 519.

163. *Id.* at 529.

164. *Id.* at 527-28.

165. *Id.* at 528.

166. *Id.* at 525-26.

167. *Id.*

Despite its limited holding, *Palmer* has authorized the curtailment of numerous other privacy interests within carceral spaces, including those associated with one's bodily right to privacy. In *Florence v. Board of Chosen Freeholders*, the Supreme Court upheld the strip search of a pretrial detainee admitted to the facility's general population based upon the spatial and security rationales discussed in *Palmer*.¹⁶⁸ Florence's arrest stemmed from a system error falsely reporting an outstanding warrant for failure to pay a fine.¹⁶⁹ Upon intake, the prison subjected Florence to an invasive strip search which included revealing his genitalia, giving rise to his Fourth Amendment challenge.¹⁷⁰ Even though Florence was a pretrial detainee (and therefore considered legally innocent), his status was of no consequence to the Fourth Amendment analysis. Instead, the Court focused on the prison environment and how the admission of a new individual posed a security risk within the general population.¹⁷¹

Notably, though, the *Florence* Court skipped *Palmer*'s expectation-of-privacy analysis. It accepted that a strip search involves a constitutionally protected expectation of privacy and instead focused on the circumstances under which such a search would be reasonable.¹⁷² But the recognition that prisoners do, in fact, retain certain expectations of privacy is a critical limitation on *Palmer*'s logic. While incarcerated people may lack an expectation of privacy within their prison cells, *Palmer* does not strip them of any constitutionally protected expectation of privacy while incarcerated.

Despite recognizing a protected interest in bodily searches, the category of concerns that qualify as "security related" also expanded through *Florence*. The *Florence* Court initially introduced the need for a strip search as a continuation of the prison's interest in information gathering, grouping the need for a strip search for contraband with the need to identify markings that could indicate gang affiliations.¹⁷³ Important for later holdings, this holding established

168. 566 U.S. 318, 328, 330 (2012).

169. *Id.* at 323.

170. *Id.* at 324.

171. *Id.* at 333-34 (explaining that "searches at intake for disease, gang affiliation, and contraband" are based on the jail's "substantial interest in preventing any new inmate, either of his own will or as a result of coercion, from putting all who live or work at these institutions at even greater risk when he is admitted to the general population"); see also *id.* at 340-41 (Alito, J., concurring) (noting that the Court's holding is limited to entries within the general population that could pose a risk to other inmates, excluding entries into a single-occupancy holding cell).

172. See *id.* at 326-27 (majority opinion).

173. *Id.* at 323-24, 330-32. The Court cited no legal precedent to support its conclusion that the Fourth Amendment permits searches to check for gang affiliations.

information gathering as a valid means of pursuing a facility's security objectives.¹⁷⁴ This extension not only added a new layer to the prison's ability to surveil but also encouraged lower courts to conclude that information gathering can extend to the digital-surveillance context.¹⁷⁵ The following Section explores how the Court harnessed *Florence's* "information-seeking" initiative to expand its framework for carceral searches.

2. *The Erosion of Spatial Limitations and Expansion of Carceral Searches*

After *Florence*, the Supreme Court began bending the limits of its own doctrine to cover contexts with unclear spatial boundaries, such as DNA searches. Lower courts have taken this apparent erosion much further, implicating the rights of nonincarcerated individuals through phone taps or searches involving parolees or probationers.¹⁷⁶ Indeed, several lower courts have misread *Palmer* as eliminating privacy expectations regardless of circumstance.

In *Maryland v. King*, we see the Court pushing the logic of *Palmer* and, in some ways, *Florence* to their extremes. The *King* Court upheld a state law permitting authorities to collect DNA samples as part of a routine booking procedure for individuals charged with particular crimes of violence.¹⁷⁷ It invoked *Florence's* information-gathering argument to find that knowledge of a prisoner's identity was necessary for the internal safety of the prison.¹⁷⁸

King reveals the Court's disposition toward carceral deference and its resulting lack of nuance in assessing the reasonableness of privacy harms.¹⁷⁹ In *Florence*, the Court nominally acknowledged strip searches as "invasive" before finding them reasonable on security grounds.¹⁸⁰ By contrast, the *King* Court described the DNA search as a lesser invasion because it does not involve bodily exposure — only a simple cheek swab.¹⁸¹ Further, the Court emphasized the limited

174. See *infra* Section II.B.2.

175. See *infra* Section III.A.

176. See *infra* Section II.D.

177. *Maryland v. King*, 569 U.S. 435, 465-66 (2013).

178. *Id.* at 452. ("[O]fficers must know the type of person whom they are detaining, and DNA allows them to make critical choices about how to proceed.")

179. See *id.* at 469-74 (2013) (Scalia, J., dissenting) (arguing that the DNA swab's "identification" function serves to evade the Fourth's Amendment's prohibition on suspicionless searches for those charged with certain felonies).

180. *Florence v. Bd. of Chosen Freeholders*, 566 U.S. 318, 330 (2012); cf. Makar, *supra* note 107, at 417 ("As the dissent in *Florence* points out, even the minimal barrier of requiring that searches be subject to individualized suspicion would be sufficient to preserve individual dignity.")

181. *King*, 569 U.S. at 461.

uses of this DNA information under Maryland law.¹⁸² Nevertheless, DNA reveals a lot more information about a person than a search of their naked body. For instance, DNA information can be linked to family members outside of the carceral sphere. Yet, in its fixation on a facility's interest in identification, the *King* Court failed to consider when the collection of personal data ceases to serve a spatially limited penological interest.

Digital surveillance raises the same key question.¹⁸³ In some ways, DNA is analogous to data collected from digital tablets because, like DNA science, technology is constantly evolving. The *King* Court classified some DNA information gained through a cheek swab as “junk regions of DNA.”¹⁸⁴ At the time, there was limited information on noncoding DNA and its uses.¹⁸⁵ But as science has evolved in the decade since *King*,¹⁸⁶ scientists and scholars have identified the short-sighted nature of permitting such privacy intrusions where there are significant unknowns.¹⁸⁷ And digital technology faces a similar problem.¹⁸⁸ In this way, *King* expanded the carceral state's access not just to an incarcerated individual's belongings and body but also to their identity and familial bonds.

Although *Palmer*, *Florence*, and *King* reduced individual rights within the carceral space, the Supreme Court's reasoning nevertheless preserved some limits. The *Florence* and *King* decisions assumed that prisoners retain some privacy expectations in the context of strip searches and DNA swabs. But lower courts frequently miss, ignore, or bypass these limits, blindly applying *Palmer* to associational communications and more advanced technologies like phone- and video-call monitoring.¹⁸⁹ The following Section addresses the overlap between current prison-law doctrine and free-world applications of the same principles before

182. *Id.* at 465.

183. See *infra* Part III.

184. *King*, 569 U.S. at 445; see *id.* at 443 (stating that the DNA “does not show more far-reaching and complex characteristics like genetic traits”).

185. See, e.g., Alice Park, *Junk DNA—Not So Useless After All*, TIME (Sep. 6, 2012), <http://healthland.time.com/2012/09/06/junk-dna-not-so-useless-after-all> [<https://perma.cc/S522-5LWB>].

186. See, e.g., PETER G. BERRIS, CONG. RSCH. SERV., LSB11339, ADVANCES IN DNA ANALYSIS: FOURTH AMENDMENT IMPLICATIONS 2-4 (2025).

187. See, e.g., George M. Dery III, *Opening One's Mouth “For Royal Inspection”: The Supreme Court Allows Collection of DNA from Felony Arrestees in Maryland v. King*, 2 VA. J. CRIM. L. 116, 147-48 (2014) (analogizing *King*'s DNA-collection holding to the societal acceptance of routine fingerprint collection before modern Fourth Amendment jurisprudence).

188. One dystopian possibility is the use of polygenic risk scores, which are growing in popularity in medical domains but could be used to calculate the genomic risk of criminal behavior in individuals. See, e.g., Natalie Ram, *Polygenic Scoring and the Criminal Legal System*, 38 HARV. J.L. & TECH. 577, 579-81 (2024).

189. See *infra* Section II.D.

addressing the normative implications of attempting to apply free-world concepts in digital-carceral spaces.

C. *Intersections Between Carceral Technologies and Free-World Law*

Data-surveillance harms that burden privacy interests are not a new problem. While courts continue to grapple with the contours of privacy writ large, the Supreme Court has laid out specific parameters for free-world applications. For example, in the Fourth Amendment context, the Court has distinguished between digital and analog searches.¹⁹⁰ And although the doctrine is less established, the Court has similarly distinguished information gathering from restrictions on speech in the First Amendment context.¹⁹¹

Many may wonder why, assuming the recognition of digital privacy rights in a carceral setting, courts would not rely on familiar free-world precedents. One problem is that the Justices on the Court appear divided on which test to apply and when.¹⁹² For example, among the various doctrines applied in the Fourth Amendment context is the longstanding third-party doctrine — akin to assumption of risk — articulated by the Court in *Smith v. Maryland*.¹⁹³ *Smith* held that individuals do not retain a reasonable expectation of privacy in telephone numbers individuals dialed because the number was voluntarily given to a third party (the phone company).¹⁹⁴

More recently, the Court considered two cases on the warrantless searches of cell phones where it declined to apply *Smith*'s third-party doctrine. In *Riley v. California*, the Court held that digital data did not pose an inherent danger to police officers and that warrantless cell-phone searches could not be categorically justified on this basis following a lawful arrest.¹⁹⁵ Four years later, the Court similarly declined to grant a warrant exception for cell-site location data in *Carpenter v. United States*, explicitly rejecting the notion that the geolocation data

190. *Riley v. California*, 573 U.S. 373, 386 (2014).

191. See Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1055 (2000) (first citing *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 32 (1984); and then citing *Houchins v. KQED, Inc.*, 438 U.S. 1, 12 (1978)).

192. See, e.g., *Carpenter v. United States*, 585 U.S. 296, 397–98 (2018) (Gorsuch, J., dissenting) (disagreeing with the Court's use of the *Katz* test and proposing a property-based analysis to analyze limits on government data surveillance); *United States v. Jones*, 565 U.S. 400, 410 (2012) (applying the trespass test to analyze whether the warrantless installation of a GPS tracking device on the defendant's vehicle violated the Fourth Amendment).

193. *Smith v. Maryland*, 442 U.S. 735, 742–44 (1979).

194. *Id.* at 744–45.

195. *Riley*, 573 U.S. at 386–87.

trail created by a cell-phone user has been “voluntarily” conveyed to the cell-phone provider.¹⁹⁶

Under existing precedent, courts will inevitably struggle to determine whether *Smith* (third-party doctrine) or *Riley/Carpenter* (reasonable expectation of privacy) is the better fit for evaluating novel digital infrastructure in carceral settings. Consider a video-visitation system. Imagine that, before the call connects, an automated recording informs all participants that their calls “may be monitored for security purposes.”¹⁹⁷ The term “monitored,” however, includes the use of artificial intelligence (AI) to scan every video call in real time, logging participants’ perceived emotions, crossmatching facial recognition against a gang-affiliation database, and flagging keywords through live audio transcription. One prisoner’s weekly call with his mom could be flagged for showing “angry expressions,” and a “known associate” might become flagged through a false facial-recognition match. The incarcerated individual may even be disciplined with restricted technology access based on the flagged call.

Free-world applications of Fourth Amendment law provide little guidance under these circumstances, as each framework possesses its own complications when deployed in carceral settings. Under *Smith*, a court might hold that no search occurred because the prisoner and carceral-adjacent individual voluntarily engaged in the video call, thereby sharing information with a third party and nullifying any expectation of privacy.¹⁹⁸ Alternatively, under *Riley*, AI surveillance may constitute a Fourth Amendment search, given that AI-enhanced scrutiny of expressive traits transforms mere visual monitoring into a qualitative examination. To add another complication, each of these precedents fails to resolve the difficult questions arising in the digital space regarding who retains a property interest in the data.¹⁹⁹

Likewise, in the First Amendment context, identifying the triggering constitutional event can be difficult, especially if the substantive right at issue is not accurately articulated. For example, with regard to outside media access, courts distinguish between restrictions on information access versus receipt, particularly in the carceral space. In *Houchins v. KQED, Inc.*,²⁰⁰ the Supreme Court considered whether the First Amendment guaranteed outside news media a right to

196. *Carpenter*, 585 U.S. at 315.

197. This is intended to be a hypothetical scenario.

198. Section II.D *infra* discusses the normative concerns that consent waivers and, relatedly, voluntary disclosure under the third-party doctrine pose to incarcerated and nonincarcerated individuals.

199. See, e.g., Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700, 704 (2010).

200. 438 U.S. 1, 3 (1978).

access prisons. KQED, a news broadcaster, sought permission to access and take pictures of the interior of the Alameda County Jail at Santa Rita, where an incarcerated individual had committed suicide.²⁰¹ The Court distinguished the right to access information—ancillary to the right to gather information for public dissemination as news—from the right to receive information—ancillary to the right to communicate.²⁰² The Court held that the news media did not have a “special privilege” to access information.²⁰³ Drawing on this logic, courts may similarly recognize limits on active data collection by other actors (in this case, prisons), particularly when the actor seeks data that is not voluntarily shared as part of a relational or communicative exchange.

Where access cannot be controlled, courts have turned their attention to data collection, a precursor to data access.²⁰⁴ For example, in an emergency order, the Supreme Court recently considered the harms associated with foreign-government access to mass troves of individual data.²⁰⁵ The First and Fourth Amendment doctrines on information creation, collection, and access in free-world contexts offer a meaningful framework whose principles can be alloyed to help distinguish legitimate regulation from unconstitutional interference.²⁰⁶

But prison law has long functioned as a separate legal ecosystem, and the proliferation of digital tablets has significantly blurred the line between carceral and noncarceral surveillance—making spatial divisions poor proxies for delineating constitutional protections. Thus, digital technologies in carceral spaces present numerous issues of first impression. The following Section addresses the normative implications of these carceral technologies for existing consent frameworks, along with the consequences of expanded suspicionless surveillance of nonincarcerated individuals.

201. *Id.*

202. *Id.* at 12.

203. *Id.* at 10.

204. See, e.g., *Ams. for Prosperity Found. v. Bonta*, 594 U.S. 595, 616 (2021) (holding that a state regulation compelling the collection of donors’ names for a tax-exempt charitable organization violates the First Amendment because the disclosure creates a risk of chilling associations); *ACLU v. Clapper*, 785 F.3d 787, 801-02 (2d Cir. 2015) (holding that appellants established standing to bring a Fourth Amendment seizure challenge to the government’s bulk collection of telephone metadata in addition to a First Amendment claim for violating associational privacy).

205. *TikTok Inc. v. Garland*, 604 U.S. 56, 72 (2025).

206. See *infra* Part IV.

D. *The Normative Implications of Carceral Technologies*

This Section addresses the ill fit between existing consent doctrine and more intrusive data-surveillance technologies, as well as the unique burdens that carceral technologies pose on nonincarcerated communities.

1. *The Fiction of Carceral Consent*

The principle of consent appears in both First and Fourth Amendment doctrine. To understand how consent is invoked, it is important to first interrogate a critical but often overlooked set of distinctions in the carceral-surveillance landscape: data *creation*, data *collection*, and data *access*. In prison law, the distinction between data creation and collection is often flattened. Traditional monitoring mechanisms—such as mail inspection or call recording—primarily involve the passive collection of preexisting information. Under current prison policies, handwritten letters can be converted to searchable text, and printed photographs can be stored in a facial-recognition repository.²⁰⁷ When the state intercepts content already written or spoken, the constitutional inquiry typically proceeds under established exceptions to the Fourth Amendment. But prison policies mandating the use of digital technologies blur this boundary, shifting from passive collection to the active creation of new data. Put differently, tablets do not simply capture what already exists—they compel incarcerated individuals to generate continuous streams of behavioral, emotional, and physiological data.²⁰⁸ As prisons phase out alternative means of communication—such as physical mail or in-person visitation—the shift from data collection to creation has diminished incarcerated persons’ capacity to consent.²⁰⁹

The creation of data may be inevitable given the increasing use of technology in carceral spaces. But the necessity of data creation should not provide presumptive consent to state actors to access and use that data. Even though baseline surveillance is often justified on the basis of security needs, a separate constitutional intrusion arises when prisons use compelled data to interfere with or condition access to fundamental rights.²¹⁰ Though data retention in an increasingly digit-

207. See, e.g., Leah Wang, *Mail Scanning: A Harsh and Exploitive New Trend in Prisons*, PRISON POL’Y INITIATIVE (Nov. 17, 2022), <https://www.prisonpolicy.org/blog/2022/11/17/mail-scanning> [<https://perma.cc/2W76-SBW4>]; Shakeil Price, *When New Jersey Switches Prison Tablet Companies, I’ll Lose 10 Years of Family Memories*, MARSHALL PROJECT (May 9, 2025), <https://www.themarshallproject.org/2025/05/09/new-jersey-prison-jpay-viapath-tablet> [<https://perma.cc/384Y-9RLN>].

208. See Makar, *supra* note 3, at 1005, 1008.

209. See Wessler & Luna, *supra* note 34.

210. See *infra* Part III.

ized world may be commonplace, the challenge lies not in preventing storage altogether, but in scrutinizing the scope of governmental access.²¹¹

Here, Fourth Amendment doctrine tends to assume the permissibility of consent waivers without interrogating whether withholding consent was ever a meaningful possibility.²¹² Lower courts have long authorized prisons to record and listen to nonlegal prison calls under the premise that at least one party on the call has consented to recording.²¹³ Prerecorded statements at the beginning of a call often indicate that the conversation involves an individual at a correctional facility and that the call is being monitored for security purposes.²¹⁴ Prison handbooks also include similar disclaimers, and notices of this type are typically posted around telephone stations.²¹⁵

Valid consent waivers typically depend on voluntariness.²¹⁶ In criminal-procedure jurisprudence, for instance, the analysis turns on many factors, including the environment, coercion, claim of authority, or deception by the officer, along with the defendant's age, education, mental state, and knowledge of the right to refuse.²¹⁷ Prison-law frameworks reinforce the legal fiction that incarcerated

211. Recent scholarship has emerged challenging the value of “inescapability” as a framework for establishing Fourth Amendment digital privacy protections. See, e.g., Tokson, *supra* note 82, at 428. This Article accepts the proposition that our society is growing increasingly reliant on innovations of digital technology and recognizes that inescapability may be a less relevant or informative inquiry. But inescapability takes on its truest form when privacy interests intersect with carceral systems. As such, I believe that inescapability is a precursor for determining whether the collection of data should be suspect, giving rise to higher scrutiny if such data needs to be accessed later by a carceral actor.

212. See Christopher Slobogin & Kate Weisburd, *Illegitimate Choices: A Minimalist(?) Approach to Consent and Waiver in Criminal Cases*, 101 WASH. U. L. REV. 1913, 1919, 1921–22, 1932, 1950–51 (2024).

213. The Supreme Court has never clarified whether prisoners have a reasonable expectation of privacy in their phone calls and, if so, whether prisoners and carceral-adjacent individuals waive their Fourth Amendment protections. See *supra* Section II.B.

214. See *infra* note 225.

215. See, e.g., Off. of the Inspector Gen., *Criminal Calls: A Review of the Bureau of Prisons’ Management of Inmate Telephone Privileges*, U.S. DEP’T JUST. ch. 3 (Aug. 1999), <https://oig.justice.gov/sites/default/files/archive/special/9908/callsp3.htm> [<https://perma.cc/2D5U-E6RL>]; *United States v. Workman*, 80 F.3d 688, 693 (2d Cir. 1996) (holding that prison monitoring is exempt from the federal wiretapping statute because prisoners voluntarily make telephone calls with the knowledge that they are recorded).

216. In *Schneckloth v. Bustamonte*, the seminal consent-search case, the Supreme Court held that voluntariness should be assessed by “careful scrutiny of all the surrounding circumstances.” 412 U.S. 218, 226–27 (1973); see Kate Weisburd, *Criminal Procedure Without Consent*, 113 CALIF. L. REV. 697, 703 (2025).

217. *Schneckloth*, 412 U.S. at 226, 233–34. A wide body of scholarship critiques as illegitimate consent searches on the front end of the criminal process. See generally Anna Arons, *Family*

individuals meaningfully consent to surveillance and communication constraints. Recall the *Safley* test described in Section II.A. *Safley*'s second prong asks whether, despite the regulation in question, alternative means remain available for the prisoner to exercise the right.²¹⁸ Under such logic, if a prison eliminates access to phone calls but permits letters or in-person visitation, the restriction is presumptively reasonable.²¹⁹ But this wooden analysis fails to grapple with the qualitative dimensions of communication. Phone calls are not simply a convenience; for many incarcerated individuals, particularly those far from their families, they are the only practical avenue for maintaining relationships.²²⁰ By treating all forms of communication as interchangeable, *Safley* obscures the reality that incarcerated people lack any meaningful ability to consent; the differing benefits of each communication mode push them to relinquish one substantively distinct experience for another to access essential services through surveillance-heavy platforms.

But consent-waiver doctrine—in both Fourth Amendment criminal procedure and prison law—still requires that a prisoner relinquish a right voluntarily.²²¹ Though the threshold for voluntariness is low, it nevertheless requires that

Regulation's Consent Problem, 125 COLUM. L. REV. 769 (2025) (discussing consent searches in state family-regulation practices); Nila Bala, *Policing Children's Data*, 103 WASH. U. L. REV. 249 (2025) (critiquing searches of children's data and the inadequacy of parental consent); Jamelia Morgan, *Disability's Fourth Amendment*, 122 COLUM. L. REV. 489, 544-45 (2022) (critiquing the totality-of-the-circumstances inquiry for individuals with disabilities). Postconviction consent waivers usually appear contractual, requiring individuals to sign away certain liberties as a condition to access another right. For instance, in the course of holding that parolees can be subject to suspicionless searches based on their legal status, the Supreme Court in *Samson v. California* noted that the defendant-petitioner had signed a form waiving his right to Fourth Amendment protections as a condition of his release on parole (though it did not ultimately rely on this argument). 547 U.S. 843, 846-47 (2006). For those released early on parole, a similar condition attaches. These consent waivers involve rights trade-offs based solely on legal status. The idea of voluntariness in such circumstances operates as a legal fiction. The operative question is not simply whether incarcerated or carceral-adjacent individuals voluntarily consented to surveillance, but whether they had any real choice to withhold consent in the first place. This is a perennial problem with consent waivers generally but especially those executed in carceral settings where choice is already limited. See, e.g., Weisburd, *supra* note 216, at 714-16.

218. *Turner v. Safley*, 482 U.S. 78, 90 (1987).

219. See, e.g., *Pell v. Procunier*, 417 U.S. 817, 824 (1974) (validating a prison's ban on face-to-face media interviews where prisoners could still communicate with reporters via mail).

220. See, e.g., Emma Kaufman, *The Prisoner Trade*, 133 HARV. L. REV. 1815, 1857-58 (2020) (discussing the costs of prison transfers and the impact of distance on familial relations).

221. Exceptions to this principle include the special-needs doctrine, which specifies that the "special needs" of prison environments reduce expectations of privacy. *Griffin v. Wisconsin*, 483 U.S. 868, 873-74 (1987). This argument may work when dealing with immediate risks posed

participants knowingly assume the risk associated with a discrete activity.²²² In traditional surveillance contexts—phone calls or physical mail—the presumption is grounded in the notion of knowing engagement.²²³ Individuals transmitting information through these channels are generally understood to be aware of the surveillance risk and the nature of the disclosed information.²²⁴ The finite scope of such monitoring bolsters this presumption: a phone call is recorded, and a letter is screened. The communicative act does not generate new layers of personal data beyond the conveyed content.

Case law on phone taps, a long-accepted, hybrid form of carceral and carceral-adjacent surveillance, reveals the haphazard application of prison law's Fourth Amendment doctrine. Federal appellate courts have regularly permitted prisons to record and eavesdrop on calls based on mistaken assumptions about Supreme Court precedent.²²⁵ In so doing, these courts do not rely on the third-party doctrine as established in *Smith v. Maryland*²²⁶ and instead invoke *Palmer*. For instance, the Second Circuit in *United States v. Amen* applied the doctrine of implied consent and claimed, "If security concerns can justify . . . wholly random cell searches . . . then surely it is reasonable to monitor prisoners' telephone conversations, particularly where they are told that the conversations are being monitored."²²⁷ This sort of cursory analysis misses a critical point: cell searches were not found to be protected "searches" within the context of the Fourth Amend-

by contraband, but it does not translate to surveillance that exceeds a penological interest. Compare *Riley v. California*, 573 U.S. 373, 386 (2014) (holding that searches of cell-phone data pursuant to an arrest generally require a warrant), with *Hudson v. Palmer*, 468 U.S. 517, 527 (1984) ("Virtually the only place inmates can conceal weapons, drugs, and other contraband is in their cells. Unfettered access to these cells by prison officials, thus, is imperative if drugs and contraband are to be ferreted out and sanitary surroundings are to be maintained.").

222. For a critique of voluntariness, see Slobogin & Weisburd, *supra* note 212, at 1935-36.

223. See *id.* at 1935.

224. See *supra* note 215 and accompanying text.

225. Lower courts have consistently held that prisoners provide implied consent to the recording and monitoring of phone conversations any time the prison provides notice of the recording. See, e.g., *United States v. Amen*, 831 F.2d 373, 378-80 (2d Cir. 1987) (holding that prisoners impliedly consented to having their phone conversations monitored where they had received notice of the surveillance through an orientation lecture, informational handbooks, and notices posted on the prison walls near telephone booths); *United States v. Corona-Chavez*, 328 F.3d 974, 978-79 (8th Cir. 2003) (upholding a finding of inferred consent when the defendant voluntarily wore investigatory recording devices); *United States v. Hammond*, 286 F.3d 189, 192 (4th Cir. 2002) (inferring consent based on the individual's use of a prison telephone); *United States v. Footman*, 215 F.3d 145, 155 (1st Cir. 2000) (same); *United States v. Van Poyck*, 77 F.3d 285, 292 & n.11 (9th Cir. 1996) (inferring consent from warning signs, receipt of a prison manual explaining the process, and a signed consent form).

226. 442 U.S. 735, 743-45 (1979).

227. *Amen*, 831 F.2d at 379-80 (citations omitted).

ment, whereas strip searches were deemed a protectable—yet nevertheless reasonable—form of search. In other words, when the court relies on implied consent, it must find that the individual has voluntarily waived an existing protected interest—one notably absent in *Palmer*.

Lower courts also improperly assume that *Palmer* eliminates all expectations of privacy for incarcerated people. In *United States v. Jarmon*, the Third Circuit analyzed prison phone taps in light of *Carpenter v. United States*, holding that the parties lacked the subjective expectation of privacy required by *Carpenter* based on the recording notices provided at the beginning of each call.²²⁸ Unlike *Amen*, *Jarmon* did not rely on consent waivers (implying a voluntary waiver of a protected interest) but instead assumed that *Palmer* erased all subjective²²⁹ expectation of privacy for incarcerated people.²³⁰

In this way, phone-tap doctrine represents the beginning of a domino effect of acquiescence for more recent technological advances like video visitations,

228. See *United States v. Jarmon*, 14 F.4th 268, 272 (3d Cir. 2021) (recognizing that the *Carpenter* framework would not apply, as “there is nothing ‘unique’ or technologically advanced about prison phone calls that counsels for extending the Fourth Amendment to that milieu”).

229. This presumption is yet another misreading of *Palmer*. The *Palmer* Court reasoned that an objective expectation of privacy did not exist because society was unprepared to recognize it. The *Palmer* Court’s use of the word “subjective” is confusing because it is invoked for the opposite purpose: “[W]e hold that society is not prepared to recognize as legitimate any subjective expectation of privacy that a prisoner might have in his prison cell and that, accordingly, the Fourth Amendment proscription against unreasonable searches does not apply within the confines of the prison cell.” *Hudson v. Palmer*, 468 U.S. 517, 525–26 (1984) (emphasis added). *Palmer* never reached a decision on the subjective prong in the context of cell searches. See *id.* at 526–27. Thus, *Palmer* does not stand for the proposition that prisoners retain “no general expectation of privacy during their incarceration,” as alleged in *Jarmon*. *Jarmon*, 14 F.4th at 272; see also Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 114 (2015) (analyzing 540 cases applying the *Katz* test and arguing that the subjective prong has no impact on case outcomes). Furthermore, few courts are willing to question whether implied consent waivers are constitutionally valid in prisons. See *Langton v. Hogan*, 71 F.3d 930, 936 (1st Cir. 1995) (identifying as a genuine dispute whether the government can obtain implied consent from detainees where it predicated phone access on a signed consent form); cf. Kay L. Levine, Jonathan Remy Nash & Robert A. Schapiro, *The Unconstitutional Conditions Vacuum in Criminal Procedure*, 133 YALE L.J. 1401, 1429 (2024) (recognizing the Fourth Amendment’s implied-consent doctrine as an unconstitutional condition that requires a rights trade-off).

230. To determine whether individuals subject to a search provide implied consent, courts look to the surrounding circumstances that indicate whether the parties knowingly agreed to the search. See, e.g., *Schneckloth v. Bustamonte*, 412 U.S. 218, 226–27 (1973); *Amen*, 831 F.2d at 378–79. When applying this standard to phone records in prisons, courts have considered whether there were disclaimers in handbooks provided upon entry to the facility, automated disclaimers at the beginning of calls, or signage posted around phone booths within the facility indicating that calls are recorded. See, e.g., *supra* notes 215, 225 and accompanying text. These disclaimers tend to convey that the substance of the communication—not necessarily a person’s voiceprint, facial features, or even the contents of one’s home—is being recorded.

causing continuing confusion regarding the existence of a protected interest (and how such an interest may be relinquished).²³¹ Yet, regardless of this confusion, cases like *Amen* and *Jarmon*, in quietly extending *Palmer* beyond its original logic, open the door for correctional officers and prosecutors to monitor video calls and peer into the homes of those on the outside.

In *United States v. Campbell*, law enforcement obtained a warrant to search and seize illegal firearms and drugs from Campbell's home observed during a video call between Campbell and an incarcerated individual.²³² The court held that no Fourth Amendment violation had occurred because Campbell "assumed the risk of surveillance" and therefore had no expectation of privacy.²³³ Although this form of interference may justify government intrusion (carceral surveillance that provides the basis for noncarceral searches),²³⁴ these extensions are far from benign. Such surveillance can provide a basis for a warrant or even new criminal prosecutions based on political motives or unpopular beliefs, disproportionately aimed at carceral and carceral-adjacent populations.²³⁵ If video calls replace in-person visits, this kind of surveillance could become an end run around Fourth Amendment protections.²³⁶ These technologies drastically expand carceral sur-

231. See, e.g., Hinds, *supra* note 108, at 825-27 (describing women as "shadow defendants" who, by their association to incarcerated associates, "are prosecuted and penalized right alongside their system-involved loved one"); cf. *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979) ("[A] search or seizure of a person must be supported by probable cause particularized with respect to *that* person." (emphasis added)).

232. No. 23-141, 2024 WL 2112873, at *1 (E.D. Pa. May 10, 2024).

233. *Id.* at *8.

234. For a discussion on justified forms of interference, see *infra* Section III.B.3.

235. See *infra* Section III.B.3.

236. Affirmation by Attorney Elizabeth Daniel Vasquez in Support of Verified Article 78 Petition, *supra* note 17, at 12-20. Litigation challenging the TSPs' community-surveillance practices is already underway. *Id.* And state legislatures are beginning to understand the deeply invasive ways that TSPs have used incarcerated people to obtain data on broader carceral-adjacent communities, introducing legislation that limits the recording and retention of any voice or text communications. See Makar, *supra* note 3, at 976-79 (identifying patents for geolocation capabilities, e-commerce searches, voice and facial recognition, and language learning models). We can imagine the nefarious ways such data might be used. For example, various police departments maintain gang databases, often based on vague criteria and without the knowledge of individuals in the database; these "known" gang associations may then be used when making arrest decisions. See Wayne A. Logan, *Policing Police Access to Criminal Justice Data*, 104 IOWA L. REV. 619, 648-49 (2019). Police already use biometric data, such as fingerprints, DNA, or iris/facial imaging, that can be obtained in several ways, including during an arrest (even if no conviction results). Further, biometric information can lead to false positives, which disproportionately impact people of color. See Logan, *supra*, at 649-50; see, e.g., Kashmir Hill, *Facial Recognition Led to Wrongful Arrests. So Detroit Is Making Changes*, N.Y. TIMES (June 29, 2024), <https://www.nytimes.com/2024/06/29/technology/detroit-facial->

eillance beyond prison walls and condition access to communication on the government's visual entry into private homes.²³⁷ It should not be assumed that these individuals consensually waived any expectations of privacy or assumed the risk of surveillance under these circumstances.²³⁸

Digital communication platforms in carceral settings unsettle this model of consent. Conditioning consent on compulsion – that is, conditioning individuals' access to rights on their use of carceral technologies – raises serious questions about the meaningful and voluntary nature of this consent, especially when refusal means total deprivation of access. Further, even when incarcerated individuals and their associates may be presented with consent forms or terms of use, disclosures are typically buried in vendor-drafted, legalistic agreements that fail to present the full picture of how data collected may serve future uses.²³⁹ Consent under these circumstances is neither fully informed nor meaningfully revocable, and digital infrastructure imposes continuous surveillance far exceeding the discrete review of traditional communications. As a result, consent frameworks function less as a safeguard and more as a permissive fiction – masking the expansion of carceral control under the guise of user agreement.²⁴⁰

2. *Expanding the Carceral Sphere*

Traditional applications of First and Fourth Amendment prison law also fail to account for the impacts of carceral technologies on outside communities. Indeed, digital technologies allow government intrusions to metastasize far beyond the physical boundaries of the prison. When an individual becomes incarcerated, their immediate community feels the repercussions, extending from

recognition-false-arrests.html [https://perma.cc/S5TP-MBQQ]; Int. No. 96, N.Y.C. Council, 2026-2029 Sess. (2026), https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=7861501&GUID=B2D0700D-oFoE-4DFE-886D-FD09108BA91B [https://perma.cc/2B7Y-FMZ2].

- 237. For a discussion of new prison policies that replace traditional modes of communication, such as physical mail or in-person visits, with tablets, see *infra* Section III.A.
- 238. In the digital space, where it is harder to affirmatively consent to every intrusion, courts might turn away from implied-consent waivers and rely on something like the third-party-doctrine rationale in *Smith v. Maryland*, 442 U.S. 735 (1979), to avoid addressing privacy harms.
- 239. See generally Stephen Raher, *The Company Store and the Literally Captive Market: Consumer Law in Prisons and Jails*, 17 HASTINGS RACE & POVERTY L.J. 3 (2020) (surveying unfair practices in the prison retail industry).
- 240. Scholars like Orin S. Kerr have identified terms of service as illegitimately waiving Fourth Amendment rights. See Orin S. Kerr, *Terms of Service and Fourth Amendment Rights*, 172 U. PA. L. REV. 287, 288 (2024) (stating that terms of service “define relationships between private parties, but private contracts cannot define Fourth Amendment rights”); see also Farhang Heydari, *The Private Role in Public Safety*, 90 GEO. WASH. L. REV. 696, 705-06 (2022) (discussing law-enforcement use of private-surveillance capacities).

financial, emotional, and care-related collateral consequences²⁴¹ to a range of rights intrusions, including physical searches and communications surveillance when interacting with an incarcerated individual.²⁴²

Temporal limits traditionally minimized the degree of intrusion against non-incarcerated individuals, based on their brief engagement with the carceral space. In phone-call monitoring, for example, prisons only have limited information about the outsider—in most cases, their name, relationship, and phone number—and not much else beyond the information shared in the phone call. And for in-person visits, prison officials must have reasonable suspicion to conduct a body-cavity search of a nonincarcerated individual.²⁴³

Through contemporary digital technologies, however, contacts with the carceral system have increased in frequency, number, and depth.²⁴⁴ The same phone call, now mediated digitally, reveals much more about the carceral-adjacent individual.²⁴⁵ For instance, it could provide live geolocation data if the individual is using a cell phone,²⁴⁶ access to a carceral-adjacent individual's e-commerce history,²⁴⁷ and voice and linguistic patterns.²⁴⁸ Prior to the advent of these technologies, this information could not have been gleaned from traditional monitoring mechanisms, even with substantial time and effort.

TSPs, unlike other private data collectors like Google or Meta,²⁴⁹ are uniquely positioned to extend the carceral sphere far beyond prison walls to family

241. See Michael Pinard, *Collateral Consequences of Criminal Convictions: Confronting Issues of Race and Dignity*, 85 N.Y.U. L. REV. 457, 489-94 (2010).

242. Though carceral-adjacent individuals are not themselves incarcerated, the privacy of their homes can be encroached upon if they are housing an individual who has been released but remains subject to government oversight due to ongoing punishment (such as parole or probation). See Hinds, *supra* note 108, at 868-70.

243. See Makar, *supra* note 3, at 981 & n.115 (discussing the distinction between carceral-level versus population-level impacts). Recall that in *Florence*, the Supreme Court held that the reasonable-suspicion standard does not apply to prisoners. *Florence v. Bd. of Chosen Freeholders*, 566 U.S. 318, 330 (2012); see *supra* Section II.B.

244. See Johnson, *supra* note 18.

245. *Id.*

246. See *Riley v. California*, 573 U.S. 373, 387, 394-96 (2014).

247. See Cooper Quintin & Beryl Lipton, *The Catalog of Carceral Surveillance: Monitoring Online Purchases of Inmates' Family and Friends*, ELEC. FRONTIER FOUND. (Sep. 7, 2021), <https://www.eff.org/deeplinks/2021/09/prison-surveillance-catalog-monitoring-online-purchases-inmates-family-and-friends> [https://perma.cc/77XK-YBCH].

248. *Discover THREADS*, *supra* note 15.

249. See, e.g., *United States v. Chatrice*, 136 F.4th 100, 102 (4th Cir. 2025) (en banc) (Diaz, J., concurring) (discussing Google's internal three-step geofence-warrant compliance procedure), *cert. granted*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026).

members, friends, and broader communities.²⁵⁰ In these situations, the TSP and the government are one and the same – once the data is collected, there is nothing to prevent the government from arbitrarily accessing it. And in this environment, one’s “digital DNA” – the behavioral and biometric data generated through everyday interactions – may be as revealing as physical sources of DNA, underscoring how carceral surveillance regimes reach deeper and wider than existing jurisprudence has recognized. Armed with this information, the government is uniquely positioned to expand its surveillance to increasingly larger groups of individuals.²⁵¹

III. CARCERAL PRIVACY THROUGH THE LENS OF DATA-SURVEILLANCE TECHNOLOGIES

With litigation over digital tablets in its early stages, lower courts have reflexively applied prison-law precedent despite its simplistic spatial logic.²⁵² This Part reviews recent decisions on digital tablets to demonstrate how lower courts have myopically focused on nonrelational rights, spatial logics, and consent waivers rather than the expressive and privacy-based harms that should guide their analysis.

Section III.A reviews recent federal district-court cases involving digital surveillance in prisons, revealing how courts’ dispositional deference to security concerns masks expressive privacy harms and results in chilled relational rights. Section III.B then reenvisions these cases through a “compelled data” lens, showing how this alternative framework reveals critical privacy harms and provides a mechanism to distinguish between legitimate and illegitimate forms of data interference.

A. *Limitations of Prison-Law Precedent: Lower-Court Applications and Loopholes*

This Section reviews recent lower-court decisions involving digital technologies in which courts applied either a traditional *Safley* or *Palmer* analysis.

250. See *Raher*, *supra* note 73, at 76–84 (likening the expansive net of surveillance to a “digital prison yard—one that ensnares not just incarcerated people, but their friends, families, and correspondents as well”).

251. See KHIARA M. BRIDGES, *THE POVERTY OF PRIVACY RIGHTS* 138 (2017).

252. An analysis of the property-law dimensions surrounding prison tablets is outside the scope of this Article and reserved for future discussion.

1. *Evaluating Digital Prison Policies Under Turner v. Safley*

Prison policies mandating the transition from paper-based to digital communications are growing in popularity across prisons and jails.²⁵³ Prisons often contract with a third-party provider to scan any incoming mail, including letters, documents, and photographs. The provider then makes this information available on shared electronic kiosks or individual digital tablets while retaining the original copies separately for a finite period.²⁵⁴

Amid an increase in litigation over digital-mail policies, lower courts have turned to *Safley* to resolve these First Amendment challenges. However, digital-based harms illustrate the shortcomings of *Safley*'s one-dimensional approach to First Amendment issues. Many of these cases touch on the chilling effects of indiscriminate access to private information, the lack of consent to data creation and digital storage, and the related deprivations of property—only to be classified by courts as simple “mail interference” challenges.²⁵⁵ The following discusses four examples.

First, consider *Smith v. Wolf*.²⁵⁶ Kareem Smith brought a First Amendment challenge to a prison's digital-scanning policy, objecting to the use of a third-party contractor to process incoming mail.²⁵⁷ The facility's policy authorized the third party to inspect mail for contraband, scan and digitize it, store the digitized images for seven years, and destroy the physical original copies after fifteen days.²⁵⁸ Smith advanced two core objections. First, he alleged that the digitization process improperly altered his correspondence: while his family had mailed color photographs, the images accessible to him on his tablet appeared only in black and white.²⁵⁹ Second, he contended that the prison lacked a legitimate penological justification for destroying the original mail and for retaining digitized family correspondence without his or his family's consent.²⁶⁰ Applying *Safley*, the district court held that the policy was reasonably related to the legitimate

253. See Wessler & Luna, *supra* note 34.

254. See Wang, *supra* note 207; Aaron Gordon, *Prison Mail Surveillance Company Keeps Tabs on Those on the Outside, Too*, VICE (Mar. 24, 2021), <https://www.vice.com/en/article/prison-mail-surveillance-company-keeps-tabs-on-those-on-the-outside-too> [<https://perma.cc/J52C-K7BF>].

255. See, e.g., *Mason v. Wright*, No. 24CV129, 2025 WL 350230, at *3 (E.D. Va. Jan. 30, 2025).

256. *Smith v. Wolf*, No. 19-cv-0711, 2020 WL 4551229, at *1 (M.D. Pa. Aug. 6, 2020).

257. *Id.*

258. *Id.*

259. *Id.*

260. *Id.* at *3.

penological objective of preventing contraband.²⁶¹ The court concluded that digital copies of mail constituted an adequate alternative under *Safley*'s framework.²⁶²

But the *Safley* test focused on the wrong issues. First, *Safley*'s framework limited the court's focus to the policy's penological interest, leading it to misconstrue the nature of the harm and mistake compulsion for consent. Smith not only argued that meaningful communication — specifically, family photographs conveying sentimental value — had been improperly altered, but he also raised concerns about the storage of personal biometric data.²⁶³ *Safley*, however, did not provide a framework for analyzing these harms. Second, *Safley*'s focus on penological interests and prisoners' rights masked the relational-privacy harms imposed upon carceral-adjacent individuals. Smith argued that the recorded images, which depicted his family members, had been retained by a third-party contractor without his or his relatives' consent. Though there may be a penological interest served in restricting physical mail, there is no legitimate penological interest in the digital storage of a nonincarcerated individual's facial image. But *Safley* does not account for the policy's impact on nonincarcerated associations and their interests.²⁶⁴

Second, in *Diez v. Texas Department of Criminal Justice*,²⁶⁵ the Southern District of Texas reviewed a digital mail-scanning policy like that in *Smith*. Here, the court raised the concern that the prison might be placing prisoners' information data on a "[p]otentially [h]ackable [s]ystem."²⁶⁶ Although prisons can delegate certain functions to private actors,²⁶⁷ the court reasoned, it was a "separate question whether the activity, as delegated, is appropriately secure so as to maintain inmate privacy, particularly given the danger of exposing personally identifying information and/or personal financial information to the free world."²⁶⁸ Despite

261. *Id.* at *8; see also *Overton v. Bazzetta*, 539 U.S. 126, 135 (2003) (applying *Safley* to an in-person visitation policy and stating that "[a]lternatives to visitation need not be ideal, however; they need only be available").

262. *Wolf*, 2020 WL 4551229, at *8.

263. *Id.* at *3; see Wang, *supra* note 254 (describing the sentimental value that physical mail provides prisoners and noting that it helps maintain mental health and reduce recidivism).

264. *Wolf* is one example of *Safley*'s dispositional favoritism, as the test itself predisposes the court to adopt a myopic approach at the detriment of the broader set of interests implicated by the scanning policy. See Dolovich, *supra* note 54, at 311-12.

265. No. 23-CV-00269, 2024 WL 1959293 (S.D. Tex. May 3, 2024), *appeal dismissed*, No. 24-40350, 2024 WL 3912951 (5th Cir. Aug. 23, 2024).

266. *Id.* at *2.

267. *Id.* (citing *Rosborough v. Mgmt. & Training Corp.*, 350 F.3d 459, 461 (5th Cir. 2003)).

268. *Id.*

a growing number of digital-mail challenges,²⁶⁹ *Diez* is unique because the court recognized the possibility that carceral digital policies present issues of first impression.²⁷⁰

Consider a third case, *Woodell v. Wetzel*,²⁷¹ in which the Third Circuit reviewed the dismissal of a plaintiff's claims that the prison's digital-mail policy, which applied to both privileged legal mail and nonprivileged mail, violated his First Amendment rights. Regarding the nonprivileged mail, Woodell argued that the policy had a chilling effect on his family's ability to communicate with him, as his "family would no longer send him correspondence or photographs because the originals would be stored in Smart Communications' database and then destroyed."²⁷² The Third Circuit affirmed the dismissal of Woodell's case, agreeing that he failed to state a First Amendment claim.²⁷³ Importantly, this case highlights additional problems within the carceral space — namely, the burden on pro se plaintiffs seeking to convincingly articulate issues of first impression posed by digital technologies.²⁷⁴

As a final example, consider a carceral-adjacent individual prevented from communicating with incarcerated individuals seeking to report prison conditions. In *Bailey v. Federal Bureau of Prisons*, Pamela Bailey, a prisoners' rights advocate, sued the Federal Bureau of Prisons (BOP) for barring her from speaking with prisoners.²⁷⁵ Bailey argued BOP targeted her after the launch of a hotline used to report mistreatment within BOP facilities, seemingly spurred by her advocacy.²⁷⁶ Granting Bailey preliminary injunctive relief on her First Amendment censorship claim, the court enjoined six of the seven BOP facilities that had blocked her access.²⁷⁷ In so doing, the court voiced concerns regarding the

269. See, e.g., *Swindler v. Hanlin*, No. 24-cv-00590, 2024 WL 4555382, at *1 (D. Or. Oct. 23, 2024).

270. *Diez*, 2024 WL 1959293, at *2.

271. No. 20-3235, 2022 WL 17424287, at *1 (3d Cir. Dec. 6, 2022).

272. *Id.*

273. *Id.* at *2. While the case was pending before the district court, the prison agreed to stop processing privileged legal mail through the third-party provider. Therefore, the Third Circuit did not need to address this issue. *Id.* Nevertheless, scanning and storing privileged legal mail underscores the privacy harms at stake when third parties and correctional officers have access to privileged communications. See, e.g., *Haze v. Harrison*, 961 F.3d 654, 661 (4th Cir. 2020).

274. Like *Smith v. Wolf*, the court framed the family's reticence to send materials as a "choice," despite the chilling effects of the digital policy. *Woodell v. Pa. Sec'y of Corr.*, No. 18-4430, 2020 WL 2841380, at *11 (E.D. Pa. June 1, 2020), *aff'd sub nom.*, *Woodell v. Wetzel*, No. 20-3235, 2022 WL 17424287 (3d Cir. Dec. 6, 2022). This framing offers yet another instance of the dispositional favoritism facilitated under *Safley*, inhibiting courts' understanding of the privacy harms at stake. See Dolovich, *supra* note 54, at 320.

275. No. 24-1219, 2024 WL 3219207, at *1-2, *8 (D.D.C. June 28, 2024).

276. *Id.* at *8.

277. *Id.* at *9.

current prison-law doctrinal frameworks, recognizing that digital platforms are wholly different from physical mail.²⁷⁸ Though the court declined to address which test—*Safley* or *Martinez*—was appropriate, it held that Bailey would prevail under either test.²⁷⁹

Cases like the four discussed above are growing in number²⁸⁰ and highlight not only the blind spots in a First Amendment test crafted for static carceral spaces but also courts' instinct to defer to carceral institutions even in the face of issues of first impression.²⁸¹ The following Section reveals lower courts reflexively turning to *Hudson v. Palmer* to navigate Fourth Amendment challenges. These cases show lower courts clearly overstepping the bounds of *Palmer* and misapprehending the nature of Fourth Amendment harms in the context of digital technologies.

2. Evaluating Digital Prison Policies Under *Hudson v. Palmer*

Fourth Amendment cases pose their own challenges, inside and outside of prisons. Often, these disputes tend to encounter standing issues before the court ever considers the merits of plaintiffs' claims, as most Fourth Amendment cases only arise when illicit activity is discovered or when the person whose property is searched becomes aware of the intrusion.²⁸² This is even more consequential in prisons as the infrequency of these cases makes it more likely that courts will automatically resort to *Palmer* without considering the broader digital consequences of such a decision.²⁸³ Further, compared to the First Amendment claims,

278. *Id.* at *5 (“Another district court, analyzing an inmate’s challenge to the Georgia Department of Corrections’ censorship of his outgoing electronic messages, noted that which standard to apply was ‘a much tougher question than it appears at first blush.’” (quoting *Benning v. Dozier*, No. 18-0087, 2021 WL 1713333, at *1 (M.D. Ga. Apr. 30, 2021))).

279. *Id.* at *8.

280. See, e.g., *Swindler v. Hanlin*, No. 24-cv-00590, 2025 WL 919488, at *2 (D. Or. Mar. 26, 2025); *Abdullah v. Briggs*, No. 24-CV-00225, 2024 WL 1313242, at *4 (M.D. Pa. Mar. 27, 2024).

281. See Dolovich, *supra* note 54, at 323.

282. Cf. Aliza Hochman Bloom, *Suspicion by Association*, 68 ARIZ. L. REV. 1, 6 (2026) (“Because of the nature of our judicial process, the only police-citizen interactions reviewed in criminal adjudications are those where police found contraband. . . . This [selection] bias creates an inaccurate perception of police infallibility whereby courts do not review cases of the hundreds of people searched daily where criminal charges do not arise.”).

283. See, e.g., *Cecil v. Keller*, No. 23-cv-00310, 2025 WL 918165, at *6 (W.D. Va. Mar. 25, 2025) (dismissing Cecil’s Fourth Amendment claim without analyzing the differences between physical and digital searches). Consider, for example, the circuit split on cell-phone searches incident to arrest before *Riley v. California*. See Jayme W. Holcomb & Nathaniel Counts, *Searches Incident to Arrest in the Smartphone Age*, FBI L. ENF’T BULL. (Dec. 10, 2013), <https://leb.fbi.gov/articles/legal-digest/legal-digest-searches-incident-to-arrest-in-the-smartphone-age> [<https://perma.cc/TC6J-FHQP>].

this body of law is still developing, as many cases alleging illegal searches of digital tablets have been dismissed at the outset of the suit. These dismissals likely stem from lower courts misunderstanding and therefore overextending *Palmer* under the false premise that it denies incarcerated individuals any expectation of privacy.

One example of this misapplication occurred in *Triggs v. Barnhardt*.²⁸⁴ In *Triggs*, a correctional officer allegedly confiscated the plaintiff's tablet without cause.²⁸⁵ From the court's telling, correctional officers found written documents during a cell search that suggested Triggs might have attempted to access Tor (the dark web); after the initial cell search, officers searched Triggs's tablet and found similar typed instructions on how to access Tor, along with other materials on group organizing that the prison deemed to be a security threat.²⁸⁶ Triggs argued that the prison had no penological interest in confiscating and searching his tablet. But the court invoked *Palmer* to hold that Triggs had no reasonable expectation of privacy in his cell or in any of the possessions stored in his cell, including the tablet.²⁸⁷ It reasoned that because *Palmer* permits cell searches for the purposes of security, the same principle surely extends to searches of electronic devices.²⁸⁸

Next, consider the limitations of *Palmer* when analyzing Fourth Amendment seizures. In *House v. Henderson County Detention Center*,²⁸⁹ the prison facility implemented a digital mail-scanning policy for all incoming mail. House raised several claims but most notably argued that the act of scanning his mail constituted an unreasonable seizure under the Fourth Amendment.²⁹⁰ The court turned to *Palmer*, citing the case for the proposition that "there can never be a reasonable expectation of privacy while in prison."²⁹¹ First, this statement is

284. No. 20-cv-8, 2020 WL 1149701, at *4 (W.D. Mich. Mar. 10, 2020).

285. *Triggs v. Barnhardt*, No. 20-cv-8, 2021 WL 6550824, at *1 (W.D. Mich. Dec. 16, 2021) ("Triggs confronted [Sgt.] Barnhardt and asked why his tablet had not been returned to him. Barnhardt allegedly told Triggs that he had intended to give the tablet back, but because Triggs wrote a grievance against him, he was 'going to make sure that [Triggs] gets nothing back.'" (citation omitted)), *report and recommendation adopted*, No. 20-cv-08, 2022 WL 170062 (W.D. Mich. Jan. 19, 2022).

286. *Triggs*, 2020 WL 1149701, at *2.

287. *Id.* at *4-5.

288. *Id.* at *4. Notably, the court need not have turned to or expanded *Palmer*, since the correctional officers had reasonable suspicion to believe that Triggs may have illegally accessed the dark web, thereby satisfying the free-world standard of particularized suspicion as grounds for a search.

289. No. 21-CV-00038, 2022 WL 4279724 (W.D. Ky. Sep. 15, 2022).

290. *Id.* at *4.

291. *Id.*

objectively incorrect based on the Court's holdings in *Florence* and *King*.²⁹² Second, this misinterpretation of *Palmer* forces the court to assume categorically that House did not have a possessory interest in his mail.²⁹³ As a result, the court missed a critical opportunity to consider whether data collection (here, the act of digitally copying mail) may constitute an unreasonable interference — as a search or a seizure.²⁹⁴

The instinct to rely on *Palmer* prevents courts from viewing the broader privacy implications at play. A tablet “search” differs markedly from a traditional cell search and raises distinct due-process concerns. A physical cell search is typically brief and, once completed, allows the individual to resume using the space. By contrast, a tablet search can function as a prolonged and opaque investigative sweep without clear time limits, making it less like a search and more like surveillance.²⁹⁵ When communication with loved ones or access to legal resources are mediated through the tablet, its confiscation triggers a cascading deprivation, magnifying due-process concerns.

Palmer therefore covers wholly different scenarios than what occurred in *Triggs* or *House*. *Palmer* permits randomized, suspicionless searches limited to the physical space of the cell where only a finite amount of information can be

292. For further analysis of *Florence* and *King*, see *supra* Section II.B.

293. See, e.g., *Haze v. Harrison*, 961 F.3d 654, 661 (4th Cir. 2020) (noting that *Palmer* provides no dispositive test in determining whether incarcerated individuals retain an expectation of privacy in their legal mail).

294. The Supreme Court's precedent exclusively analyzes digital technologies as searches, thereby justifying the reflex to categorize *House*'s Fourth Amendment claim in this way. Nevertheless, given the all-encompassing nature of the data collection at issue, prison tablets supply a unique opportunity to view data collection as a seizure and reconsider how property interests might be implicated in the digital age. Cf. *Carpenter v. United States*, 585 U.S. 296, 397–98 (2018) (Gorsuch, J., dissenting) (proposing a property-based analysis to analyze limits on government data surveillance).

295. Data collected on tablets can be relayed back to TSPs and accessed by correctional officers through various different infrastructures. For example, the tablet may need to be hooked up to a kiosk in order to transmit data that it collects. See, e.g., Div. of State Gov't Accountability, *Controls over Tablet and Kiosk Usage by Incarcerated Individuals*, N.Y. STATE OFF. STATE COMPTROLLER (May 11, 2023), <https://www.osc.ny.gov/state-agencies/audits/2023/05/11/control-s-over-tablet-and-kiosk-usage-incarcerated-individuals> [<https://perma.cc/H94E-N2AW>]. Data may also be relayed back to TSPs and available to correctional officers in real time where TSPs have installed their own private Wi-Fi network in the facility. See, e.g., *Raher*, *supra* note 21.

held.²⁹⁶ In other words, if contraband is found within a prison, a court is not going to prevent the prison from discovering the evidence or using it to discipline an individual.²⁹⁷ Through cases like *Triggs* and *House*, however, courts open the door to long-term surveillance of digital technology that contains far more information than what can be gleaned from the physical items in a cell.

B. Drawing a Line Between the Need for Security and Obscurity

Recognizing digital privacy rights for incarcerated individuals would limit the state's ability to monitor and prevent potential criminal activity. But in permitting total surveillance, courts conflate surveillance with security, collapsing the distinction between legitimate security interests and unconstitutional carceral control.²⁹⁸ The default of total surveillance, rooted in the fallacious “nothing to hide”²⁹⁹ argument, underestimates the power of surveillance tools to interfere with individuals’ interior lives.³⁰⁰

The baseline argument for surveillance is that individuals convicted of a crime are “dangerous” because they committed a crime; therefore, due to their

296. *Triggs* also cites *DiGuiseppa v. Ward*, a case permitting the search of a prisoner’s diary. 698 F.2d 602, 604–05 (2d Cir. 1983). This case is particularly misleading: unlike *Palmer*, the court found that it was *reasonable* to search the individual’s diary within the meaning of the Fourth Amendment, as the search formed a direct and timely response to recent a prison riot. In other words, the court conducted its analysis as though the prisoner retained a reasonable expectation of privacy in his diary. The *DiGuiseppa* court also noted the difficulty in navigating which constitutional amendment to apply when dealing with the right to privacy and ultimately chose to analyze the right under the Fourth Amendment as opposed to the First. *Id.* at 605. The Supreme Court has never addressed whether an indiscriminate search of a prisoner’s diary is constitutional under either the First or Fourth Amendments. Lower courts’ general lack of care in acknowledging the limits of existing precedent and the impacts of their holdings on the experiences of incarcerated individuals reiterates their favorable disposition toward institutional actors. See Dolovich, *supra* note 54, at 341–42.

297. Cf. Dolovich, *supra* note 54, at 302–03 (arguing that prison law’s incoherence stems from its deference and favoritism toward carceral institutions).

298. See BRIDGES, *supra* note 251, at 138 (“[W]hen the state’s knowledge about its subjects approximates perfection, state power approximates perfection.”).

299. Daniel J. Solove, “I’ve Got Nothing to Hide” and Other Misunderstandings of Privacy, 44 SAN DIEGO L. REV. 745, 748–53 (2007).

300. See Woodrow Hartzog, *What Is Privacy? That’s the Wrong Question*, 88 U. CHI. L. REV. 1677, 1680–81 (2021); cf. G.W.F. HEGEL, HEGEL’S PHILOSOPHY OF RIGHT 37–57 (T.M. Knox trans., Oxford Univ. Press 1942) (1820) (articulating a theory of property and describing positive rights as tied to and materializing in external objects).

dangerousness, they have relinquished any expectation of privacy.³⁰¹ This argument assumes that prisoners, by the very nature of their legal status, are typically seeking to engage in and hide bad activity.³⁰² Not only is this logic problematic, but it also assumes good motives by those in charge of surveillance.³⁰³

As demonstrated in Section III.A above, existing prison-law jurisprudence militates in favor of surveillance and thereby promotes this misguided logic. For instance, the *Turner v. Safley* test,³⁰⁴ which originated prior to the modern digital world, makes it far too easy to conclude that any right can be limited in its access through a single medium (including a tablet), any right can be abused to engage in bad activity, and the only reasonable way to keep tabs on what a prisoner is doing on a tablet is to surveil all data on it.³⁰⁵ Put differently, any surveillance requirements placed on the use of the tablet would presumably always pass muster under the *Safley* test. This test, coupled with *Hudson v. Palmer*—frequently misinterpreted to afford zero Fourth Amendment protection to prisoners—results in a doctrinal dead end for the intractable problems of data compulsion.³⁰⁶ As such, the existing jurisprudence assumes that prisoners raising privacy claims intend to withhold something illegal, rather than something legal (or deeply personal).³⁰⁷

This Section turns to the concept of compelled data to show where privacy-based interferences exist within data-driven surveillance regimes. But this Section also considers where security and obscurity³⁰⁸ can coexist, outlining three

301. Cf. Driver & Kaufman, *supra* note 120, at 553–54 (noting that the Court has “described prison as the paradigmatic privacy-free zone”); *id.* (“[P]arolees sit on a ‘continuum’ that runs from probation to prison, with fewer and fewer privacy rights as the punishment gets more severe.”).

302. Cf. *Hudson v. Palmer*, 468 U.S. 517, 528 (1984) (emphasizing the effectiveness of randomized searches).

303. Cf. Walter Pavlo, *Corrections Officers Often Key to Contraband Introduced into Prison*, FORBES (Sep. 30, 2021), <https://www.forbes.com/sites/walterpavlo/2021/09/30/corrections-officers-often-key-to-contraband-introduced-into-prison> [<https://perma.cc/CBQ5-VTVU>] (describing how corrections officers facilitate the introduction of contraband into prisons).

304. See 482 U.S. 78, 89 (1987).

305. See *supra* Section II.A.2; cf. Driver & Kaufman, *supra* note 120, at 537–39 (arguing that prison law is premised on inaccurate and inconsistent generalizations about incarcerated people).

306. *Palmer*, 468 U.S. at 530.

307. Cf. *DiGuiseppe v. Ward*, 514 F. Supp. 503, 505 (S.D.N.Y. 1981) (quoting *Lanza v. New York*, 370 U.S. 139, 143–44 (1962)), *rev’d*, 698 F.2d 602 (2d Cir. 1983).

308. The Supreme Court first endorsed the concept of “practical obscurity” in *U.S. Department of Justice v. Reporters Committee for Freedom of Press*, recognizing that individuals may retain a privacy interest in information that, although technically available to the public, is not easily accessible. 489 U.S. 749, 762 (1989). With rapid technological advancements posing increas-

key categories of interference³⁰⁹: (1) surveillance as passive interference (intrusions that incarcerated persons never recognize and that have no legitimate penological aim other than to collect information); (2) surveillance as active interference (intrusions prisoners only become aware of through retaliatory action); and (3) surveillance as justified interference (intrusions resulting from suspected illicit activity). This Section addresses each form of interference to demonstrate how the concept of compelled data remedies current prison-law doctrine's conflation of surveillance and security.

1. *Passive Interference*

Surveillance for the sake of surveillance — that is, for nonpenological aims — can result in harmful consequences for both incarcerated and carceral-adjacent individuals. Such surveillance is likely to be passive, meaning that no immediate action is taken based on real-time monitoring; information is simply stored and used in some manner at an undetermined time. The policies at issue in *Smith*, *Diez*, and *Woodell* exemplify this category of interference, permitting the retention of recordings, texts, or mail for extended periods.³¹⁰ With inexpensive data storage, facilities often lack any safeguards to prevent correctional officials from accessing this stored data long after it was originally gathered.³¹¹ Such unfettered

ing threats to individual privacy, scholars have examined the ways in which obscurity functions as a critical privacy interest. See, e.g., Daniel J. Solove & Woodrow Hartzog, *The Great Scrape: The Clash Between Scraping and Privacy*, 113 CALIF. L. REV. 1521, 1562 (2025); Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 388 (2013). Obscurity supports this Article's conception of compelled data by recognizing the inevitability of data collection — and even creation — while appropriately balancing the privacy harms associated with access to and use of that data.

309. Incarcerated individuals form the locus of carceral institutions' surveillance — the greater the incarcerated individual's contacts with society, the more points of information that the institution can collect and the larger the carceral sphere. This Section explores this relationship in greater depth, examining how, when accompanied by unchecked interference, surveillance that occurs in the carceral setting can nevertheless have significant ripple effects on outside communities.

But it is difficult to know exactly when and why correctional officers use digital surveillance, as these practices are embedded in almost every activity. As such, this Section examines only those digital-surveillance intrusions visible from the perspective of the incarcerated individual.

310. See *supra* Section III.A.1.

311. See, e.g., Barry Friedman, *Lawless Surveillance*, 97 N.Y.U. L. REV. 1143, 1196 (2022) (identifying the tension between the government's possession of large volumes of data and the absence of safeguards governing later access and use).

access allows for retrospective investigations, exploitation of private communications, or even the development of predictive algorithms.³¹²

These harms extend beyond incarcerated individuals.³¹³ Data that is passively collected, stored, and later utilized can lead to surveillance of carceral-adjacent individuals, advocacy groups, or individuals who merely cross paths with an incarcerated individual.³¹⁴ Data such as zip codes, facial-recognition profiles, and purchase histories may be shared with correctional officials or used for broader law-enforcement surveillance.³¹⁵ Here, there is an important value in obscurity. Once collected, information like zip codes can be used to map networks of associations³¹⁶ or exploited for commercial purposes, capitalizing on the vulnerabilities of individuals with incarcerated loved ones.³¹⁷ Although passive interference may appear insignificant, it has the potential to create new avenues for systemic exploitation and exacerbate subordination among vulnerable communities.

2. Active Interference

Carceral surveillance may also manifest as a form of active content moderation.³¹⁸ Without barriers between correctional officers and an incarcerated individual's data, this information becomes vulnerable to arbitrary oversight and retaliatory actions. The absence of safeguards allows for unchecked discretion, enabling correctional officers to target individuals based on personal biases or institutional objectives.³¹⁹ For example, in cases where incarcerated individuals

312. See Viljoen, *supra* note 61, at 587–91.

313. See Makar, *supra* note 3, at 1000; Viljoen, *supra* note 61, at 579.

314. Cf. Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 855 (2022).

315. See *supra* note 236 and accompanying text.

316. See, e.g., O'Donnell, *supra* note 94; Viljoen, *supra* note 61, at 579.

317. See, e.g., Dave Maass, *The Catalog of Carceral Surveillance: Tablet Advertising that Can Also Issue Discipline*, ELEC. FRONTIER FOUND. (Apr. 7, 2022), <https://www EFF.ORG/deeplinks/2022/04/catalog-carceral-surveillance-tablet-advertising-can-also-issue-discipline> [<https://perma.cc/86WS-H9RZ>] (describing a hypothetical scenario—based on a 2016 patent obtained by Securus—in which TSPs introduced pop-up advertisements during video calls which targeted users based on AI learning).

318. Content moderation can be both passive and active. Passive content moderation might involve limiting incarcerated people to preapproved lists of apps, e-books, and calling lists. This Section uses an example of active content moderation that occurs in real time.

319. See, e.g., Jeremy Busby, *The Latest FCC Censorship Push No One Is Talking About Targets Incarcerated People*, INTERCEPT (Oct. 3, 2025), <https://theintercept.com/2025/10/03/fcc-brendan-carr-cellphone-prison-censorship> [<https://perma.cc/7V2S-WGFL>] (reporting that prison officials invoke security concerns to justify cell-phone jammers aimed at preventing discl-

use digital platforms to communicate grievances or engage in advocacy, officers may censor or punish such communications as a form of retaliation, even in the absence of any legitimate security threat.³²⁰

Digital surveillance not only heightens the likelihood of content moderation conducted for nonpenological purposes but also compounds the difficulty of challenging such retaliatory actions. The inherent information asymmetry between what incarcerated individuals know about the scope of surveillance and what correctional officers articulate as the justification for a punitive measure creates a profound imbalance. In practical terms, this disparity makes it harder for incarcerated individuals to contest such actions in grievance processes or court.

Recall *Bailey*, the case on retaliatory e-messaging censorship.³²¹ The primary harm in this dispute involved the policy's chilling effect on criticisms of authority—both by prisoners and carceral-adjacent individuals like Bailey.³²² Incarcerated individuals have a legal right to challenge adverse experiences or confinement conditions within carceral facilities, and they already face significant challenges in accessing means to redress. Between legal doctrines permitting bans on media access to prisons³²³ and litigation hurdles under the Prison Litig-

osure of prison conditions or abuse through contraband phones); Sheera Frenkel & Mike Isaac, *Homeland Security Wants Social Media Sites to Expose Anti-ICE Accounts*, N.Y. TIMES (Feb. 13, 2026), <https://www.nytimes.com/2026/02/13/technology/dhs-anti-ice-social-media.html> [<https://perma.cc/4QVC-TANX>].

320. For an example of e-messaging retaliation, see *supra* notes 275-278.

321. See *supra* Section III.A.1.

322. See Citron & Solove, *supra* note 314, at 845-55 (discussing autonomy harms that include coercion, manipulation, failure to inform, and chilling effects); Franks, *supra* note 56, at 453 (“If being forced to alter one’s online search habits is considered a chilling effect that undermines democracy, being forced to alter one’s clothing, job, school, choice of friends, communication with family, romantic relationships, or freedom of movement should surely be viewed even more seriously. For the less privileged members of society, surveillance does not simply mean inhibited Internet searches or decreased willingness to make online purchases; it can mean an entire existence under scrutiny, with every personal choice carrying a risk of bodily harm.”); Michele Estrin Gilman, *The Class Differential in Privacy Law*, 77 BROOK. L. REV. 1389, 1408 (2012); David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1094-1101 (2014).

323. See, e.g., *Pell v. Procunier*, 417 U.S. 817, 835 (1974) (upholding a prison policy that banned in-person contact between media representatives and inmates).

ation Reform Act,³²⁴ government actors suppress criticism in ways both anti-democratic and troubling.³²⁵

But the ability to censor information can leave incarcerated individuals powerless to redress harms that occur against them and can itself be used as a retaliatory tool. Active speech restrictions in carceral settings do more than limit personal expression—they also interfere with the full array of speech-based constitutional rights.³²⁶ The lack of transparency surrounding surveillance not only heightens the chilling effect on speech but also complicates efforts to challenge retaliatory actions. Incarcerated individuals often remain unaware of the basis for punitive measures taken in response to their speech. This absence of disclosure fosters a climate of self-censorship, where individuals must weigh the risks of expressing themselves against the unknown consequences of government interference.³²⁷ Though courts have traditionally afforded deference to the penological interests assumed to justify prison policies, retaliatory surveillance practices shielded from scrutiny present a significant departure from traditional modes of prison security.

3. *Justified Interference*

In carceral settings, rampant surveillance—passive or active—can lead to the post hoc discovery of unauthorized activity. These situations raise critical questions about the proper balance between legitimate security interests and expansive surveillance practices. When defined too loosely, “security” rationales enable disproportionate responses untethered from concrete penological needs.

Consider the case of Devin Jarid Vu, an incarcerated individual at Minnesota Correctional Facility-Faribault enrolled in an educational program that provided

324. See, e.g., Danielle C. Jefferis, *Carceral Deference: Courts and Their Pro-Prison Propensities*, 92 FORDHAM L. REV. 983, 992–93 (2023).

325. Cf. Bloom, *supra* note 282, at 6 (describing the selection bias in physical-search case law). Given the relatively frictionless nature of digital surveillance, the likelihood that a particular search would be noticed, tied to an adverse action, and challenged is even lower.

326. See Citron & Solove, *supra* note 314, at 854–55 (describing the ripple effects of chilling injuries); Jonathon W. Penney, *Understanding Chilling Effects*, 106 MINN. L. REV. 1451, 1463 (2022) (describing common theories of chilling harms). Carceral facilities often use tablet revocation as a disciplinary tool. See, e.g., Burrell v. DOCCS, 655 F. Supp. 3d 112, 123 (N.D.N.Y. 2023) (“On June 2, 2022, [the correctional officer] conducted another hearing and denied plaintiff’s requests for witnesses, documentary evidence, and legal representation. [The officer] sentence[d] plaintiff to a loss of tablet use ‘because he liked filing grievances.’” (citation omitted)).

327. See, e.g., Class Action Complaint for Injunctive Relief and Damages, *supra* note 15, at 15–16.

digital-tablet access.³²⁸ On January 23, 2025, officials allegedly discovered Vu in possession of digital copies of child pornography.³²⁹ Importantly, the discovery of Vu's illicit content was not a product of unchecked, indiscriminate surveillance. Correctional officers had learned that several tablets in this educational program had been altered to allow for unrestricted internet access.³³⁰ Officials sent all tablets in the program out for forensic analysis³³¹ and found illegal content only on Vu's tablet.³³²

Here, correctional officers had an individualized basis and a legitimate penological purpose to investigate Vu's tablet.³³³ Like in *Triggs*, applying some form of heightened scrutiny would not hinder a prison's ability to identify and prevent such activity.³³⁴ Even so, the harms in *Triggs's* and Vu's cases do not justify expanding the scope of *Palmer*, which held that incarcerated individuals have no reasonable expectation of privacy in their cells.³³⁵ A prison cell, though it holds personal possessions, is visible to anyone who walks past it; any expectation of privacy is therefore minimal. Digital tablets contain a different type and quantity of information, often extending beyond what can be discovered through a traditional search of a physical cell.³³⁶ The distinction between these two forms of privacy complicates the argument justifying indiscriminate digital surveillance, even where this surveillance occurs in carceral spaces.

In stretching *Safley* or *Palmer* to justify increasingly invasive forms of technological surveillance, lower courts have seriously eroded key First and Fourth Amendment protections.³³⁷ Instead of focusing on penological interests and

328. Press Release, Faribault Police Dep't & Rice Cnty. Att'y's Off., D.O.C. Inmate Charged with 22 Counts of Possessing Pornographic Images Involving Minors 1 (Jan. 23, 2025), <https://ci.faribault.mn.us/DocumentCenter/View/11317/012325---Media-Release---Unauthorized-tablet-use-at-DOC> [<https://perma.cc/4BNT-3WRT>].

329. *Id.*

330. *Id.*

331. *Id.*

332. *Id.*

333. *Id.*

334. See *Florence v. Bd. of Chosen Freeholders*, 566 U.S. 318, 348 (2012) (Breyer, J., dissenting) (arguing that the reasonable-suspicion standard would not hinder penological interests); *Hudson v. Palmer*, 468 U.S. 517, 551 (1984) (Stevens, J., concurring in part and dissenting in part) (arguing that the deference afforded prisons officials prevents the court from assessing whether the prison's conduct satisfies a legitimate penological interest).

335. *Palmer*, 468 U.S. at 525-26 (majority opinion).

336. See, e.g., *Riley v. California*, 573 U.S. 373, 401 (2014).

337. See, e.g., David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 71-72 (2013) (arguing that the threshold Fourth Amendment inquiry should be "whether

reasonable expectations of privacy (or the lack thereof), courts should assess whether the conditions compelling the creation and retention of digital information unjustly interfere with constitutionally protected interests. Part IV proposes an unjust-interference framework to analyze data-surveillance harms that arise through compelled-data regimes.

IV. RECONCEPTUALIZING THE BOUNDARIES OF CARCERAL INTERFERENCE

The compelled-data framework views all data generated through data-surveillance technologies as inherently suspect, yet these intrusions have received greater deference in the lower courts than existing precedent allows.³³⁸ This Part contends that digital carceral spaces ought to be treated as categorically distinct from their physical counterparts. In support of this claim, this Part offers one possible doctrinal departure: rather than relying on standard prison-law precedent—*Turner v. Safley* and *Hudson v. Palmer*—courts should reconceptualize data-driven surveillance as compulsion and consider whether the government has engaged in unjust interference with respect to constitutionally protected, privacy-based rights. Under the current framework, use of a rights-accessing device serves as implied consent to pervasive surveillance, foreclosing any inquiry into whether the scope of monitoring constitutes unconstitutional interference. Reframing these practices as compelled data collection exposes the legal fiction embedded in implied-consent and assumption-of-risk doctrines³³⁹ and allows courts to bypass the isolated analysis of whether a First or Fourth Amendment violation has occurred. By alloying principles drawn from the First Amendment’s compelled-speech doctrine and the Fourth Amendment’s evolving data-privacy jurisprudence, this Part offers a framework in response to the deficiencies encountered in early prison-tablet litigation.³⁴⁰

This Part does not intend to propose a singular or exclusive solution to the pervasive problems raised by data compulsion, but rather a starting point for

a technology has the capacity to facilitate broad and indiscriminate surveillance that intrudes upon reasonable expectations of *quantitative* privacy” (emphasis added)); SOLOVE, *supra* note 58, at 63–64; Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1018 (2010) (articulating a framework to analyze Fourth Amendment issues through a content vs. noncontent distinction).

338. See *supra* Section I.B.

339. Legal scholars such as Kate Weisburd have critiqued the fictitious role consent plays when used to justify the deprivation of another person’s rights. Weisburd, *supra* note 216, at 730; see also Franks, *supra* note 56, at 437 (noting that doctrines of consent tend to equate privacy with secrecy, requiring individuals to keep private information entirely secret in order to retain constitutional privacy rights).

340. See *supra* note 67.

conceptualizing how digital-surveillance technologies reshape the boundaries of state power.³⁴¹ Though this theory primarily applies within carceral settings, its application to carceral-adjacent individuals proves its workability in other arenas, pushing courts away from the free-world versus prison divide (and perhaps even from the Fourth Amendment's reasonable-expectations-of-privacy test in digital spaces writ large).³⁴²

Section IV.A provides a framework applying the concept of unjust interference to compelled-data policies. Section IV.B situates compelled data in the larger data-privacy and consumer-rights movements and recognizes supplemental data-governance interventions to promote neutrality and transparency.

A. *Unjust Interference*

The Constitution contains no rights to receive a colored photograph, to hold a paper letter, to send a text message, or to visit someone in person. But there is a right to communicate. There is no freestanding right that prohibits data collection by private companies. But there is a right to be free from unreasonable searches and seizures. The conduct at issue in many carceral-surveillance cases — often hyper-specific, technologically novel, and deeply contextual — can obscure the fundamental constitutional rights truly at stake. In reality, such conduct constitutes the *form* of interference, not the *substance* of the right. Reframing carceral surveillance as *data compulsion* — where communication is not merely observed but compelled and transformed into analyzable and retainable digital traces — offers two immediate analytic benefits. First, it clarifies how digital infrastructure converts private and expressive activity into a source of ongoing governmental control through public-private partnerships. And second, it emphasizes the necessity of recalibrating constitutional doctrine to recognize the qualitative differences between analog and digital intrusions on privacy.

Generally, interference occurs when the government injects itself in a manner that either burdens or meaningfully obstructs access to a constitutionally protected right.³⁴³ For example, interference occurs when prison officials open

341. Data collection by government actors is a pervasive problem. Legal scholars have proposed various constitutional and normative interventions to address these issues. *See generally* Barry Friedman, *The Constitutionality of Indiscriminate Data Surveillance*, 174 U. PA. L. REV. 293 (2026) (arguing that bulk data collection by policing agencies is unconstitutional). This Article contributes to the literature a new framework for balancing individual interests against security concerns.

342. *See, e.g.*, Kerr, *supra* note 229, at 115 (arguing that the objective-expectation prong of the *Katz* test should be the sole normative inquiry).

343. *See, e.g.*, *Procunier v. Martinez*, 416 U.S. 396, 408–09 (1974), *overruled in part by*, *Thornburgh v. Abbott*, 490 U.S. 401 (1989); *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

mail.³⁴⁴ Mail is meant to communicate private information, though the sender and recipient may expect the mail to be screened. The nature of this interference may also be appropriate to advance a legitimate penological objective, such as preventing contraband. This form of interference is neither intended to prohibit the overarching substantive right—that is, the right to communicate—nor does it do substantially burden the substantive right.³⁴⁵

But *unjust* interference arises when the interference alters or undermines the substantive content of the right itself, in ways not sufficiently justified by a legitimate governmental objective. Take, for example, a prison policy upheld under *Safley* that mandates the digitization of all incoming physical mail.³⁴⁶ Although the stated penological justification may be detecting contraband,³⁴⁷ the policy compels the conversion of handwritten or printed communications into digital files, later stored in privately managed databases. In this way, the prison policy generates new, analyzable data points. Thus, while the act of opening mail itself does not create an interference, prison policies that embed government actors in the architecture of communication by manipulating storage and taking ownership over its future use materially transform the communicative right at stake.³⁴⁸

The Supreme Court hinted at the concept of interference in the carceral space when discussing incoming and outgoing mail communications in *Procunier v. Martinez*.³⁴⁹ The Court's concern over unjust interference arose when navigating the relational rights of carceral-adjacent individuals. Justice Powell, writing for the majority, explained, "In the case of direct personal correspondence between inmates and those who have a particularized interest in communicating with them, mail censorship implicates more than the right of prisoners."³⁵⁰

Two core insights emerge from the *Martinez* Court's analysis. First, the Court acknowledged the distinct constitutional stakes associated with relational rights

344. *Martinez*, 416 U.S. at 408-09. Other examples might include restricting visit formats, screening publications, and requiring identity verification for tablet usage. Here, the rights are not denied, but they are burdened for security objectives.

345. *Cf. Volokh, supra* note 64, at 369 (discussing the constitutional infirmities of compelled speech, even when such compulsions do not interfere with or prohibit an individual's other speech rights).

346. *See, e.g., Smith v. Wolf*, No. 19-cv-0711, 2020 WL 4551229, at *1 (M.D. Pa. Aug. 6, 2020).

347. *Id.* at *7.

348. *Cf. United States v. Jones*, 565 U.S. 400, 408 n.5 (2012) (explaining that a trespass alone does not necessarily trigger a Fourth Amendment search or seizure).

349. *Martinez*, 416 U.S. at 409.

350. Here, the Court recognized that communication by letter is not accomplished by the act of writing words on paper. Rather, it is effected only when the letter is read by the addressee. Therefore, corresponding parties have an interest in that result, and communication censorship and information retention necessarily impinge on the interests of each individual. *Id.* at 408.

that cross prison walls and accordingly applied intermediate scrutiny to evaluate policies burdening outgoing mail.³⁵¹ Second, although the Court accepted that incarceration necessarily entails some curtailment of rights, it emphasized that where the stakes involve something as serious as censorship of relational rights, intrusions must be justified by important or substantial penological objectives.³⁵² The Court thereby affirmed a constitutional boundary for permissible state interference, one confined to the institutional context of the prison itself.

Subsequent developments, including the *Safley* test and the historical insulation of carceral institutions from public scrutiny, likely stymied the growth of an “unjust interference” doctrine in the prison context. To date, this author has identified only a single instance in which a federal appellate court has undertaken analysis grounded in *Martinez’s* unjust-interference framework: *Gassler v. Wood*.³⁵³ Yet this case may provide some parameters for limiting government interferences that are not spatially bound by incarceration.

In this case, Gassler and Scott, two pretrial detainees indicted for first-degree murder and related charges, brought a § 1983 action against prison officials for violating their First Amendment rights.³⁵⁴ After receiving information that Gassler and Scott had tried to intimidate witnesses set to testify against them, the criminal investigator contacted the detention facility and asked that the two individuals be separated to prevent coordination.³⁵⁵ Although all incoming and outgoing mail was delivered to the intended recipients, the warden also approved the delivery of photocopies of their outgoing mail to the criminal investigator.³⁵⁶ Gassler and Scott alleged that by providing a third party access to photocopies of their nonlegal mail, the prison violated the First Amendment.

The Eighth Circuit considered whether sharing this information with a third party (the criminal investigator) would have a chilling effect upon free expression.³⁵⁷ The court ultimately held that this interference was legitimate,³⁵⁸ reasoning that the criminal investigator had reason to believe the pretrial detainees

351. *Thornburgh v. Abbott*, 490 U.S. 401, 413-14 (1989) (overruling *Martinez* to the extent that it recognized a distinction based on the status of the sender of correspondence to incarcerated individuals); see *supra* note 125 and accompanying text (describing the context of *Thornburgh*); *supra* note 140 and accompanying text (analyzing *Thornburgh’s* effect).

352. *Martinez*, 416 U.S. at 413-14.

353. 14 F.3d 406 (8th Cir. 1994).

354. *Id.* at 407.

355. *Id.* at 407-08.

356. *Id.* at 408.

357. *Id.* at 408-09.

358. *Id.* at 409.

were engaged in coordinated witness-intimidation efforts through the mail.³⁵⁹ Further, the party reviewing the mail was in charge of investigating the case, which included conduct that allegedly occurred while incarcerated.³⁶⁰

This holding illustrates the courts' failure, in *Martinez* and *Gassler*, to grasp the full constitutional stakes of a compulsory data regime. For instance, *Gassler* treats the sharing of photocopied mail as an isolated disclosure justified by a specific investigative need, rather than one part of a broader system in which copying, retention, and aggregation expand governmental access beyond the original security rationale. In analog form, duplication was event-based and bound to an identifiable and actualized government interest; in digital environments, copied documents can be reproduced tenfold and preserved indefinitely, rendering the government's access functionally unlimited.³⁶¹ The constitutional concern, therefore, is not merely that information is "searched" and "copied" but that the architecture of data collection collapses any meaningful firewall between penological monitoring and unjustified government use – transforming incidental review into constant availability.³⁶²

Drawing from the concerns raised by compelled data and the *Gassler* court's analysis, this Section advances four distinct criteria worth considering when determining whether carceral interference in digital spaces is unjust: (1) the nature of the interference; (2) the burden on a substantive right; (3) the circumstances necessitating interference; and (4) the connection between the penological interest and the interference.³⁶³ Each of these criteria is defined below.

Nature of the Interference. This factor identifies the specific conduct challenged and assesses the degree to which the interference occurs. Central to this inquiry is whether the interference remains spatially confined within the prison walls or extends into the broader social domain. The broader the interference's reach, the greater the state's justificatory burden. For instance, surveillance limited to the incarcerated person's e-book purchases may present a relatively

359. *Id.*

360. *Id.* at 407-09.

361. *Cf.* *United States v. Ganas*, 824 F.3d 199, 217-18 (2d Cir. 2016) (noting significant differences between seizures of digital materials as opposed to hard copies and recognizing that indefinite retention of copied digital data raises distinct Fourth Amendment concerns beyond the initial search).

362. *Cf.* *Frenkel & Isaac*, *supra* note 319 (illustrating how government demands for access to private digital communications can collapse the distinction between security monitoring and political surveillance).

363. *Gassler*, 14 F.3d at 407-10.

narrow intrusion and require a lower burden of justification.³⁶⁴ By contrast, interference that reaches beyond the prison, such as monitoring communications with family members, implicates not only relational and expressive interests protected by the First Amendment, including concerns of censorship and chilled association,³⁶⁵ but also Fourth Amendment interests in the possession, retention, and control of expressive materials.³⁶⁶ These dual concerns—increasingly prevalent in the free world—become even more acute in prison settings, where the architecture of surveillance collapses spatial limits and renders both expressive activity and its informational residue continuously accessible to the state.

Burden on a Substantive Right. This factor assesses how the interference affects a substantive right, such as the First Amendment’s right to free speech or the Fourth Amendment’s right to be free of unreasonable searches. It prevents courts from defining the right by the specific conduct challenged, such as the right to text, which tends to favor prison officials.³⁶⁷ For example, in *Bailey*, the challenged interference involved prison officials reviewing and blocking electronic communications between an incarcerated individual and a prisoners’ rights advocate.³⁶⁸ There, the interference chilled dissent and curtailed access to legal advocacy and redress.³⁶⁹ Though the conduct at issue was texting, the burden impacted what the First Amendment protects—speech critical of prison conditions and actors. Focusing on the broader substantive right provides a more holistic look at the impact of the interference.

Circumstances Necessitating Interference. This factor ensures that government interference is tethered to a legitimate, articulable justification—not an abstract or speculative concern. This means the interference must be grounded in a demonstrable penological interest. Importantly, this standard departs from the deferential approach that permits restrictions based on unsubstantiated or

364. This is not to say that book censorship is nonproblematic. See, e.g., Keri Blakinger, Ryan Murphy, Elan Ullendorf & Andrew Rodriguez Calderón, *The Books Banned in Your State Prisons*, MARSHALL PROJECT (Feb. 23, 2023, 10:30 PM EST), <https://www.themarshallproject.org/2022/12/21/prison-banned-books-list-find-your-state> [<https://perma.cc/YP3J-HYRW>]. Rather, this form of interference is different in nature from the harm articulated by data compulsion.

365. See BRIDGES, *supra* note 251, at 152–53.

366. See Kerr, *supra* note 199, at 704.

367. Cf. Dolovich, *supra* note 54, at 316 (arguing that courts often frame the facts to favor the carceral institution).

368. *Bailey v. Fed. Bureau of Prisons*, No. 24-1219, 2024 WL 3219207, at *1-2 (D.D.C. June 28, 2024).

369. *Id.* at *8.

generalized claims of institutional necessity.³⁷⁰ This framework demands that the asserted penological interest be either actualized or supported by a reasonable probability of occurrence. The Eighth Circuit's decision in *Gassler v. Wood* offers a compelling illustration. There, the court upheld the interference only after determining that the criminal investigator had a concrete and credible basis for believing that the parties involved likely posed a real and ongoing threat.³⁷¹ This heightened evidentiary threshold serves a critical function: absent a clear rationale, surveillance and other interferences risk devolving into indiscriminate monitoring.³⁷²

Importantly, this factor does not preclude correctional officers from addressing bona fide security threats.³⁷³ Rather, it operates as a safeguard against abuse, requiring that any intrusion into private communications be sufficiently justified and address a clearly defined and temporally specific concern. By demanding specificity and accountability, this approach protects constitutional rights while preserving institutional safety.

Connection Between Penological Interest and the Interference. The final factor assesses whether the interference serves an important penological interest and whether the policy is substantially related to that interest. It is not sufficient that a penological interest be asserted; the intrusion must be tailored to advance that interest.³⁷⁴ And it must be executed by actors whose involvement is both necessary and appropriate under the circumstances. Again, *Gassler* illustrates this point well. There, the court found the interference justified because the investigator had a compelling, individualized reason to examine the correspondence. The information obtained was not disseminated to third parties beyond those necessary to address the identified threat.³⁷⁵ This logic illustrates the type of alignment needed between the penological interest and the interference associated with compelled data.

370. See Dolovich, *supra* note 54, at 316 (arguing that courts often frame the facts to favor the carceral institution).

371. See *Gassler v. Wood*, 14 F.3d 406, 409-10 (8th Cir. 1994).

372. See Friedman, *supra* note 341, at 309.

373. Compare *Bailey*, 2024 WL 3219207, at *1-2 (finding illegitimate the censorship of e-messages in which incarcerated individuals reported civil-rights violations), with *Triggs v. Barnhardt*, No. 20-cv-8, 2021 WL 6550824, at *2-4 (W.D. Mich. Dec. 16, 2021) (approving the search of a tablet based on a prison officer's reasonable belief that the incarcerated individual was illegally accessing the dark web).

374. Cf. Dolovich, *supra* note 54, at 311, 322 (arguing that courts routinely uphold prison restrictions based on defendants' bare assertions of penological necessity, without requiring evidence that the restriction is actually tailored to advance the stated interest).

375. *Gassler*, 14 F.3d at 409.

The conditions of carceral data collection—often mandatory or effectively so—render these practices especially vulnerable to constitutional scrutiny. Because compelled disclosure of private information is inherently suspect, heightened scrutiny is warranted to ensure that only necessary levels of data can be accessed. Consider two common examples illustrating how the unjust-interference framework might be applied in response to the harms of compelled data.

First, consider a jail policy that bans in-person visitation in favor of video calls.³⁷⁶ The video systems use emotional-detection software that analyzes tone, facial expressions, and speech cadence to infer users' emotional states in real time.³⁷⁷ *Palmer* offers little recourse here, as courts often find no reasonable expectation of privacy due to implied consent waivers or assumption of risk.³⁷⁸ Likewise, *Safley* has had little influence on general policies that restrict one form of communication while leaving another open.³⁷⁹ Traditional doctrine focuses on the policy itself, but the harms identified here stem from the policy's ancillary effects—passive data extraction and emotional profiling.

The real question is not whether prisons may restrict visits, but whether the digital surveillance exerts a chilling or distorting effect on protected expression. Under the proposed framework, this surveillance raises significant constitutional concerns. First, we would consider the nature of the interference. Here, the interference extends beyond the prison, capturing intimate emotional cues exchanged with family members. Second, and critically, the monitored conduct involves tone and expression, thereby burdening the core First Amendment rights of association and expressive intimacy. Third, the circumstances necessitating the interference rely on generalized concerns about physical security rather than individualized suspicion. Finally, the connection between the stated penological interest and biometric surveillance is tenuous.

Consider next a policy requiring all grievance submissions to be filed through prison tablets, ostensibly to reduce contraband risks associated with

376. This is a fictionalized example based on the complaint in *S.L. v. Swanson*. See Class Action Complaint and Demand for Jury Trial, *supra* note 85, at 4.

377. This is a fictionalized example drawing on documents obtained through a Freedom of Information request by the New York Civil Liberties Union. Simon McCormack, *Inaccurate Facial Recognition in Prisons Is Keeping Families Apart*, N.Y.C.L. UNION (Mar. 17, 2023), <https://www.nyclu.org/commentary/inaccurate-facial-recognition-prisons-keeping-families-apart> [<https://perma.cc/5P6G-E7Q8>] (describing the New York Department of Corrections and Community Supervision's use of facial-recognition technology to admit visitors into a correctional facility).

378. See *supra* note 229 and accompanying text.

379. See, e.g., *S.L. v. Swanson*, No. 24-120601-CZ, slip op. at 4-5 (Mich. Cir. Ct. Dec. 30, 2024) (granting the defendant's motion to dismiss and holding that the jail's policy of banning in-person visitation in lieu of video visitation was reasonably related to a legitimate penological interest).

paper.³⁸⁰ AI tools scan the text and flag keywords for review.³⁸¹ Under *Safley* or *Palmer*, this might withstand scrutiny as routine internal monitoring.³⁸² Though surveillance begins inside the facility, its temporal reach—storing and potentially repurposing sensitive grievance information—greatly expands the intrusion. The burden falls on the First Amendment right to seek recourse and speak critically about prison conditions. Absent a specific penological need, such data access risks enabling institutional retaliation and chilling dissent.³⁸³ This framework emphasizes that even seemingly neutral administrative tools can impose disproportionate constitutional burdens when they chill critical speech or enable unchecked surveillance.

The unjust-interference framework offers distinct advantages for addressing the complex privacy concerns in carceral contexts. First, the unjust-interference framework's principal strength lies in its departure from the conventional approach, which defines constitutional claims based solely on the specific conduct challenged. Instead, the unjust-interference framework invites courts to situate the interference within the broader body of law surrounding a substantive constitutional right, such as speech, association, or informational privacy. Second, it accommodates evidentiary challenges in litigation that often undermine individualized claims—particularly the cause-and-effect problem where a “constitutional event” is required to pinpoint the resultant harm—by shifting the focus from the plaintiff's burden to the structural nature of the interference and its likely effects.³⁸⁴ Third, this approach avoids the conceptual limitations of *Palmer* and related cases, which tether privacy rights to physical spaces and thus fail to account for the distinct character of data environments.³⁸⁵

Importantly, adopting an unjust-interference analysis does not require courts to displace established doctrines like *Safley* or *Palmer*. It instead recognizes that digital spaces—particularly those involving compelled use of tablets, communication platforms, and biometric systems—constitute a qualitatively distinct

380. Cf. Tiffany Yang, *The Prison Pleading Trap*, 64 B.C. L. REV. 1145, 1156–57 (2023) (describing the functional importance of a prison grievance).

381. See O'Donnell, *supra* note 94.

382. *Id.*

383. There can be many benefits to digitizing grievance submissions, including improved record keeping and greater accountability. But given cases like *Bailey* that reveal the retaliatory side of unregulated datafication, without sufficient safeguards like those proposed in this Article, the potential benefits to incarcerated persons can quickly be swallowed by the cons. For a discussion on the benefits of data-governance models aimed at improving conditions for incarcerated individuals, see *infra* Section IV.B.

384. See Citron & Solove, *supra* note 314, at 817 (describing the difficulty in recognizing unknown or future privacy harms under the current legal framework).

385. See *Hudson v. Palmer*, 468 U.S. 517, 521 (1984).

category. In this respect, the framework leaves existing precedent untouched while acknowledging that evolving technologies demand new tools. At its core, the claim is not that incarcerated individuals possess an unqualified right to withhold evidence of unlawful activity, but rather that they retain a legitimate privacy interest in their internal lives that gives effect to key First Amendment protections.³⁸⁶ Further, this proposal resolves doctrinal confusion arising from expectation-of-privacy analysis and consent-waiver applications by, again, presuming that data compulsion is inherently suspect and therefore protected. The unjust-interference framework thus affirms that, even in prison, incarcerated people are still entitled to meaningful constitutional protection against unjustified intrusions on their foundational rights.

B. Carceral Privacy and Broader Digital-Rights Movements

The emerging terrain of carceral privacy sits at a critical juncture between the broader data-privacy movement and the digital-consumer-rights movement. Importantly, the expansion of digital technologies into prisons—through tablets, video calls, biometric monitoring, and algorithmic surveillance—mirrors the consumer-data practices seen in society.³⁸⁷ Yet it operates in a legal vacuum where incarcerated individuals are presumed to have forfeited basic privacy claims.³⁸⁸ This assumption allows carceral institutions and their private partners to collect, store, and monetize deeply personal information without meaningful oversight or consent. As a result, the prison becomes both a site of confinement and a data-extraction regime, where incarcerated individuals are stripped not only of their liberty but also of the informational autonomy that data-privacy frameworks increasingly recognize as foundational to democratic life.³⁸⁹

Yet this divide between consumer-facing digital rights and the absence of carceral data protections is neither coherent nor normatively defensible. Contemporary digital-rights advocacy emphasizes transparency, consent, data minimization, and user control—principles rooted in the idea that individuals should retain agency over how their information is used.³⁹⁰ These principles resonate no less forcefully within carceral settings, where surveillance technologies blur

386. See HEGEL, *supra* note 300, at 37–57.

387. “Consumer-data practices” refers to the collection of data about people, ranging from personal identifying information to personal preferences. Notably, this data can be monetized through practices that, for example, push advertisements to users who are more likely to purchase certain products. Legal scholars have referred to this data as “social data.” Amanda Parsons & Salomé Viljoen, *Valuing Social Data*, 124 COLUM. L. REV. 993, 1010 (2024).

388. See *supra* Part II.

389. See Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1905 (2013).

390. *Id.* at 1907.

the line between penal security and commodified observation.³⁹¹ The incarcerated, often from historically marginalized communities, become test cases for invasive technologies later deployed in schools, housing, and public spaces.³⁹² Recognizing carceral privacy as part of the larger digital-rights ecosystem thus demands a reorientation of data-privacy law—one that treats incarceration not as an off-ramp from constitutional or consumer protection but as a focal point for confronting the outer limits of surveillance capitalism and the structural exclusions it perpetuates.

Recognizing the structural asymmetries between carceral data practices and broader digital-rights frameworks raises another, more immediate question: what forms of legal or institutional design might meaningfully constrain the unchecked collection and use of personal information within carceral systems? The conceptual imperative to treat digital carceral surveillance as a matter of privacy-based constitutional concern must be matched by practical mechanisms that respond to its diffuse and often invisible harms. And while courts may be reluctant—or institutionally ill-equipped—to scrutinize every instance of state interference through carceral technologies, that reality does not absolve lawmakers from acting. Rather, it heightens the need for legislative interventions that place *ex ante* limits on how carceral data is accessed, processed, and distributed.

One such proposal comes from legal scholar Barry Friedman, whose innovative data-trust model would require multiple keys to access discrete information by law-enforcement officers.³⁹³ Under this vision, collected personal information would not be held by law-enforcement officers individually. If these officers need access to certain information in order to identify a potential suspect of a crime, the officer would have to request the data from multiple key holders that have to meet certain legal requirements to provide the data.³⁹⁴ These limitations would ensure that officers can access only the discrete information necessary to accomplish legitimate law-enforcement goals, rather than all of an incarcerated individual's personal data.³⁹⁵ Friedman shows how this idea has been proposed and implemented in other settings involving commercial entities or government use of private data for social-welfare purposes.³⁹⁶

A similar approach to data governance could have great appeal in the carceral context, particularly where data can reveal insights on how the state interacts

391. See Raheer, *supra* note 73, at 98-104.

392. See, e.g., SCOTT SKINNER-THOMPSON, *PRIVACY AT THE MARGINS* 44 (2020); BRIDGES, *supra* note 251, at 138.

393. Barry Friedman, *Policing Agency Data Trusts*, 120 NW. U. L. REV. 817, 851-53 (2026).

394. *Id.*

395. *Id.*

396. *Id.* at 856-58.

with those it incarcerates.³⁹⁷ Crucially, the value of carceral data increases when the focus of collection shifts from the incarcerated individual to the institutional processes themselves. Rather than surveilling individuals for punitive or investigative purposes, data can be used to evaluate broader operational patterns—such as staffing shortfalls, procedural bottlenecks, or disparities in treatment outcomes.³⁹⁸ In this form, data becomes a diagnostic tool, allowing stakeholders to identify systemic deficiencies and target reform efforts accordingly.³⁹⁹ Data-governance models can help utilize information collection as a mechanism for institutional self-assessment rather than a means of individual subordination, facilitating a move toward greater transparency and responsiveness. This structure not only aligns with constitutional norms of dignity and fairness but also restores some legitimacy to institutions frequently subject to public scrutiny by promoting evidence-based governance and reducing the risk of arbitrary or retaliatory decision-making.⁴⁰⁰ Yet these benefits are, at best, modest responses to the intractable problems at hand.

Under the existing doctrine of carceral privacy, the state already holds all the keys in the prison. Data-governance models such as data trusts offer partial responses to the pervasive problem of data compulsion, yet they do little to resolve the exploitation of incarcerated individuals and their loved ones by private

397. Cf. Littman, *supra* note 12, at 1390–93 (arguing that applying free-world regulatory frameworks to carceral institutions can reconceptualize incarcerated individuals as members of the public entitled to the protections afforded by broader regulatory infrastructure).

398. See, e.g., Barbie Melendez, *Assessment of Grievance Procedures and Processes in the New York City Department of Correction: 2021–2023*, N.Y.C. BD. CORR. 4 (Dec. 2024), <https://www.nyc.gov/assets/boc/downloads/pdf/Reports/BOC-Reports/LL-133-Grievance-Report-NYC-BOC-12.31.24.pdf> [<https://perma.cc/2H8S-MDBR>] (recommending that the New York City Department of Corrections adopt digital measures to improve submissions and tracking of incarcerated persons' grievance forms).

399. See Shannon Heffernan, *Even Where Abortion Is Legal, People in Jail Face Huge Barriers*, MARSHALL PROJECT (Mar. 26, 2024), <https://www.themarshallproject.org/2024/03/26/jail-abortion-policy-study-illinois-oregon> [<https://perma.cc/EQM9-5TC9>] (describing an incarcerated person who placed a medical request via electronic messaging for an abortion due to a high-risk pregnancy and received a typed sad-face emoticon in response); see also C.R. Div., *Investigation of the Fulton County Jail*, U.S. DEP'T JUST. 58–59 (Nov. 14, 2024), <https://www.justice.gov/crt/media/1377011/dl> [<https://perma.cc/J68C-FYC7>] (finding deficiencies in Fulton County's paper sick-call processes, which resulted in harm to incarcerated individuals).

400. See, e.g., Stephen Rahe, *Best Practices for Prison and Jail Tablet Procurement*, PRISON POL'Y INITIATIVE (July 3, 2024), https://www.prisonpolicy.org/messaging/rfp_guidance.html [<https://perma.cc/AU7H-MX2W>] (recommending that correctional facilities' procurement officials evaluate their tablet vendors on factors like privacy and security, hardware, and availability of valuable apps and programs).

providers.⁴⁰¹ Even forms of data governance that purport to monitor the activities of the prison do not prevent the prison from monitoring the activities of prisoners themselves. Expanding data oversight to be inclusive of carceral actors, though beneficial, would nonetheless amount to an illusory victory in the face of the privacy-crushing doctrinal heavyweights of *Safley* and *Palmer*. Because the erosion of privacy in prisons is produced and sustained by these doctrinal frameworks themselves, it cannot be meaningfully remedied through extraconstitutional oversight mechanisms and instead demands a doctrinal response. Ultimately, if prisons compel incarcerated individuals to disclose digital data about every aspect of their lives, no door to their interiority—or to that of their contacts in the outside world—will remain unopened.⁴⁰²

CONCLUSION

The recent datafication of the carceral experience provides an opportunity to reevaluate privacy interests within prisons, particularly as they extend beyond physically confined spaces into larger communities. Although prisons maintain a legitimate interest in security and order, this Article challenges the indiscriminate deference traditionally given to carceral authorities, especially as digital tools such as tablets reshape interactions within and outside the prison walls. By exploring the intersection of digital technologies and carceral governance, this Article presses us to rethink how privacy should be assessed in this evolving context, recognizing the important and nuanced relationships between incarcerated individuals and those on the outside.

401. See Farhang Heydari, *Understanding Police Reliance on Private Data*, HOOVER INST. 2 (2022), https://www.hoover.org/sites/default/files/research/docs/heydari_webreadypdf.pdf [<https://perma.cc/9LSB-4W2L>].

402. See Cohen, *supra* note 389, at 1906 (“Privacy is shorthand for breathing room to engage in the processes of boundary management that enable and constitute self-development. . . . In a world characterized by pervasive social shaping of subjectivity, privacy fosters (partial) self-determination. It enables individuals both to maintain relational ties and to develop critical perspectives on the world around them.”).