POLICING CHILDREN'S DATA

NILA BALA*

ABSTRACT

In recent years, advances in policing technology have dramatically expanded law enforcement's ability to access data. This includes children's data—their photographs, text messages, geolocation data, health information, and online search histories—revealing intimate details of a child's life. While scholars have examined law enforcement's access to data generally, this Article offers the first comprehensive analysis of children's digital evidence—how it is produced, how it is obtained by law enforcement, and how parents are a part of these processes. And it reveals a striking challenge to the conventional wisdom: We often think of parents as a source of protection against government overreach. Instead, parents are the primary agents in consenting to data exposure.

This Article makes three primary contributions. First, it maps the direct and indirect routes law enforcement use to obtain children's data, revealing parents as an unexpected source of evidence. Second, it connects two previously siloed areas, Fourth Amendment doctrine and family law jurisprudence, to show that parents' broad authority in this area is a relic—and an error. Parents' authority stems from outdated notions of child coverture—the legal fiction that children are fully represented by their parents with complete unity of interest. Coverture helps explain current Fourth Amendment doctrine which allows parents to consent to searches over their child's objections, thus eroding children's intimate privacy. Finally, this Article proposes reconceptualizing children's digital information as more akin to their bodies or DNA—intimate and deserving of robust protection—and thus, also exempt from parental consent as a route to search. To adequately protect children's data, this Article also calls for legislative reforms moving away from reliance on parental protection and toward truly regarding children's independent interests in their data.

* Thank you to Jonathan Abel, Anna Arons, Nadia Banteka, Bennett Capers, Danielle Citron, Brenda Dvoskin, Jessica Eaglin, Barbara Fedders, Kellen Funk, Daniel Harawa, Esther Hong, David Horton, Alma Magana, Evelyn Malave, Jamelia Morgan, Nathaniel Mensah, Eve Primus, Emily Suski, and Aaron Tang. Thank you for the wonderful feedback received at the Decarceration Workshop, Crimfest, Privacy Law Scholars Conference, SW Criminal Legal Conference, AALS Crim Pro and Law & Technology WIPs, and the Olivas Institute, all of which made this piece stronger. I am so grateful to all my research assistants who contributed to this work: Noreen Auyoung, Simone Montgomery, Rebecca Nathan, Sinporion Phuong, Madeline Reed, and Seton Talty. Special thanks to Kamran King. Most of all, thank you to my children and all the children I have had the privilege of serving.

TABLE OF CONTENTS

INTRODUCTION

Jane's dad finds nude pictures of Jane on her phone. She has taken these pictures herself. Jane is only ten years old. Her father is concerned the pictures have been solicited or sent to others and goes to the police for help. The police ask Jane if they can seize the device. Should Jane be able to consent? What if the police ask her dad? What if Jane and her dad disagree?[1]

1. Keenan Willard, *Nash County Father Goes to Police for Help, Then They Charged His 10-year-old Daughter for Having Nude Photos of Herself on Phone*, WRAL NEWS (Sept. 2, 2023, 8:55 AM), https://www.wral.com/story/nash-county-father-goes-to-police-for-help-then-police-charged-his-

This example is based on an actual case, where the situation quickly spun out of control. Jane's father consented to the police search of Jane's phone, and his daughter was charged with a felony: second-degree exploitation of a minor, based on intimate photos she had taken of herself.[2] Jane's story exposes a critical paradox: Parental consent, ostensibly meant to protect children, can instead facilitate a child's criminalization.

Jane is not alone.[3] Increasingly, parents are creators, contributors, and consenters to their children's data, and they play a foundational role in generating the information collected about their children. This wealth of data—including location information, photographs, videos, search histories, and health and biometric data—can be highly attractive to law enforcement officers seeking information about a child.[4] In some instances, such as in Jane's case, direct parental consent to law enforcement facilitates the turnover. However, law enforcement can also obtain children's information from schools, third parties, and data brokers, often because a parent has technically consented to the initial data creation and collection.

Law enforcement seeks digital evidence—both from children and adults—because it plays an increasing role in prosecutions.[5] Children's devices include smartphones, tablets, computers, smart watches, and the "Internet of Things" (IoT) devices (physical smart objects, including toys, that can exchange data online).[6] Children use these devices at home and at school, where children must use platforms that constantly track their activity.[7] Law enforcement may be particularly interested in searching cell phones. Smartphones are mobile and accessed by ninety-five percent of

10-year-old-daughter-for-having-nude-photos-of-herself-on-pho/21027714/ [https://perma.cc/22XB-45WQ].

2. *Id.*

3. *See* Melissa Santos, *In Washington, Teen Sexting is a Felony — But That Could Change*, CASCADE PBS (Mar. 5, 2019), https://www.cascadepbs.org/politics/2019/03/washington-teen-sexting-felony-could-change [https://perma.cc/3WTX-TVAL] (telling the story of Nicole, who was arrested for receiving nude photos sent to her from another student, that she did not open).

4. For example, both parents and law enforcement might find specific location tracking to be insightful. *Over Four in Five Parents Cite Safety and Peace of Mind as the Top Reasons for Parents Allowing Children to Have Cell Phones*, IPSOS (Aug. 17, 2010), https://www.ipsos.com/en-us/over-four-five-parents-cite-safety-and-peace-mind-top-reasons-parents-allowing-children-have-cell [https://perma.cc/79YW-DHTE].

5. NAT'L POLICE CHIEFS COUNCIL, DIGITAL FORENSIC SCIENCE STRATEGY 5 (2020), https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/2020/national-digital-forensic-science-strategy.pdf [https://perma.cc/9XPZ-BDNB] ("Over 90% of all crime is recognised as having a digital element.").

6. *What is Digital Device?*, IGI GLOB. (Apr. 2022), https://www.igi-global.com/dictionary/digital-device/76206 [https://perma.cc/RL92-VYJX].

7. Danielle Keats Citron, Essay, *The Surveilled Student*, 76 STAN. L. REV. 1439, 1443–44 (2024).

teens.[8] Additionally, many cell phone apps market tracking technologies to parents as a means of ensuring their children's safety. For example, the rise of "Parental Control Apps" allows parents to monitor their children's use of devices.[9] These apps generate digital evidence that is useful to law enforcement.

To take this wealth of data from children, law enforcement agencies commonly rely on parental consent. This practice stems from two factors: parents frequently generate data about their children, and they typically have common authority over the devices containing this data.[10] This means that parents can exercise that authority and consent to law enforcement searches of children's devices even over the child's refusal.[11] The rules for children stand in stark contrast to those governing adults who share property: When adult co-occupants disagree about consenting to a search, the government must respect an objecting adult's refusal.[12] But a parent can override a child's objection to the search. This stems from the Supreme Court's dicta in *Georgia v. Randolph* regarding searches of a child's room.[13] Courts have since extended this principle to apply to cell phone searches, despite the many dissimilarities between a child's room and a child's cell phone.[14]

I argue that this extension is misguided. Even if the parent formally owns the device—the physical container of the phone—the insides of the device may contain the child's innermost thoughts and communications. It may contain the child's therapist, period tracker, wallet, and medication management. The cell phone is the closest thing to externalizing the child's inner world, their mind itself.[15] Cell phones contain intimate and profound information, more akin to the child's body, or the child's DNA.[16]

8. MONICA ANDERSON, MICHELLE FAVERIO & EUGENIE PARK, PEW RSCH. CTR., HOW TEENS AND PARENTS APPROACH SCREEN TIME (2024), https://www.pewresearch.org/internet/2024/03/11/how-teens-and-parents-approach-screen-time/ [https://perma.cc/9WSZ-3YAC] ("Fully 95% of teens have access to a smartphone.").

9. *See Top 10 Best Parental Control Apps (2025)*, FAMILYONLINESAFETY.COM (Aug. 2025), https://www.familyonlinesafety.com/best-paretnal-control-apps [https://perma.cc/Z5W2-HBEW] (listing products such as Aura, Qustodio, bark, and Net Nanny); *see, e.g.*, LIFE360, https://www.life360.com/ [https://perma.cc/XX96-R2B6].

10. *See infra* Section II.A.

11. *See* Georgia v. Randolph, 547 U.S. 103, 114 (2006).

12. *Id.* at 121–22.

13. *Id.* at 112.

14. *See, e.g.*, *infra* notes 93–101 and accompanying text.

15. This idea of technology as creating the self will be explored more below, but other scholars have also engaged in similar ideas. *See, e.g.*, Maria Bakardjieva & Georgia Gaden, *Web 2.0 Technologies of the Self*, 25 PHIL. TECH. 399, 400 (2012) (examining blogs and social networking sites as examples of Foucault's "technology of the self," as a practice of care for the self); CASS R. SUNSTEIN, #REPUBLIC: DIVIDED DEMOCRACY IN THE AGE OF SOCIAL MEDIA (2017).

16. *See infra* Section III.A.

Significantly, under Fourth Amendment doctrine, parental consent alone is insufficient to permit a search of the child's body and DNA, unlike the child's possessions.[17] Just as the parent does not have absolute authority over the child's body, a child's mind too, personified in their cell phone data, should be beyond parental consent for law enforcement access.

Criminal law scholars have long argued that voluntary consent to law enforcement is largely a legal fiction.[18] For children, the problem of voluntary consent is even more obvious.[19] This Article pushes this critique further: If we acknowledge that children's consent is problematic in the context of law enforcement, why do we automatically vest this power in their parents? This Article examines this transfer of authority at a crucial moment: As courts and scholars increasingly scrutinize parental control in contexts like abortion and gender-affirming care, the implications of parental consent for children's data remain unexplored in the scholarly literature.[20] This Article analyzes how this parental power, exercised in the context of digital searches by police, can permanently compromise children's privacy and autonomy, often leading to their increased criminalization. In doing so, this Article makes three primary contributions, which are explored across its three parts.

Part I of the Article bridges traditionally distinct areas of law: family law and Fourth Amendment doctrine. The Article demonstrates that the intersection of these fields has expanded the reach of parental control—and shows how established principles in both domains are poor fits for the modern problem of digital evidence. Using the lens of digital searches, this Article reveals that certain Fourth Amendment doctrines concerning parents and children reflect an outdated coverture-style understanding of the parent-

17. *See infra* notes 305–07 and accompanying text.

18. *See, e.g.*, Roseanna Sommers & Vanessa K. Bohns, *The Voluntariness of Voluntary Consent: Consent Searches and the Psychology of Compliance*, 128 YALE L.J. 1962, 2009–10 (2019); I. Bennett Capers, Essay, *Criminal Procedure and the Good Citizen*, 118 COLUM. L. REV. 653, 655 (2018); Ric Simmons, *Not "Voluntary" but Still Reasonable: A New Paradigm for Understanding the Consent Searches Doctrine*, 80 IND. L.J. 773, 779 (2005); Marcy Strauss, *Reconstructing Consent*, 92 J. CRIM. L. & CRIMINOLOGY 211, 236 (2001).

19. *See, e.g.,* Megan Annitto, *Consent Searches of Minors*, 38 N.Y.U. REV. L. & SOC. CHANGE 1 (2014). Much of the literature has analyzed the analogue to juveniles' consent under the Fourth Amendment: juveniles' ability to make voluntary, knowing, and intelligent waivers of their *Miranda* rights. *See infra* Section I.C.1.

20. *See, e.g.*, Naomi Cahn, *The Political Language of Parental Rights: Abortion, Gender-Affirming Care, and Critical Race Theory*, 53 SETON HALL L. REV. 1443 (2023). For scholarship adjacent to the question I am exploring, see Zahra Takhshid, *Children's Digital Privacy and the Case Against Parental Consent*, 101 TEX. L. REV. 1417 (2023*)* (arguing against parental consent for commercial use of children's data—but not considering the law enforcement context, or parents as creators of data) and Stacey Steinberg, *The Myth of Children's Online Privacy Protection*, 77 SMU L. REV. 441 (2024) (discussing the inadequacy of current privacy protections, but not criminal legal impacts, or parental participation).

child relationship, with parents possessing an almost absolute authority to make decisions on behalf of children.

In practice, the presence of a parent is unlikely to safeguard children's interests and may actually leave them more vulnerable—a pattern that is evident in the analogous Fifth Amendment context. Research on *Miranda* waivers reveals that parents, positioned as "interested adults," frequently encourage children to waive their rights rather than protect them. This parallel exposes a problem that exists in the Fourth Amendment context as well: Parents have complicated, often conflicting interests, and, particularly in the digital evidence space, are ill-equipped to prevent law enforcement encroachment.

Part II provides a descriptive account of children's digital evidence—how it is produced, how it is obtained by law enforcement, and how parents are a part of these processes. The Article provides a taxonomy of the various methods for how police obtain children's data, including direct and indirect routes to get this data. To do so, it relies on the results of an original survey of law enforcement departments. This survey reveals a striking absence of policies governing consensual digital searches of children.

Beyond direct consent, the Article reveals how law enforcement exploits indirect methods to access children's data, repurposing consent given for other purposes—typically to commercial entities or schools. Parents emerge as both consent providers and data creators in this ecosystem, as notions of "good" parenting have become increasingly intertwined with child surveillance. The harms of this data being turned over to police are significant, and include the increased criminalization of children.

Part III takes up reforms that could address the limitations of Fourth Amendment doctrine and family law. This Article proposes advocacy strategies to contest a *child's consent* to searches, drawing on the more rigorous voluntariness analysis emerging under the Fifth Amendment. It also offers a framework for challenging *parental consent* to search a child's digital devices, building on *Riley v. California,* as well as case law considering the child's body and DNA.[21] This analysis extends arguments I have previously advanced regarding the complex ownership questions surrounding children's genetic material.[22]

Alongside these doctrinal interventions, the Article outlines legislative reforms to severely limit consensual digital searches of children and better regulate children's data. Recognizing that we are asking too much of parents as "interested adults" in this context, I call for providing children with an

21. 573 U.S. 373 (2014); *see infra* notes 305–07.
22. *See* Nila Bala, *Who Owns Children's DNA?*, 122 MICH. L. REV. 457 (2023).

attorney consultation before a consent search of their device. Rather than directly regulate the parent-child relationship, the legislative strategies proposed aim to minimize data collection, sharing, and retention.

I. CHILDREN, CONSENT, AND THE FOURTH AMENDMENT

This Part aims to address two key issues: first, how child coverture has shaped Fourth Amendment doctrine around searches of the child, and second, the pitfalls of relying on either the child or parent's consent.

A. Why We Let Parents Consent

Parental authority over children, including the ability to make decisions on their behalf, is firmly established in history. Starting in the early twentieth century, the Supreme Court identified a parent's fundamental right to make decisions regarding the "care, custody, and control of their children."[23] In *Meyer v. Nebraska*, and two years later in *Pierce v. Society of Sisters*, the Court held that educational regulations infringed upon parental authority.[24] Later cases, like *Wisconsin v. Yoder*, again ratified the parents' right to control their child's education, this time in the context of Amish schooling.[25] Finally, the Court's most recent pronouncement on this issue occurred in *Troxel v. Granville*, where it reaffirmed the primacy of parental discretion to determine their child's best interests, including the right to control visitation by others.[26] Even as the Supreme Court has grown increasingly skeptical of unenumerated constitutional rights, it continues to treat parental rights as sacrosanct.[27]

Parents are unique as private actors in the power they hold over another person. Parents can control their child's speech, access to other individuals, the ability to practice a religion. They can deprive them of any money earned.[28] Parents can control a child's ability to access ideas, books, and resources. We allow parents to engage in corporal punishment, something we do not even allow the state to do to prisoners. To add to this list of near-absolute authority over children, modern parents have a new power at their

23. Troxel v. Granville, 530 U.S. 57, 66 (2000); *see also* Meyer v. Nebraska, 262 U.S. 390 (1923); Pierce v. Soc'y of Sisters, 268 U.S. 510 (1925); Wisconsin v. Yoder, 406 U.S. 205 (1972).
24. *Meyer*, 262 U.S. at 401; *Pierce*, 268 U.S. at 534–35.
25. *Yoder*, 406 U.S. at 213–15.
26. *Troxel*, 530 U.S. at 68–69.
27. *See* Dobbs v. Jackson Women's Health Org., 597 U.S. 215, 256 (2022).
28. Anne C. Dailey, *In Loco Reipublicae*, 133 YALE L.J. 419, 422–23 (2023).

disposal—the ability to track their children, create a data record, and turn this information over to the government.[29]

Still, parental authority is not without limits. As noted above, the State will intervene where there are allegations of abuse or neglect, conflicts in the home, and/or a great risk to the child.[30] In *Prince v. Massachusetts*, the Court upheld a child labor restriction as reasonable, even when it conflicted with a parent's decision to have her child distribute religious literature.[31] Similarly, in *Parham v. J.R.*, the Court imposed limitations on parents' unfettered discretion to place their children in mental institutions but was unwilling to require any additional process when a child disagreed with a parent's decision.[32]

Many of these cases do not directly address situations where a child explicitly disagreed with parental decisions. The voice of the child was silent in *Meyer* and *Pierce*; it was presumably assumed that parent and child shared the same desire to choose a different educational plan.[33] We hear the faintest glimmer of Frieda Yoder's voice, that she does not want to attend high school, in agreement with her parents and the Amish community's position.[34] But the dissent rightly points out that we do not know what the other two Amish children, Vernon and Barbara, wanted for themselves.[35] The Court qualified its decision, stating that it was not "determin[ing] the proper resolution of competing interests" among the state, parents, and children. *Parham*, which seemingly approached a disagreement between parent and child, was actually initiated because state experts believed institutional care was unnecessary for the children involved.[36] The court made clear that it would not require any additional process just because a child disagreed with a parent's decision.[37] Tragically, one of the children in

29. *See* Danielle Keats Citron & Ari Ezra Waldman, *Rethinking Youth Privacy*, 111 VA. L. REV. (forthcoming 2025).

30. Kristin Henning, *The Fourth Amendment Rights of Children at Home: When Parental Authority Goes Too Far*, 53 WM. & MARY L. REV. 55, 79 (2011).

31. 321 U.S. 158, 170 (1944).

32. 442 U.S. 584, 603 (1979).

33. *See* Pierce v. Soc'y of Sisters, 268 U.S. 510, 534–36 (1925); Meyer v. Nebraska, 262 U.S. 390, 400–01 (1923).

34. Wisconsin v. Yoder, 406 U.S. 205, 243 (1972).

35. *Id.*

36. Interview by Clifford M. Kuhn with John L. Cromartie, Attorney, Georgia Legal Services Program (Sept. 18, 2002), https://digitalcollections.library.gsu.edu/digital/api/collection/ggdp/id/5504/download [https://perma.cc/X5ZA-E5X7] (interview with attorney representing J.L. and J.R. in the *Parham* case).

37. *Parham,* 442 U.S. at 598–617. A tragic footnote in the decision states that pending review, J.L. died. *Id.* at 587 n.1. After the Supreme Court decision came down, efforts were made to place Joey (J.L). When he was placed back with his father, he committed suicide. Roy B. Lacoursiere, *A Footnote to* Parham*: Was J.L. a Casualty of the Mental Health Bar?*, 11 BULL. AM. ACAD. PSYCHIATRY L. 279, 279–82 (1983) (wondering if the bar "made law" by inappropriately pushing for Joey's release).

Parham, J.L., actually committed suicide after being released from the institution.

The abortion context represents the Court's most direct engagement with parent-child conflicts, establishing that parents cannot exercise an absolute veto over their child's decision to have an abortion.[38] But outside of the realm of reproductive care, legislators and courts have mostly sidestepped challenging the assumption of a unified parent-child relationship.[39] Even in restricting parental authority over abortion, the Court was driven less by children's rights and more by pragmatism—recognizing that parental authority could do little in a situation where the family was already so fractured.[40]

While the Court at least acknowledged the possibility of parent-child conflicts in the abortion context, its Fourth Amendment jurisprudence reveals an even deeper commitment to preserving traditional familial hierarchies. In *Georgia v. Randolph*, the Court considered a wife's consent to a warrantless search of her home when her husband was physically present and objected.[41] It held that the police could not reasonably rely on this consent given the dynamics of co-occupancy, with a search over the objection of one co-occupant considered presumptively unreasonable.[42]

However, the Court suggested it would not extend the rule in *Randolph* when the co-occupants were parent and child in the home.[43] Because of the "recognized hierarchy" of superior and inferior between a parent and child, a parent can consent to a search of the child's room, even over the child's objection, and regardless of the child's maturity.[44] Thus, even when the child objects to a search over their most private space—their bedroom—parental consent takes precedence over their wishes.[45] Courts have followed *Randolph's* dicta, utilizing language of parental "dominance" and "authority" to justify searches over the child's objection.[46]

---

38. But even within the abortion jurisprudence pre-*Dobbs*, the Court did not so much as elevate children's rights over parental authority but throw their hands up. *See* Planned Parenthood of Cent. Mo. v. Danforth, 428 U.S. 52, 75 (1976).

39. Anne C. Dailey & Laura A. Rosenbury, *The New Parental Rights*, 71 DUKE L.J. 75, 139 (2021).

40. *Planned Parenthood of Cent. Mo.*, 428 U.S. at 75.

41. 547 U.S. 103, 107 (2006).

42. *Id.* at 106.

43. *Id.* at 114.

44. *Id.* at 104.

45. *See id.*

46. *In re* A.S., 443 P.3d 618, 622 (Or. Ct. App. 2019) (grandmother had authority to consent to search despite youth's objection); State v. S.B., 758 So. 2d 1253, 1255 (Fla. Dist. Ct. App. 2000) (father's consent to search overrode juvenile's objection to search); *see also* RESTATEMENT OF CHILDREN AND THE LAW § 12.11 (AM. L. INST., Tentative Draft No. 3, 2021) (objection by a minor to

This language emphasizing parental control reflects the historical treatment of children as a parent's property throughout much of Western history.[47] Courts have also invoked notions of possession and ownership of children in family law decisions.[48] Early Supreme Court decisions—*Meyer v. Nebraska* and *Pierce v. Society of Sisters*—ostensibly concerning parental choice in schooling, may have actually been motivated by the parent's "confiscated property" interest in their child.[49] These early cases paradoxically framed the right of parental control as "liberty."[50] Walter Pierce, the appellant in *Pierce*, astutely noted that "it is a strange perversion of the word 'liberty' to apply it to a right to control the conduct of others."[51] But liberty makes sense as a frame if children are considered patriarchal property.[52]

A husband's control and property interest over his wife, known as the doctrine of marital coverture, has largely ended.[53] But child coverture persists, with vestiges we can see throughout the law.[54] The concept of child coverture dates back to Greek, Roman, and Judeo-Christian traditions.[55] Male dominance over women, slaves, and children was seen as natural and correct, drawing justification from scripture.[56] The notion of children as chattel carried over and became ingrained in American jurisprudence, with parental rights mirroring the bundle of rights associated with property ownership. This property-like conception of children was particularly

---

parental consent to search will not render the consent invalid). On language, see United States v. Di Prima, 472 F.2d 550, 551 (1st Cir. 1973) ("[E]ven if a minor child, living in the bosom of a family, may think of a room as 'his,' the overall dominance will be in his parents."); State v. Wagster, 361 So. 2d 849, 855 (La. 1978) ("[E]xcept in unusual circumstances, the parent possesses at least common authority, if not the principle authority, over the residence . . . .").

47. Barbara Bennett Woodhouse, *"Who Owns the Child?":* Meyer *and* Pierce *and the Child as Property*, 33 WM. & MARY L. REV. 995, 997 (1992) ("*Meyer* and *Pierce* constitutionalized a narrow, tradition-bound vision of the child as essentially private property. This vision continues to distort our family law and national family policy . . . .").

48. *Id.*; *see also* Kevin Noble Maillard, *Rethinking Children as Property: The Transitive Family*, 32 CARDOZO L. REV. 225 (2010).

49. Woodhouse, *supra* note 47, at 1105 (citing Editorial, *School, Church and State*, NEW REPUBLIC, June 24, 1925, at 114).

50. As Woodhouse writes, the Court's decision was ironic, as the Fourteenth Amendment was explicitly ratified to secure liberty for formerly enslaved individuals. *See* Woodhouse, *supra* note 47, at 1042 n.207; *see also* U.S. CONST. amend. XIV, § 1; *Developments in the Law: The Constitution and the Family*, 93 HARV. L. REV. 1156, 1353 (1980) (writing that liberty as control of another is an unusual oxymoron).

51. Woodhouse, *supra* note 47, at 1042 (quoting Supplement to the Brief of Appellant, the Governor of the State of Oregon, at 8; Pierce v. Soc'y of Sisters, 268 U.S. 510 (1925) (No. 584)).

52. *See id.* at 1042.

53. *See* Dailey & Rosenbury, *supra* note 39, at 78.

54. *Id.* at 84.

55. *See* Woodhouse, *supra* note 47, at 1043–44.

56. *Id.* at 1043.

pronounced in Colonial and nineteenth-century America.[57] Early judicial opinions spoke of custody using the language of property; a father could "assign[] and transfer[]" rights to a child; the mother, on the other hand, "was not vested with the testamentary disposition of the child."[58] Performing medical care on the child without the father's consent was wrong "as the father is the natural guardian of the child and is *entitled to his custody and his services*, he cannot be deprived of them without his consent."[59]

The legacy of child coverture persists in modern law, though its justifications have evolved much like those for married women's coverture. While the law gradually recognized married women as independent legal entities, the evolution of children's rights has proven more complex.[60] Modern courts no longer explicitly frame children as parental property, instead grounding parental consent in children's developmental limitations. Because children lack maturity to make important decisions, the doctrine positions parents as the natural protectors of their interests. Yet this shift in rationale—from property rights to protective capacity—has largely preserved coverture-era rules under new justifications.

If protecting children due to their dependency truly drove this framework, we might expect parents to be positioned more like fiduciaries, with special duties of loyalty and diligence toward their children, and recognition that children might have conflicting interests.[61] But our legal system has not adopted this approach. Instead, it continues to treat parent and child as a single legal entity, focusing almost exclusively on protecting against third-party intrusions rather than considering potential conflicts between parent and child. [62] The law's failure to account for the distinct interests of parents and children is particularly striking in the Fourth Amendment context, an area that remains underexplored in legal scholarship. Given that children rarely have exclusive ownership over anything, parental consent, through common authority, can cover almost anything a child possesses, including cell phones.[63] Contemporary notions

57. *Id.* at 1045.

58. Lee v. Lee, 65 So. 585, 585 (Fla. 1914); Harper v. Tipple, 184 P. 1005, 1007 (Ariz. 1919).

59. *See, e.g.*, Bakker v. Welsh, 108 N.W. 94, 95 (Mich. 1906) (emphasis added).

60. Dailey & Rosenbury, *supra* note 39, at 90–92.

61. Elizabeth S. Scott & Robert E. Scott, *Parents as Fiduciaries*, 81 VA. L. REV. 2401, 2404 (1995).

62. Dailey & Rosenbury, *supra* note 39, at 78.

63. If children are conceptualized as property, it would also not make sense to talk about them as being able to possess property. But apart from that, the law also imagines children as having no property.

of "good" parenting, emphasizing parental oversight and access to children's belongings, further reinforce this legal approach.[64]

Courts have recognized one notable limit to parental authority: when searches involve a child's body or DNA, acknowledging that parents and children may have distinct interests in these intimate Fourth Amendment contexts. While case law is limited, courts that have considered the issue have held that parents cannot unilaterally consent to searches of a child's person.[65] This aligns with a larger recognition, starting in *In re Gault,* that children involved in the criminal/juvenile system have rights too vital to be left to parents' unilateral control.[66] The Court held that juveniles accused of crimes in delinquency proceedings must be afforded many of the same due process rights as adults, including the right to counsel.[67] Legal representation for children post-*Gault* has been interpreted to mean counsel acts based on the child's direction and interests, even when it is against a parent's desires.[68] In addition, key decisions such as going to trial or taking a plea, testifying at trial, agreeing to probation conditions, and appealing are the child's choice. While children almost always seek guidance from their parents when available, there is a broad consensus that the child has ultimate decision-making authority.[69] This principle of children's autonomy during trial, however, stands in stark contrast to the treatment of children's interests in Fourth Amendment cases.

In many domains, the most protective thing we can do for children is to strengthen parental rights. This is why many scholars, particularly those writing in the family regulation space as well as the Restatement of Children and the Law, strongly endorse parent's rights.[70] Strong parental rights prevent outside intervention into the home, where a state actor, who barely knows the child, is tasked with determining what is best for the child.[71]

64. *See infra* note 246 and accompanying text.

65. *In re* H.K.D.S., 469 P.3d 770, 771 (Or. Ct. App. 2020) (holding parental consent with child acquiescence does not amount to voluntary consent); *see also* RESTATEMENT OF CHILDREN AND THE LAW § 12.11 (AM. L. INST., Tentative Draft No. 3, 2021). *But see* People v. K.N., 87 N.Y.S.3d 862, 869 (N.Y. Crim. Ct. 2018) (holding a request for buccal saliva swab must be in presence of parent, guardian, attorney in an age appropriate setting). The legal analysis also shifts based on the child's position—courts are more likely to validate parental consent when the child is a suspected victim rather than the target of a criminal investigation.

66. *In re* Gault, 387 U.S. 1, 13 (1967) *see also* Margareth Etienne, *Managing Parents: Navigating Parental Rights in Juvenile Cases*, 50 CONN. L. REV. 61, 68 (2018).

67. *See Gault*, 387 U.S. at 4.

68. Kristin Henning, *It Takes a Lawyer to Raise a Child?: Allocating Responsibilities Among Parents, Children, and Lawyers in Delinquency Cases*, 6 NEV. L.J. 836, 837 (2006).

69. *Id.*

70. *See e.g.*, Clare Huntington & Elizabeth Scott, *The Enduring Importance of Parental Rights*, 90 FORDHAM L. REV. 2529 (2022); Martin Guggenheim, *The (Not So) New Law of the Child*, 127 YALE L.J.F. 942, 949 (2018).

71. Guggenheim, *supra* note 70.

Strong parental rights can thus minimize the severe and traumatic impacts of the family regulation system. However, in the realm of a child's Fourth Amendment rights, parental authority takes on a different character. When parents consent to searches, it invariably reduces a child's privacy, acting as a one-way ratchet. This stands in stark contrast to other areas of parental authority recognized by the Court, such as the education decisions in *Meyer*, *Pierce*, and *Yoder*, where parental rights can potentially expand a child's opportunities rather than restrict them.[72]

Parental consent does not provide sufficient protection for children's privacy interests, particularly in the context of digital data. Despite parental strengths in many areas, the following Section argues that while current Fourth Amendment doctrine allows for parental consent to access the child's data, we should critically examine whether such consent truly safeguards children's interests.

B. Who Can Consent

Coverture has created a legal paradigm where parents can consent to searches, and indeed, they often do.[73] This Section starts by examining the foundational principles of consent searches, then critically analyzes how courts adapt these principles—against the backdrop of parental authority—to cases involving children and parents.

The Fourth Amendment doctrine displays an inherent inconsistency and irony—children are deemed simultaneously too young to resist their parents' consent, yet old enough to directly consent to law enforcement searches. This paradox raises serious concerns about the ability of the Fourth Amendment to safeguard children's privacy rights, especially as the nature of searches has evolved dramatically in the digital age. Indeed, the inadequacies of existing constitutional doctrines become even more apparent when considering how law enforcement can indirectly access children's data through parental control apps.

Despite the imbalance of power between children and law enforcement, courts rarely find that searches of minors, based solely on the minor's consent, are involuntary.[74] Courts make a voluntariness determination by

72. Meyer v. Nebraska, 262 U.S. 390 (1923); Pierce v. Soc'y of Sisters, 268 U.S. 510 (1925); Wisconsin v. Yoder, 406 U.S. 205 (1972).

73. While there is no empirical research quantifying how often parents actually consent, there is a strong legal consensus that they often do. Hillary B. Farber, *A Parent's "Apparent" Authority: Why Intergenerational Coresidence Requires a Reassessment of Parental Consent to Search Adult Children's Bedrooms*, 21 CORNELL J.L. & PUB. POL'Y 39, 58 (2011) ("[T]he cases finding parental consent inadequate are the exception, not the rule.").

74. Annitto, *supra* note 19.

evaluating the totality of the circumstances in a case, including the subject's characteristics and circumstances of the search.[75] In reality, scholars, advocates, and community members have criticized "voluntary" consent searches as a legal fiction.[76] As Justice Thurgood Marshall explained in his dissent in *Schneckloth v. Bustamonte,* "[a]ll the police must do is conduct what will inevitably be a charade of asking for consent. If they display any firmness at all, a verbal expression of assent will undoubtedly be forthcoming."[77] Recent research validates Justice Marshall's concerns: Most individuals feel compelled to consent.[78] Minorities are asked to consent to searches more frequently than white individuals, and they often comply out of fear of retaliation.[79] Courts also fail to meaningfully consider how age and vulnerability can alter the voluntariness of consent, even though the Court has recognized children's distinct status in other contexts.[80] Despite acknowledging "kids are different" in many contexts, courts have not meaningfully done so with regard to Fourth Amendment consent searches.[81]

There are almost no surveys of case law on consensual searches of minors, aside from Megan Annitto's work a decade ago, which looked at cases where minors were directly asked for consent.[82] Courts have consistently found there is no *per se* rule barring youth consent, leaving

75. *Id.* at 11.

76. *See* Alafair S. Burke, *Consent Searches and Fourth Amendment Reasonableness*, 67 FLA. L. REV. 509, 511 & n.5 (2015) (explaining the widespread consensus that there is a disconnect between doctrine and reality).

77. Schneckloth v. Bustamonte, 412 U.S. 218, 284 (1973) (Marshall, J., dissenting).

78. *See* Roseanna Sommers, *Are Consent Searches Truly Voluntary?*, SCHOLARS STRATEGY NETWORK (May 14, 2019), https://scholars.org/contribution/are-consent-searches-truly-voluntary [https://perma.cc/J574-782G] ("[M]ore than nine in ten searches are conducted with the consent of the person being searched."); *see also* Burke, *supra* note 76, at 515; Oren Bar-Gill & Barry Friedman, *Taking Warrants Seriously*, 106 NW. U. L. REV. 1609, 1618 (2012) ("Consent is placed in scare quotes . . . because virtually no one believes these searches are the product of a voluntary choice.").

79. *See, e.g.*, Press Release, ACLU Ill., New Data Shows Racial Bias in Police Consent Searches (July 13, 2011), https://www.aclu-il.org/en/press-releases/new-data-shows-racial-bias-police-consent-searches [https://perma.cc/AP3A-QUQH] (describing a report showing that Hispanic motorists were 3.38 times more likely than Caucasian motorists to be asked for a consent search and African American motorists were nearly 3 times (2.96) more likely); MAGNUS LOFSTROM, JOSEPH HAYES, BRANDON MARTIN & DEEPAK PREMKUMAR, PUB. POL'Y INST. OF CAL., RACIAL DISPARITIES IN TRAFFIC STOPS (2022) ("Black Californians are more than twice as likely to be searched as white Californians, but searches of Black Californians are somewhat less likely to yield contraband or evidence"); Amanda Graham et al., *Race and Worrying About Police Brutality: The Hidden Injuries of Minority Status in America*, 15 VICTIMS & OFFENDERS 549, 557 (2020) (finding that Blacks are five times more likely and Latinos four times more likely to fear police brutality than whites).

80. *See also* Bryce Anderson, *The Costs of Youth: Voluntary Searches and the Law's Failure to Meaningfully Account for Age*, 62 ARIZ. L. REV. 241, 241 (2020).

81. *See id.* at 251.

82. *See* Annitto, *supra* note 19.

youth extremely vulnerable to searches.[83] In fact, the Supreme Court suggested in dicta that a child as young as eight could consent on their own to the search of the family home.[84] A survey of cases I completed, focusing on the last decade, reveals a clear trend: Courts rarely find children's consent involuntary.[85] This pattern extends across various contexts, including family homes, automobiles, backpacks, and even searches of their own persons.

The law contorts itself to justify searches of young children: "The boy obviously had more than a passing familiarity with pat-down searches."[86] The officer spoke in a calm, casual way;[87] the encounter was short;[88] the child was told they could refuse—even though such information is not required.[89] With this type of rhetoric, courts minimize the inherent coercion at play and sidestep basic protections for children. Despite the coerciveness that characterizes these encounters, several court decisions have affirmed that children can voluntarily consent to digital searches without any adult presence.[90]

---

83. *See, e.g.*, United States v. Bermel, 88 F.4th 741, 745 (8th Cir. 2023) ("The dearth of authority supporting a *per se* rule makes sense, as the Supreme Court has observed that even 'a child of eight might well be considered to have the power to consent to the police crossing the threshold into that part of the house where any caller . . . might well be admitted.'" (quoting Georgia v. Randolph, 547 U.S. 103, 112 (2006) (dictum))); People v. Rogers, 636 N.E.2d 565, 570 (Ill. App. Ct. 1992) ("There is no *per se* rule that precludes a minor child from giving consent to a search by police. . . . Age is but one factor considered by a court . . . .").

84. *Randolph*, 547 U.S. at 112 ("[A] child of eight might well be considered to have the power to consent to the police crossing the threshold into that part of the house where any caller, such as a pollster or salesman, might well be admitted.").

85. In my survey of cases, I primarily focused on those from the last ten years, as Annitto's survey covered cases prior to that.

86. F.C. v. State, 205 So. 3d 831, 833 (Fla. Dist. Ct. App. 2016) (describing how the boy was not "green" being in the district court opinion); *see also In re* L.C., No. 03-02-00070-CV, 2003 WL 21241582, at *4 (Tex. Ct. App. May 30, 2003).

87. *In re* Clinton G., 669 N.W.2d 467, 471 (Neb. Ct. App. 2003), *disapproved of on other grounds by* State v. Hammond, 996 N.W.2d 270 (Neb. 2023) (the [j]uvenile against a police cruiser"); *In re* D.S officer used a conversational tone); State v. Carlos A., 284 P.3d 384, 388 (N.M. Ct. App. 2012) ("low-key, polite encounter and cooperation"); Commonwealth v. Latimer L., 86 N.E.3d 512, (Mass. App. Ct. 2017) (lower court finding that an officer "did not act in an intimidating manner or exhibit any overt show of authority," when in fact, the detective "was pinning., 329 Or. App. 96, 99 (2023), *review denied sub nom*, State v. D.S., 544 P.3d 1000 (Or. 2024) (language and tone of the deputy's request were not coercive).

88. *In re* Victor B., No. 2 CA-JV 2008-0073, 2009 WL 104776, at *2 (Ariz. Ct. App. Jan. 15, 2009) (encounter lasted only a couple of minutes); *In re* Lester, No. CA2003–04–050, 2004 WL 549815, at *4 (Ohio Ct. App. Mar. 22, 2004) (stop was not unusually long); *Carlos A.*, 284 P.3d at 388 (encounter lasted about ten minutes).

89. *Lester*, 2004 WL 549815, at *4 (consent form signed said he has "the right to refuse this search"); State v. C.S., 632 So. 2d 675, 675 (Fla. Dist. Ct. App. 1994) (officer advised C.S. he was free to refuse consent or to stop the search).

90. *In re* M.S., No. G049693, 2014 WL 6425943, at *1 (Cal. Ct. App. Nov. 17, 2014) (police obtained minor's consent to search his cell phone text history); People v. Patterson, No. D077938, 2021

But much of the time, law enforcement officers do turn to parents. This may be because (1) state/local policies recommend or require parent involvement, (2) parents are present when police make decisions to search, and/or (3) parents own the devices, and therefore, are seen as having authority over the child's device based on the Court's dicta in *Georgia v. Randolph*.[91]

Randolph has significantly influenced lower courts considering the Fourth Amendment rights of minor children. Over a decade ago, Professor Kris Henning predicted that *Randolph*'s dicta would have broad implications "for the validity of third-party consent in a variety of parent-child scenarios, including parental consent to a police search of computer files, social networking sites, e-mail exchanges, Internet searches, and closed containers or locked spaces belonging to the minor."[92]

This prediction has proven accurate, particularly regarding cell phones. Courts have consistently ruled that a parent with common authority over a phone—either through ownership or access—can consent to its search.[93] This doctrine originates from *United States v. Matlock*, where the Supreme Court established that common authority over a property interest can provide valid consent for a search.[94] The Court defined common authority as:

> [M]utual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.[95]

WL 4314372, at *6 (Cal. Ct. App. Sept. 23, 2021) (16 year old can consent to search of her pimp's phone); United States v. Alexander, No. 17-CR-0072, 2019 WL 2016856, at *4 (D. Nev. May 7, 2019) (minor victim can consent to search of phone, adult cannot vitiate valid consent); *In re* M.S., 244 Cal. Rptr. 3d 580, 589 (Cal. Ct. App. 2019), *as modified on denial of reh'g* (Apr. 3, 2019) (15 year old in hospital can consent to search of her phone); State v. J.L.S., 343 P.3d 670, 673 (Or. Ct. App. 2015) (obtained youth's consent to search two cell phones); United States v. Gardner, 887 F.3d 780, 784 (6th Cir. 2018) (discussing in dicta that a minor who used cell phone to communicate with undercover police officer, had it in her possession during police sting, knew the passcode, and gave it to officers had apparent authority to consent to search); *In re* B.R., 24 Pa. D. & C.5th 563, 567 (2011) (juvenile consented to an examination of his cell phone, had mother sign a consent-to-search form after searching phone).

91. Georgia v. Randolph, 547 U.S. 103, 114 (2006); *see also* Henning, *supra* note 30, at 58.

92. *See* Henning, *supra* note 30, at 55–56.

93. *See infra* notes 95, 99, and 102.

94. United States v. Matlock, 415 U.S. 164, 171 (1974).

95. *Id.* at 171 n.7.

Lower courts have combined the *Matlock* doctrine with *Randolph*'s dicta to justify parental consent as sufficient for accessing a child's data, effectively extending the concept of "common areas" to digital spaces.[96]

A trilogy of recent cases reveals a similar theme: parental consent is seen as sufficient to search children's devices. For example, in *Campos v. State*, police officers asked a fifteen-year-old's parents for consent to look in his two cell phones.[97] The court found that his parents had actual authority over the phones: They paid the bills and owned the phones, and the phones were registered under their names.[98] There was no passcode on one phone, and the other had a passcode the father knew.[99] The court also noted that even without actual authority, apparent authority would suffice if officers reasonably believed the parents had the right to consent.[100]

Similarly, in *In re T.R.,* sixteen-year-old T.R. was arrested for cyberbullying after his mother signed a consent form, allowing law enforcement to search T.R.'s phone. The search provided the key evidence for her son's arrest and prosecution.[101] The court pointed to the mother being "fully aware of the circumstances surrounding the search of the phone."[102] They further emphasized that she signed a broad consent form that stated the phone "will be searched for data and information which may include photos and videos" and had written her son's passcode on the form.[103]

Finally, *In re J.P.* exemplifies the complexities surrounding parental consent: Parents are often pressured by police and, in turn, apply pressure on their child to consent to a search the child wants to refuse.[104] J.P. was accused of making bomb threats at school.[105] The officers took J.P. to the station without informing his mother, where he refused a search of his cellphone.[106] Upon learning how law enforcement handled the situation, J.P.'s mother felt her son had been unfairly treated and asked for the phone back, stating it was hers. [107] The police told her they were going to get a search warrant, so to have her phone returned faster, she consented to a search of it. She told her son to turn over his passcode repeatedly, after

96. *See infra* notes 95, 99, and 102.
97. Campos v. State, No. 14-18-00989-CR, 2020 WL 1528122, at *6 (Tex. Crim. App. Mar. 31, 2020).
98. *Id.*
99. *Id.* at *7.
100. *Id.* at *6.
101. *In re* T.R., 2015-0902 (La. App. 1 Cir. 11/6/15), *writ denied* 2015-2232, p. 1 (La. 5/2/16), 206 So. 3d 878, 878.
102. *Id.* at p. 4.
103. *Id.* at p. 3.
104. *See In re* J.P., 2018 WI App 66, 384 Wis. 2d 415, 921 N.W.2d 529.
105. *Id.* ¶¶ 5–12.
106. *Id.* ¶¶ 13–15.
107. *Id.* ¶¶ 15–16.

which he eventually acquiesced.[108] The court found J.P.'s mother had actual and apparent authority because (1) the mother owned the phone and paid for its service and that (2) her son "failed to exercise complete dominion and control over the phone" since he turned over the passwords "without a protest" after she asked him twice.[109]

However, reliance on J.P.'s lack of protest is flawed. A child worn down by both police and his mother may not protest at all. Acquiescence, which the court relies on, is not equivalent to consent.[110] This case underscores the complex dynamics at play: a minor objecting to a search, police exerting pressure on a parent, and a parent directing their child to surrender privacy.

The situation becomes even more problematic for children who are wards of the state. For instance, in California, the iFoster Pilot program assisted in making mobile services a permanent state benefit for foster youth.[111] Depending on the placement, case workers or foster parents may require the young person to provide their passcode.[112] In such an instance, the state, with its policing power, could ask for consent. That same state could exercise an absolute veto over a child's refusal of consent to search, by acting under the doctrine of *parens patriae*, which grants the government authority to care for those unable to care for themselves.[113] The state shapeshifts effortlessly, with the same entity acting as both guardian and investigator of the child.

This direct exercise of state authority, however concerning, is at least somewhat visible. More subtle—and perhaps more pervasive—are the indirect routes through which the state can access children's digital information. This is a pathway that does not involve a child visiting the

108. *Id.* ¶¶ 32–33.

109. *Id.*

110. *See, e.g.*, *In re* H.K.D.S., 469 P.3d 770, 779 (Or. Ct. App. 2020) (rejecting a child's acquiescence to a buccal swab as sufficient consent.); State v. Johnson, 729 N.W.2d. 182, 183, 188 (Wis. 2007) ("Acquiescence to an unlawful assertion of police authority is not equivalent to consent."); Taylor v. City of Saginaw, 620 F. Supp. 3d 655 (E.D. Mich. 2022); Ferrara v. State, 319 So. 2d 629, 632 (Fla. Dist. Ct. App. 1975) ("[A]cquiescence is not equivalent to consent.").

111. Press Release, iFoster, iFoster Distributes Phones to Foster Youth (Aug. 15, 2021), https://www.ifoster.org/blogs/ifoster-distrubutes-fisrt-round-of-phones/ [https://perma.cc/UQ9Z-9EZ7]. However, a recent vote will cut access for former foster youth. Jeremy Loudenback, *California Former Foster Youth Will Lose Access to Free Cell Phones*, IMPRINT (May 10, 2024, 4:17 PM), https://imprintnews.org/top-stories/california-former-foster-youth-will-lose-access-to-free-cell-phones/249380 [https://perma.cc/SAD7-HYCY].

112. For example, in New York, there may be a number of sources to cover the costs of cell phones, including foster parents and state funding through the "Chafee fund." N.Y. OFF. OF CHILD. & FAM. SERVS, STRATEGIC PLAN. AND POL'Y DEV., INFORMATIONAL LETTER (2019), https://ocfs.ny.gov/main/policies/external/ocfs_2019/INF/19-OCFS-INF-04.pdf [https://perma.cc/C7G5-WJDN].

113. The doctrine of *parens patriae* ("parent of the nation") is a legal principle allowing the government to act as guardian for individuals who cannot care for themselves, such as children. David L. Myers, *Parens Patriae*, EBSCO (2024), https://www.ebsco.com/research-starters/law/parens-patriae [https://perma.cc/NE35-NUSF].

station house, or a parent talking directly to law enforcement. Instead, police can take advantage of the large and robust market of "parent-controlled" phones, "parental control" apps, and "kid-safe" phones specifically marketed toward parents of minors.[114] These apps allow parents to monitor children's activities, and "provide parents with fine-grained reports about children's usage of the phone, their social interactions, and their physical location."[115] When parents deploy these apps, they inadvertently create another conduit for law enforcement access: The data flows not just to parents but to third-party companies, making it accessible to law enforcement.[116]

In *Carpenter v. United States*, the Supreme Court grappled with the continued viability of the third-party doctrine, which traditionally held that individuals have no reasonable expectation of privacy in information shared with third parties.[117] The Court reconsidered this doctrine's application in the digital age and held that accessing a week's worth of cell location data requires a warrant, even though individuals shared this information with service providers who are third parties.[118] This decision recognized that people still have a "reasonable expectation of privacy" in certain types of digital information despite sharing it with a third party.[119] The *Carpenter* Court relied on two key factors: that the state's intrusion involved a large amount of private data and that society essentially requires us to have phones (in a way paralleling parents' requirements for children to have phones for safety and tracking purposes).[120]

Despite a seemingly broad decision, the Court emphasized the *Carpenter* ruling was narrow.[121] Agencies and lower courts have followed suit in interpreting *Carpenter*.[122] Policing agencies still justify acquisition of data

114. *See*, *e.g.*, *#1 Parental Control & Monitoring App*, BARK, https://www.bark.us/learn/ps-spy-app [https://perma.cc/BG2K-ZCDZ] (describing itself as the "#1 Parent Controlled Phone, with location tracking, text and app monitoring & more tamper-proof parental controls").

115. Álvaro Feal, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso & Alessandra Gorla, *Angel or Devil? A Privacy Study of Mobile Parental Control Apps*, 2 PROC. ON PRIV. ENHANCING TECHS. 314, 314 (2020).

116. In addition, seventy-two percent of these apps share the data even beyond the application to online advertising and analytical services. *Id*.

117. 585 U.S. 296, 313–16 (2018).

118. *Id.*

119. *Id.* at 314–16.

120. *Id.* at 311 (calling cellphones almost a "feature of human anatomy").

121. *Id.* at 316 ("Our decision is a narrow one. We do not express a view on matters not before us . . . .")

122. *See*, *e.g.*, United States v. Tuggle, 4 F.4th 505, 526 (7th Cir. 2021) (holding the warrantless use of pole cameras to continuously surveil a suspect for eighteen months did not constitute a Fourth Amendment search); Matthew Tokson, *The Aftermath of* Carpenter*: An Empirical Study of Fourth Amendment Law*, *2018–2021*, 135 HARV. L. REV. 1790, 1824 n.206, 1830 (2022) (finding a shockingly

from third parties by arguing that individuals effectively consented to turning over their data when they used apps and shared their information. Indeed, a number of lower courts have differentiated between voluntarily affirmative acts and automatically generated information.[123] This has resulted in rulings in favor of the government in the majority of cases raising this issue post-*Carpenter*.[124] These decisions argue that voluntary information creation, without steps to prevent disclosure, falls outside *Carpenter*'s limited third-party doctrine exception.[125]

This narrow interpretation of *Carpenter* ignores how individuals actually interact with their digital devices. Even when adults take voluntary actions that create data, they generally do not meaningfully consent to the private-sector apps they use.[126] It seems even clearer that children do not consent to the disclosure of their data, particularly in cases where parents, not children, are installing apps on children's phones that are then being mined for data. At the same time, the government might argue that by voluntarily and affirmatively utilizing location tracking, parents have proactively created data that falls outside of *Carpenter*'s narrow exception for data automatically generated without the user acting.[127] Unlike the passive location tracking on adult phones, parents may actively opt into tracking their children's location, with law enforcement agencies taking advantage of such data for their own purposes.

This is the complex landscape of who can consent: We let children consent to searches of their devices. We also let parents consent over their child's objection. For children who are in government custody, control—and consent over the device—may lie with the state itself. And direct consent isn't even necessary given parental control apps.

---

high rate of cases resolved based on the "good faith exception" to the exclusionary rule, and that in 82.6 percent of cases post-*Carpenter*, courts denied fourth amendment protections).

123. *See* Tokson, *supra*, note 122, at 1803.

124. *Id.* at 1823.

125. *See e.g.*, *id.*; United States v. Trader, 981 F.3d 961, 967 (11th Cir. 2020).

126. *Data Brokerage, the Sale of Individuals' Data, and Risks to Americans' Privacy, Personal Safety, and National Security: Hearing on "Who is Selling Your Data: A Critical Examination of the Role of Data Brokers in the Digital Economy" Before the Subcomm. on Oversight and the Judiciary of the H. Comm. on Energy & Com.*, 118th Cong. 8 (2023) (written testimony of Justin Sherman), https://d1dth6e84htgma.cloudfront.net/Sherman_Testimony_4_19_23_b40d947a8e.pdf?updated_at=2023-04-17T17:40:42.415Z [https://perma.cc/JW3P-G4E5].

127. Carpenter v. United States, 585 U.S. 296, 315–16 (2018). In previous work, I have advocated for a parent-child privilege to protect children's communications intended just for their parents. *See generally* Nila Bala, *Parent-Child Privilege as Resistance*, 65 B.C. L. REV. 2629 (2024).

C. Who Should Consent

This Section advances two key arguments: first, a child's consent to law enforcement digital searches should not be considered voluntary, and second, relying on parental consent to protect children's data is fundamentally flawed.

1. A Child's Consent

Both minors and adults feel compelled to cooperate with the police, but this tendency is especially pronounced among young people, particularly youth of color. Research indicates young people are especially vulnerable to coercion and pressure.[128] Children are conditioned to comply with authority figures—police, judges, teachers, faith leaders, and parents.[129] Furthermore, they are less experienced in the legal arena, and may not understand that officers cannot force their compliance.[130] Compounding these factors, Black and brown children are especially likely to have been given "the talk," and understand that it may be deadly for them not to comply.[131]

Given what we know about adolescent development, the legal system's routine acceptance of minors' consent to searches is difficult to justify. Especially so because we are far more protective of children's vulnerability and incapacity with regard to decision-making in other contexts. For example, children's ability to voluntarily agree to police demands is treated with greater skepticism in the custodial interrogation.[132] The same "freely

128. Laurence Steinberg & Elizabeth S. Scott, *Less Guilty by Reason of Adolescence: Developmental Immaturity, Diminished Responsibility, and the Juvenile Death Penalty*, 58 AM. PSYCH. 1009, 1014 (2003).

129. Thomas Grisso et al., *Juveniles' Competence to Stand Trial: A Comparison of Adolescents' and Adults' Capacities as Trial Defendants*, 27 L. & HUM. BEHAV. 333, 357 (2003) [hereinafter *Juveniles' Competence to Stand Trial*] (explaining that the choices of juveniles seem to reflect their tendency to heed authority figures); *see also* TOM R. TYLER & RICK TRINKNER, WHY CHILDREN FOLLOW RULES: LEGAL SOCIALIZATION AND THE DEVELOPMENT OF LEGITIMACY (2017).

130. *See* Kristin Henning, *The Reasonable Black Child: Race, Adolescence, and the Fourth Amendment*, 67 AM. U. L. REV. 1513, 1523 (2018) (stating that youths' cognitive levels can impact their choices, and that their cognitive abilities greatly improve through life experience and education).

131. *See* Leslie A. Anderson, Margaret O'Brien Caughy & Margaret T. Owen, *"The Talk" and Parenting While Black in America: Centering Race, Resistance, and Refuge*, 48 J. BLACK PSYCH. 475, 476 (2021); *see also* Juan J. Barthelemy, Cassandra Chaney, Elaine M. Maccio & Wesley T. Church, II, *Law Enforcement Perceptions of Their Relationship with Community: Law Enforcement Surveys and Community Focus Groups*, 26 J. HUM. BEHAV. SOC. ENV'T 413, 424 (2016).

132. *See, e.g.*, J.D.B. v. North Carolina, 564 U.S. 261, 280 (2011); State v. G.O., 543 P.3d 1096, 1101 (Kan. 2024) (the Due Process Clause of the Fourteenth Amendment protects against an involuntary confession, even when reliable); *In re* Andre M., 88 P.3d 552, 556 (Ariz. 2004) (excluding mother created presumption of involuntariness); *In re* Jerrell C.J., 699 N.W.2d 110, 110 (Wis. 2005) (juvenile's

and voluntarily given" standard ostensibly applies to both consent searches and confessions. But courts more readily recognize involuntariness in the custodial interrogations. The discrepancy between searches and interrogations is evident in cases like *J.D.B. v. North Carolina* and in state court decisions excluding coerced confessions from minors.[133]

In non-criminal contexts, we also take juvenile status more seriously. Adolescents generally do not possess the legal capacity to consent to medical procedures, with a few exceptions.[134] Children generally cannot consent to sex.[135] We have also placed limitations on minors' ability to contract.[136] In some jurisdictions minors cannot contract at all.[137] There is no implicit assumption that young people possess decision-making capacities comparable to adults when it comes to consent, waiver, and making agreements.

Take the Children's Online Privacy Protection Act (COPPA) as a point of comparison to the criminal context.[138] COPPA ostensibly prevents adolescents under thirteen from consenting to data sharing with commercial third parties without parental consent.[139] COPPA 2.0—a bipartisan bill introduced in 2023—would go even further by prohibiting collection of personal information from users under sixteen, create an "eraser" button to eliminate personal information from children, and establish a "digital marketing bill of rights for teens" to limit the collection of personal information.[140] U.S. Senator Edward Markey (Massachusetts), one of the sponsors of the bill, explains "Congress must pass *COPPA 2.0* to put immediate safeguards in place that prevent Big Tech from tracking,

written confession to police was not voluntarily given); Ochoa v. State, 707 S.W.3d 344, 365–65 (Tex. Crim. App. 2024) (fourteen-year-old's confession was rendered involuntary due to coercive law enforcement tactics).

133. *See supra* note 130.

134. These exceptions include birth control, pregnancy related care, care around sexually transmitted diseases, and substance abuse and alcohol disorder treatment. Douglas S. Diekema, *Adolescent Brain Development and Medical Decision-Making*, 146 PEDIATRICS S1, S19 (2020).

135. *Age of Consent by State 2025*, WORLD POPULATION REV., https://worldpopulationreview.com/state-rankings/age-of-consent-by-state [https://perma.cc/7A5H-GPSR].

136. *See* Cheryl B. Preston & Brandon T. Crowther, *Infancy Doctrine Inquiries*, 52 SANTA CLARA L. REV. 47, 50 (2012).

137. *Id.*

138. 15 U.S.C. §§ 6501–06.

139. I say ostensibly because one criticism of COPPA is the easy workaround of children lying about their age. Lauren A. Matecki, *Update: COPPA Is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era*, 5 NW. J.L. & SOC. POL'Y 369, 383 (2010).

140. Press Release, Sen. Ed Markey, Senators Markey and Cassidy Reintroduce COPPA 2.0, Bipartisan Legislation to Protect Online Privacy of Children and Teens (May 3, 2023), https://www.markey.senate.gov/news/press-releases/senators-markey-and-cassidy-reintroduce-coppa-20-bipartisan-legislation-to-protect-online-privacy-of-children-and-teens [https://perma.cc/CGW9-J9XG].

traumatizing, and targeting young people every second, every minute, and every hour of the day."[141]

However, Big Tech isn't the only entity engaging in such practices. Law enforcement, in collaboration with schools and companies, does much of the same. COPPA has been criticized by many: It is easy for children to subvert, it provides too narrow a definition of personal information, it is insufficiently enforced, and the parental consent requirement does little to protect minors.[142] Still, COPPA demonstrates that we at least value, and attempt to keep private, children's data on the commercial side. But paradoxically we have yet to extend any similar protection to children's data within the criminal and juvenile legal systems.

This lack of protections has serious consequences for children. In the last decade, law enforcement has made increasingly consequential requests of minors. For example, officers have directly approached children to obtain consent for DNA collection.[143] Similarly, officers may deliberately approach children when they are alone for their data, as children may be more likely to consent than adults.[144]

One solution is to allow mature minors to consent, while requiring parental consent for younger adolescents, as Kris Henning proposes.[145] An approach resting on the "mature minor" doctrine may be an improvement over the current state of affairs—at least it provides some decisional autonomy to older adolescents who somehow have the wherewithal to object to the police, even over their parent's disagreement. This is the brave and exceedingly rare adolescent.

Henning's approach, however, leaves out younger adolescents who would not qualify as "mature minors," but are still in need of protection. It assumes that parents are adequate protection for younger adolescents—which, as raised above in Section I.B—is shortsighted. Second, relying on

141. *Id.*

142. *See* Takhshid, *supra* note 20, at 1422.

143. People v. K.N., 87 N.Y.S.3d 862, 871 (N.Y. Crim. Ct. 2018) (discussing the practice and proclaiming DNA buccal swab should not be taken without presence of a parent, guardian, attorney); Dana Littlefield, *ACLU Sues San Diego Police over How It Collects DNA from Juveniles*, SAN DIEGO UNION-TRIBUNE (Feb. 20, 2017, 2:00 PM), https://www.sandiegouniontribune.com/news/courts/sd-me-dna-lawsuit-20170217-story.html# [https://perma.cc/FUK2-5JUL] (ACLU sued police for obtaining DNA from minors without notifying a parent); Lauren Kirchner, *DNA Dragnet: In Some Cities, Police Go from Stop-and-Frisk to Stop-and-Spit*, PROPUBLICA (Sept. 12, 2016, 8:00 AM), https://www.propublica.org/article/dna-dragnet-in-some-cities-police-go-from-stop-and-frisk-to-stop-and-spit [https://perma.cc/658P-G2LC] (describing police approaching young people alone for DNA).

144. *See, e.g.*, Saavedra v. State, 622 So. 2d 952, 962 (Fla. 1993) (Barkett, C.J., concurring) (describing that a troubling consequence of a decision allowing juveniles to consent to police searches may be "an invitation to look for opportunities when officers know a juvenile is present in the home they wish to search without a warrant"); Littlefield, *supra* note 143; Kirchner, *supra* note 143.

145. Henning, *supra* note 30, at 83.

the mature minor doctrine asks too much of older adolescents in this context. The mature minor doctrine is mainly used in the medical context to allow minors to consent to certain medical treatments without parental involvement.[146] But the medical context, while not free from bias, lacks the acute coercion and risk inherent in law enforcement interactions. Even older adolescents may struggle to resist police pressure.

A framework that is more protective of *all* children is needed—one that would create guardrails and not depend on parents to determine how best to protect the child's data. In juvenile system involvement, parents are particularly ill-suited to protect children. In *The New Law of the Child*, and later in *The New Parental Rights*, Anne Dailey and Laura Rosenbery set forth a proposal to take children's interests seriously, even over parent's objections, across various domains including medical care, corporal punishment, and public schooling.[147] Adding to this line of scholarship, this Article considers the criminal and juvenile spaces as domains where we must create safeguards to protect children, moving beyond reliance on their parents.[148] If, as Kate Weisburd argues, consent is doing the "dirty work" in the criminal legal system to continue to subordinate marginalized groups, the following subsection argues how parental consent is doing the dirty work in the state's continued ability to prosecute juveniles.[149]

2. A Parent's Consent

We should avoid relying on parental consent for two interconnected reasons. First, parents often fail to serve as effective safeguards against police intrusion and may not fully understand or assert their children's rights. Second, placing the burden of consent on parents can strain the parent-child relationship, which the legal system should aim to protect rather than jeopardize.

The notion that parental access to a child's device justifies unlimited authority to consent to government searches contradicts modern privacy principles. As the Court affirmed in *Carpenter v. United States*, an adult can still have a legitimate expectation of privacy in cell site data they share with service providers.[150] People inherently understand their own privacy in this

146. Shawna Benston, *Not of Minor Consequence?: Medical Decision-Making Autonomy and the Mature Minor Doctrine*, 13 IND. HEALTH L. REV. 1, 2 (2016).

147. Anne C. Dailey & Laura A. Rosenbury, *The New Law of the Child*, 127 YALE L.J. 1448, 1452 (2018); *see also* Dailey & Rosenbury, *supra* note 39.

148. *See* Dailey and Rosenbury, *supra* note 39.

149. Kate Weisburd, *Criminal Procedure Without Consent*, 113 CALIF. L. REV. 697 (2025).

150. Carpenter v. United States, 585 U.S. 296, 309–13 (2018).

way as well, as context dependent.[151] For children, relational privacy—this sense of privacy within the relationship and family—is vital.[152] Relational privacy recognizes that rather than privacy being an all-or-nothing concept, the relationship between who is doing the searching and who is being searched matters.[153] Confidentiality and trust that the information will not be divulged is necessary for the child to form positive relationships with her parents.[154] However, the dicta from *Randolph* incentivizes law enforcement to bypass a child's refusal by seeking parental consent. This approach pits child against parent, potentially straining already tense relationships due to police involvement.[155]

In contrast, current case law only protects children who *do not* share with their parents, paradoxically incentivizing secrecy within the parent-child relationship. Children have a legitimate expectation of privacy when alone: If a child refuses a search of the home, the State cannot enter the family home anyway.[156] But children generally do not live alone.[157] They also tend not to own their own phones, with passwords they keep from their parents. If J.P. remained alone in the station and objected to the search, the search would not have taken place. If the police had forced J.P. to reveal his passcode, that would likely raise constitutional issues.[158] But the child has no refuge in the Fourth Amendment when it is their mother who is forcing the password out of him and turning over evidence to the police.

Additionally, the empirical research suggests J.P.'s story is all too common: Instead of obstructing searches, parents often facilitate them. While people may believe they would refuse consent in theory, research shows they rarely do when actually confronted by law enforcement.[159] Thus, while the ex ante idea of parents serving as independent protectors of their children's interests seems intuitively appealing, research suggests this

151. Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCI. MAG. 509, 509–10 (2015).

152. *See* Laurent Sacharoff, *The Relational Nature of Privacy*, 16 LEWIS & CLARK L. REV. 1249, 1250–51 (2012).

153. *Id.* at 1251.

154. For a longer discussion of relational privacy, see Bala, *supra* note 127.

155. *See* Mariam Hinds, *Tools and Targets: The Unconstitutional Surveillance of System-Adjacent Individuals*, 103 WASH. U. L. REV. (forthcoming 2026) (manuscript at 42) (on file with author) (discussing how families become deputized as state agents to report on their system involved family members).

156. *See* Henning, *supra* note 30, at 70.

157. *Id.*

158. *See, e.g.*, Brief of *Amicus Curiae* Electronic Frontier Foundation in Support of Petitioner at 2, Sneed v. Illinois, No. 23-5827 (U.S. Nov. 16, 2023), 2023 WL 8085021 (arguing compelling a passcode to be akin to self-incrimination).

159. Roseanna Sommers & Vanessa K. Bohns, *The Voluntariness of Voluntary Consent: Consent Searches and the Psychology of Compliance*, 128 YALE L.J. 1962, 1988 (2019).

safeguard has largely failed in practice.[160] The law has tried relying on parents before. The Supreme Court's 1945 decision in *Haley v. Ohio* introduced the concept of the "interested adult,"[161] an adult, typically a parent, independent from the prosecution who is supposed to protect the child's welfare.[162] Due to the juvenile's youth and lack of maturity, the *Haley* Court recommended (though did not require) that a child have the help of a trusted adult, like a parent, "during the critical hours of questioning" so the "overpowering presence of the law . . . [may not] crush him."[163] The Court had reason to be concerned. For example, adults choose to avoid self-incrimination in forty percent of cases, while children remain silent only nine to eleven percent of the time after being advised of their rights.[164]

So, it is understandable that courts would turn to parents to protect youth in the Fifth Amendment context. In recent years, states have increasingly required the presence of an interested adult to make a young person's statements admissible during a custodial interrogation.[165] Most of these states do not differentiate between the presence of a parent and an attorney.[166] Only three states recognize that a parent may have an interest adverse to the child's, but even here, a conflict of interest is narrowly characterized, focusing solely on situations where the parent is a suspected co-defendant or victim, neglecting more nuanced issues that can pose problems.[167] For example, parents may themselves be fearful of law

160. Sommers and Bohns's research supports this proposition, as does the research cited below concerning custodial interrogations and parents' failure to protect their children in that context. *See id.*; *infra* note 165–66.

161. 332 U.S. 596, 600 (1948).

162. *See, e.g.*, *In re* E.T.C., 449 A.2d 937, 940 (Vt. 1982) (ruling that the "adult must be one who is not only genuinely interested in the welfare of the juvenile but completely independent from and disassociated with the prosecution, e.g., a parent, legal guardian, or attorney representing the juvenile").

163. *Haley*, 332 U.S. at 600.

164. *See* J. Thomas Grisso & Carolyn Pomicter, *Interrogation of Juveniles: An Empirical Study of Procedures, Safeguards, and Rights Waiver*, 1 LAW & HUM. BEHAV. 321, 339 (1977) (demonstrating enormous disparity between adults' and juveniles' utilization of *Miranda* rights).

165. Andy Clark, Comment, *"Interested Adults" with Conflicts of Interest at Juvenile Interrogations: Applying the Close Relationship Standard of Emotional Distress*, 68 U. CHI. L. REV. 903, 903–04 (2001).

166. Twenty states provide protections to adolescents that require the involvement of a parent, guardian, attorney, or other interested adults; others simply consider it a factor in the totality of circumstances analysis. Michelle Jeffs & Sean Brian, *Parental Presence or Totality of Circumstances? An Assessment of Utah's Juvenile* Miranda *Law & 50 State Survey,* 24 N.Y.U. J. LEGIS. & PUB. POL'Y 565, 586, 594 (2022).

167. KAN. STAT. ANN. § 38-2333 (2024) (if parent is victim or codefendant and juvenile is less than 14, attorney must be consulted); MONT. CODE ANN. § 41-5-331 (2023) (if the parent or guardian disagrees with waiver, and young person wants to waive, then the minor must consult an attorney); *Floor Debate on H.B. 158 Juvenile Interrogation Amendments*, UTAH STATE LEGIS., at 1:30:13–1:46:55 (Feb. 11, 2021), https://le.utah.gov/av/floorArchive.jsp?markerID=113877 (last visited Aug. 21, 2025).

enforcement or may initiate a police response to their child's perceived misbehavior.[168] In such scenarios, the parents' interests may not necessarily align with protecting the child.[169]

Additionally, empirical research calls into question whether parents can successfully serve as an interested adult, even without obvious conflicts of interest. One study found that parents who attended interrogations generally offered no advice to their children; many did not even speak to their children at all.[170] When parents did converse with their children, they recommended waiver of *Miranda*.[171]

Many of the same issues that make relying on parents problematic in the *Miranda* waiver context are true in the Fourth Amendment context as well. More specifically with regard to digital evidence, four issues can emerge around appointing parents as the interested adults: parental ignorance around digital data, parental fear of law enforcement, a desire to "scare children straight," and a more obvious conflict of interest.[172]

First, most parents, and indeed, most adults, lack a basic understanding of the data stored on cell phones and what they might be sharing.[173] Most Americans report general confusion over data, expressing a lack of understanding about data use.[174] This ignorance has relevant implications regarding direct consent to search their child's data, as well as indirect consent scenarios where law enforcement purchase or otherwise obtain data from third parties. Both situations epitomize "unwitting consent," a concept privacy scholars Neil Richards and Woodrow Hartzog define as instances where individuals consent without understanding the scope or consequences of what they have agreed to.[175] Unwitting consent "can take at least three forms, including not understanding the legal agreement, not understanding

168. *See infra* Section I.C.2 (describing four ways parents can be an inadequate safeguard).

169. Cynthia Godsoe, Response, *A Perfect Storm: Young People, False Confessions & Prosecutorial Involvement (Response to Dan Medwed's* Barred: Why the Innocent Can't Get Out of Prison*)*, 58 NEW ENG. L. REV. 1, 24 (2023).

170. *See* THOMAS GRISSO, JUVENILES' WAIVER OF RIGHTS: LEGAL AND PSYCHOLOGICAL COMPETENCE 182–86 (1981) (describing a study finding that most of the time parents do not offer advice to their children during interrogations, and often they instruct their children to waive their rights—including their right to an attorney).

171. *Id.*

172. I use this taxonomy in my work around children's DNA. *See* Bala, *supra* note 22, at 492–94.

173. Hannah J. Hutton & David A. Ellis, *Exploring User Motivations Behind iOS App Tracking Transparency Decisions*, CHI: CONF. ON HUM. FACTORS COMPUTING SYS., April 2023. This is particularly true as older individuals are less likely to be digital natives than their younger counterparts.

174. BROOKE AUXIER ET AL., PEW RSCH. CTR., AMERICANS AND PRIVACY: CONCERNED, CONFUSED AND FEELING LACK OF CONTROL OVER THEIR PERSONAL INFORMATION (2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/Q7U2-W6LV].

175. Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1478 (2019).

the technology being agreed to, or not understanding the practical consequences or risks of agreement."[176] All three are at play with regard to police use of children's data. Individuals possess the right to restrict the scope of data searches or refuse them entirely. However, these rights are only effective if people are aware of them.

An illustration that makes clear the dangers of unwitting consent is when the child is a victim (typically defined as someone who has been harmed by a crime).[177] Children who are "victims" may also be suspects, yet the criminal legal system continues to posit the victim/offender binary as obvious and rigid.[178] The complexities with assigning the "victim" label is evident with sexting, which is common among children and teens.[179] Jane's story at the beginning of this Article is one such illustration: a child taking sensitive pictures of themselves, a father worried their child is a victim and is being exploited, and police instead arresting the child. Jane's story is not an isolated one; it is becoming increasingly prevalent for states to prosecute teenagers for sending pictures of themselves and creating child pornography.[180] In this scenario, a parent turning over a child's phone aids the police in collecting evidence against his child. Similarly, the criminalization of victims of child sex trafficking blurs the line between victims and offenders.[181] There have also been a number of cases where law enforcement made assumptions that a child was a victim, received parental consent to search, and the child later became a suspect.[182]

176. *Id.* at 1466.

177. Black's Law Dictionary defines "victim" as "[a] person harmed by a crime, tort, or other wrong." *Victim,* BLACK'S LAW DICTIONARY (11th ed. 2019); *see, e.g.*, *In re* H.K.D.S., 469 P.3d 770, 777 (Or. Ct. App. 2020) (citing Dubbs v. Head Start, Inc., 336 F.3d 1194 (10th Cir. 2003)) (warrantless searches of child's body permissible where child is not a suspect in criminal investigation); Roe v. Tex. Dep't of Protective & Regul. Servs., 299 F.3d 395 (5th Cir. 2002); Wallis v. Spencer, 202 F.3d 1126 (9th Cir. 2000); Calabretta v. Floyd, 189 F.3d 808 (9th Cir. 1999). Note if the parent is the alleged source of the abuse, parental consent to conduct a search or medical exam may not be needed.

178. Cynthia Godsoe, *The Victim/Offender Overlap and Criminal System Reform*, 87 BROOK. L. REV. 1319, 1319–23 (2022).

179. Sheri Madigan, Anh Ly, Christina L. Rash, Joris Van Ouytsel & Jeff R. Temple, *Prevalence of Multiple Forms of Sexting Behavior Among Youth: A Systematic Review and Meta-Analysis*, 172 JAMA PEDIATRICS 327, 327–35 (2018).

180. *See* Megan Sherman, Note, *Sixteen, Sexting, and A Sex Offender: How Advances in Cell Phone Technology Have Led to Teenage Sex Offenders*, 17 B.U. J. SCI. & TECH. L. 138, 139 (2011)*; see also* Daniel Griffin, Caleb Michael & Matthew Night, *Ohio Police Suggested Charging an 11-year-old for Her Explicit Photos. Experts Say the Practice is Common*, FOX59 NEWS (Sept. 22, 2023, 9:26 AM), https://fox59.com/news/national-world/ohio-police-suggested-charging-an-11-year-old-for-her-explicit-photos-experts-say-the-practice-is-common/ [https://perma.cc/N5BG-YH5Y].

181. Tamar R. Birckhead, *The "Youngest Profession": Consent, Autonomy, and Prostituted Children*, 88 WASH. U. L. REV. 1055, 1068–69 (2011) (prostituted minors being treated as offenders and victims).

182. *See, e.g.*, Commonwealth v. Kaipat, No. 2021-SCC-0016-CRM, 2022 WL 18046438, at *11 (N. Mar. I. Dec. 31, 2022) (collecting buccal and fingernail swabs when child was assumed to be a victim).

With digital evidence in particular, which can far outlast the case at hand, the information from the child-as-victim can be used against them in unexpected ways. Information collected by the state from children alleged to have been abused or neglected may resurface in various contexts, including repercussions in the delinquency system, criminal system, immigration system, or even if they themselves are later a parent in the family regulation system.[183] There are no protections for digital evidence gathered when the state shapeshifts, and moves from viewing the child as a victim to as a suspect. Thus, unwitting parental consent for the child-as-victim may raise complicated issues.

Second, parents themselves may fear law enforcement.[184] Minority communities fear and distrust police, with Black individuals five times more likely to fear police brutality than whites.[185] In one of the most famous examples of parental pressure on a child, the father of Antron McCray—one of the Central Park Five who was wrongfully convicted of assaulting a woman—forced his child to comply with the police because of his own fear of the police.[186] But less notable examples of parental pressure occur every day, including sixteen-year-old J.P. (described by the court as a young African American male) who initially refused the search of his phone until his mother persuaded him to turn over the device and passcode to law enforcement.[187] As Kris Henning and Rebba Omer write, "Black and Latinx youth have the added complication of fear, anxiety, and parental instructions to comply with police to stay alive." Along with fear of police brutality, parents may also fear being held formally accountable in criminal or civil court for their children's misconduct.[188] The recent case of Jennifer and James Crumbley, parents convicted for a mass school shooting committed by their son, serves as a stark reminder that parents should be fearful that

183. *See, e.g.*, S. Lisa Washington, *Fammigration Web*, 103 B.U. L. REV. 117, 124 (2023) (immigration officials make use of the family regulation system's coercive nature and ability to gather detailed information.) [hereinafter Washington, *Fammigration Web*]; S. Lisa Washington, *Pathology Logics*, 117 NW. U. L. REV. 1523, 1552 (2023) (childhood mental health and school records may be used in family regulation proceedings); Anna Arons, *The Empty Promise of the Fourth Amendment in the Family Regulation System*, 100 WASH. U. L. REV. 1057, 1119 (2023) (describing the states' own invasiveness and use of family regulation records).

184. Monica C. Bell, *Police Reform and the Dismantling of Legal Estrangement*, 126 YALE L.J. 2054, 2054 (2017) (describing the sense of estrangement that African Americans and residents of high poverty communities experience, that they are within the law but outside its protection).

185. *New Study Reveals Racial Disparities in Fear of Police Brutality*, NEUROSCIENCE NEWS (June 15, 2020), https://neurosciencenews.com/racial-disparity-police-brutality-16545/ [https://perma.cc/5NLL-WEL4].

186. Ronald Sullivan, *Youth's Father Says He Urged Park-Rape Lie*, N.Y. TIMES (July 28, 1990), https://www.nytimes.com/1990/07/28/nyregion/youth-s-father-says-he-urged-park-rape-lie.html [https://perma.cc/A834-ECWZ].

187. *In re* J.P., 2018 WI App, ¶¶ 14–16, 384 Wis. 2d 415, 921 N.W.2d 529.

188. *See* Henning, *supra* note 68, at 839.

their child's misbehavior can lead to consequences for them.[189] Thus, it may be in a parent's best interest to call the police if they are scared of their own potential legal consequences.

Third, parents may want to scare their children straight. In some instances, a parent may believe he is helping his child by calling the police. An entire industry feeds on this parental desire, placing "troubled teens" in bootcamps and wilderness programs, both with and without formal court involvement.[190] Parents can and do call the cops on their children.[191] Anthony Bandiero, an attorney who trains law enforcement, notes a frequent inquiry he has received involves "parents [who] believe that the[ir] son is engaged in some kind of criminal activity on the cellphone, and they want the cops to look in the cell phone . . . ."[192]

Finally, and relatedly, parents may have a direct conflict of interest with their child. Sometimes this occurs when the parent is a victim or co-defendant, or one of the child's siblings is in that position and the parent's loyalties are split.[193] In these cases, the parent may protect their own interest over those of their child. In the custodial interrogation context, certain states have begun to recognize the dangers of allowing parents to assist their children when a conflict of interest is present.[194] However, there is no similar legal recognition preventing parents from consenting to searches on behalf of their child.

Digital searches pose real harms. In the next Part, I will describe the nature of such searches, their typical execution, extensive scope, and the significant risks they present to children's well-being.

---

189. *See* Jamiles Lartey, *The Parents Paying for Their Children's Crimes*, MARSHALL PROJECT (Apr. 13, 2024, 12:00 PM), https://www.themarshallproject.org/2024/04/13/michigan-school-shooting-parents [https://perma.cc/7MU3-PPF6].

190. Catherine E. Krebs, *Five Facts About the Troubled Teen Industry*, AM. BAR ASSOC. (Oct. 22, 2021), https://www.americanbar.org/groups/litigation/resources/newsletters/childrens-rights/five-facts-about-troubled-teen-industry/ [https://perma.cc/8ALW-J3JF].

191. When I was a juvenile attorney, for example, the mother of one of my clients called the police on her child when she found a small amount of marijuana in his sock drawer. In the process, she initiated both delinquency and dependency proceedings. Instances of parents initiating delinquency proceedings against their own children are more prevalent than one might expect. *See also* Monica C. Bell, *Situational Trust: How Disadvantaged Mothers Reconceive Legal Cynicism*, 50 LAW & SOC'Y REV. 314, 315–17 (2016).

192. Blue to Gold, *Ep. #82: Can Parents Allow Police Officers to Look Through a Child's Cell Phone?*, YOUTUBE (Feb. 22, 2021), https://www.youtube.com/watch?v=Nk8hccSm6TY (last visited Aug. 21, 2025).

193. *See* Hayley M.D. Cleary, *10 Reasons Why Parent Involvement Is Not Enough to Protect Adolescent Suspects During Custodial Police Interrogations*, NACDL: THE CHAMPION (Dec. 2022), https://www.nacdl.org/Article/Dec2022-10ReasonsWhyParentInvolvementIsNotEnoughto [https://perma.cc/JRP3-X9VZ]; *see, e.g.*, *In re* H.K.D.S, 469 P.3d 770, 772 (Or. Ct. App. 2020) (one child was the suspect and the other the alleged victim, where parents consented to buccal swab).

194. *See supra* note 167.

II. LAW ENFORCEMENT ACQUISITION OF CHILDREN'S DATA

A. Searches of Digital Evidence

Cellphones, wearable devices, and the other technologies children interact with offer a wealth of information into their inner private lives. As Chief Justice Roberts explained a decade ago in *Riley v. California*:

> The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.[195]

In the decade since *Riley*, technological advancements have made digital devices integral to daily life. They track location, time, and even physical activity. These capabilities also make digital evidence irresistible to law enforcement officers, offering insight into a suspect's intent, whereabouts, and actions. These devices may "serve[] as the perfect eyewitness that can be seized, searched, and used" against the individual.[196] Juries increasingly expect digital evidence in cases and may be skeptical of prosecutors that do not present substantial technological evidence.[197] As a result, law enforcement officers are keen to seek out this evidence.

Digital searches are categorically different from all other searches. The Court in *Riley* noted that the search of a phone is even more invasive "than the most exhaustive search of a house . . . it also contains a broad array of private information never found in a home of any form . . . ."[198] Unlike physical searches that provide information tied to a specific moment, digital data persists and remains exploitable well into the future.[199] Additionally, a digital search extends beyond the individual minor's data to capture their entire social network, including other children who interact with them through the device.

It is hardly a surprise that digital searches have a different impact on young people. For adolescents, digital devices mediate nearly all intimate relationships—from friendships and family connections to romantic

195. 573 U.S. 373, 393 (2014).

196. Pat Augustine, *Wearable Evidence: Why the Pennsylvania Judiciary Should Require a Warrant to Search Wearable Technology*, 17 U. PITT. J. TECH. L. POL'Y 1, 2 (2017).

197. *See* Donald Shelton, Juror Expectations of Forensic Science Evidence (Feb. 18, 2025) (unpublished manuscript), https://papers.ssrn.com/abstract=5153931 [https://perma.cc/5WNC-TMJ8].

198. *See Riley*, 573 U.S at 396–97.

199. Kevin Lapp, *Databasing Delinquency*, 67 HASTINGS L.J. 195, 196–97 (2015).

partnerships.[200] Devices have dual functions of intimacies—first, it is the medium through which intimacies are forged, the "kinds of connections . . . on which they depend for living," but also through which education about intimacies can be created.[201] One psychological study found that young people rated a body search as fairly intrusive and personal and viewed cell phone searches similarly.[202] For digital data, there is no "true vindication of . . . privacy rights" when the reviewer has copied all of its contents and knows intimate details that cannot be deleted from the mind.[203]

Searches of children are also different. In *Roper v. Simmons* and its progeny, the Supreme Court cited developmental psychology and neuroscience to establish a foundational principle: "kids are different."[204] Children are especially likely to agree to consent, for the same reasons they are especially likely to falsely confess when interrogated by law enforcement.[205] They experience coercion and pressure differently from adults.[206] Police encounters in childhood can inflict lasting harm: They can lead to psychological distress, negative outcomes in physical health, and worse educational outcomes.[207] Police stops can constitute an adverse childhood event, causing a long-term threat to the wellbeing of the child.[208]

Children are also especially prone to creating digital evidence. Over ninety-five percent of teens aged thirteen to seventeen years have a

200. Rachel H. Scott et al., *What and How: Doing Good Research with Young People, Digital Intimacies, and Relationships and Sex Education*, 20 SEX EDUC. 675, 676 (2020).

201. *Id.*

202. Lori A. Hoetger, How Can Teens Be Reasonable? Reasonable Expectations of Privacy in the Digital Age 23 (June 29, 2018) (Ph.D. dissertation, University of Nebraska-Lincoln), https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1111&context=psychdiss [https://perma.cc/V55E-E45V].

203. Nathaniel Mensah, *"Can You Hear Me Now?": The Right to Counsel Prior to Execution of a Cell Phone Warrant Search*, 107 MINN. L. REV. 1129, 1146 (2023).

204. *See generally* Roper v. Simmons, 543 U.S. 551, 568–69 (2005) (relying both on death is different and kids are different as a principle); Miller v. Alabama, 567 U.S. 460, 471 (2012) ("[C]hildren are constitutionally different from adults"); Stephen St.Vincent, *Kids Are Different*, 109 MICH. L. REV. FIRST IMPRESSIONS 9, 9 (2010) ("While the old approach was summed up by the adage 'death is different,' the new approach may be that 'kids are different'").

205. Children are two to three times more likely to confess than adults. *See* Megan Crane, Laura Nirider & Steven A. Drizin, *The Truth About Juvenile False Confessions*, 16 INSIGHTS ON L. & SOC'Y 10, 12 (2016).

206. *See, e.g., In re* Elias V., 188 Cal. Rptr. 3d 202, 217 (Ct. App. 2015) (youth "rendered [the child] 'most susceptible to influence' and 'outside pressures'" (quoting *Roper*, 543 U.S. at 269)); Crane et al., *supra* note 205, at 15 ("[T]actics which may be legitimate when used on adults may be coercive when applied to children . . . .").

207. Victor J. St. John, Andrea M. Headley & Kristin Harper, *Reducing Adverse Police Contact Would Heal Wounds for Children and Their Communities*, CHILD TRENDS (June 14, 2022), https://www.childtrends.org/publications/reducing-adverse-police-contact-would-heal-wounds-for-children-and-their-communities [https://perma.cc/W3HJ-WKC5].

208. *Id.*

smartphone, with over half obtaining one by age eleven.[209] For many youth, their mobile devices are deeply intertwined with their personal identities and sense of self.[210] As one youth involved in the legal system said, "this phone is the only thing I have that is actually mine."[211] For some adolescents, their phones create their "safe space, places where they can go for mental health, places that make them feel human."[212] Devices are not only indispensable for personal purposes, but children are required to use them at most schools: Ninety-four percent of public schools reported they are providing laptops or tablets to their students.[213] Students and parents generally cannot opt-out of this privacy-invading technology.[214]

High percentages of digital platform use by young people, as well as a strong identification with their devices, increases the possibility that young people might unwittingly produce digital evidence. First, young people may be more susceptible to creating and retaining digital evidence on their phone due to the factors that characterize adolescent development. Even though adolescents and adults perform comparably on certain cognitive tests, young people display "psychosocial immaturity," demonstrating differences in perspective taking, susceptibility to peer pressure, and controlling impulsive behavior.[215] Adolescents are less likely to consider the consequences of their actions, which could lead to higher rates of recording and retaining incriminating evidence.[216] Second, most teens prefer texting or other forms

209. Aliah Richter, Victoria Adkins & Ellen Selkie, *Youth Perspectives on the Recommended Age of Mobile Phone Adoption: Survey Study*, 5 JMIR PEDIATRICS & PARENTING, issue no. 4, Oct. 2022, art. no. e40704, at 1, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9664330/ [https://perma.cc/BW39-78SG].

210. Val Hooper & You Zhou, *Addictive, Dependent, Compulsive? A Study of Mobile Phone Usage*, 20th Bled eConference eMergence: Merging and Emerging Technologies, Processes, and Institutions 272 (2007), https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1021&context=bled2007 [https://perma. cc/P7N6-VKSU].

211. Michelle Lyttle Storrod, Digital Justice: Girls, Phones, & Juvenile Justice 1 (May 2020) (Ph.D. dissertation, Graduate School-Camden, Rutgers, The State University of New Jersey), https://rucore.libraries.rutgers.edu/rutgers-lib/65731/PDF/1/play/ [https://perma.cc/88TG-YY7Y].

212. Jason Kelley, *Thousands of Young People Told Us Why the Kids Online Safety Act Will Be Harmful to Minors*, ELEC. FRONTIER FOUND. (Mar. 15, 2024), https://www.eff.org/deeplinks/2024/03/thousands-young-people-told-us-why-kids-online-safety-act-will-be-harmful-minors [https://perma.cc/RGV2-TDYH].

213. Press Release, Nat'l Ctr. for Educ. Stats., Too Few Candidates Applying for Teaching Jobs the Primary Hiring Challenge for More than Two-Thirds of Public Schools Entering the 2022-23 School Year (Sept. 27, 2022), https://nces.ed.gov/whatsnew/press_releases/09_27_2022.asp [https://perma.cc/285A-BMLQ].

214. *See, e.g.*, FRIDA ALIM, NATE CARDOZO, GENNIE GEBHART, KAREN GULLO & AMUL KALIA, ELEC. FRONTIER FOUND. SPYING ON STUDENTS: SCHOOL-ISSUED DEVICES AND STUDENT PRIVACY 5 (2017), https://www.eff.org/files/2017/04/13/student-privacy-report.pdf [https://perma.cc/MFT6-5VC7].

215. Elizabeth Cauffman, Adam Fine, Alissa Mahler & Courtney Simmons, *How Developmental Science Influences Juvenile Justice Reform*, 8 U.C. IRVINE L. REV. 101, 103 (2018).

216. *Id.* at 102.

of messaging to speaking on the phone, leaving electronic records behind.[217] Third, young people with limited access to information may inadvertently create online footprints, for example, to access information about abortion and gender affirming healthcare.[218] In the aftermath of *Dobbs*, a simple Google search may hold criminal implications.[219]

So, it is no surprise that police are eager to seek digital evidence. They acquire children's data through two main routes: direct consent searches and indirect searches facilitated by third parties. Both methods often involve parental participation. The following subsections examine these approaches, highlighting the role of parental involvement in each.

1. Direct Consent Searches

Officers typically collect digital evidence through consent searches. Despite a general requirement that law enforcement must obtain a search warrant before searching the contents of a phone, upwards of ninety percent of searches are completed through consent.[220] Cost and time used to deter indiscriminate consent searches of devices. That is no longer the case.

Today, almost all agencies have access to mobile device forensic tools (MDFTs), "a powerful technology that allows police to extract a full copy of data from a cellphone—all emails, texts, photos, location, app data, and more—which can then be programmatically searched."[221] These tools can bypass security features, accessing both device and cloud-based data, and even find deleted materials and behavioral data an individual may not even

---

217. AMANDA LENHART, RICH LING, SCOTT CAMPBELL & KRISTEN PURCHELL, PEW RSCH. CTR., TEENS AND MOBILE PHONES (2010), https://www.pewresearch.org/internet/2010/04/20/teens-and-mobile-phones/ [https://perma.cc/S6CZ-T6L4].

218. *See* Anna Lea Altshuler, *How Is the* Dobbs *Ruling Affecting U.S. Adolescents?*, 73 J. ADOLESCENT HEALTH 969, 969–70 (2023); *American Adolescents' Sources of Sexual Health Information*, GUTTMACHER INST. (Dec. 2017), https://www.guttmacher.org/sites/default/files/fact sheet/facts-american-teens-sources-information-about-sex.pdf [https://perma.cc/39ZT-TVMK] (online sources are important for adolescents to get information.)

219. *See* Rebecca Saber, *The Impact of the Post*-Dobbs *Criminalization of Abortion on the Cybersecurity Ecosystem in the United States*, N.Y.U. J. LEGIS. & PUB. POL'Y (Mar. 27, 2023), https://nyujlpp.org/quorum/saber-cybersecurity-post-dobbs/ [https://perma.cc/GK37-HHDG] (describing police access to pregnant persons' data).

220. Adam Schwartz, *So-Called "Consent Searches" Harm Our Digital Rights*, ELEC. FRONTIER FOUND. (Jan. 14, 2021), https://www.eff.org/deeplinks/2021/01/so-called-consent-searches-harm-our-digital-rights [https://perma.cc/UUP5-RLQA]; Alafair S. Burke, *Consent Searches and Fourth Amendment Reasonableness*, 67 FLA. L. REV. 509, 511 (2015) ("Multiple scholars have estimated that consent searches comprise more than 90% of all warrantless searches by police.").

221. *See* LOGAN KOEPKE, EMMA WEIL, URMILA JANARDAN, TINUOLA DADA & HARLAN YU, UPTURN, MASS EXTRACTION: THE WIDESPREAD POWER OF U.S. LAW ENFORCEMENT TO SEARCH MOBILE PHONES 4 (2020), https://www.upturn.org/static/reports/2020/mass-extraction/files/Upturn-Mass Extraction.pdf [https://perma.cc/R47F-DG8H].

know their phone holds.[222] Agencies store the phone's data once acquired in perpetuity, and even create databases aggregating information, including contacts, location data, or anything else of interest.[223] The power of MDFTs is multiplied when used with consent searches: Officers can copy an entire device's contents, whereas some courts require warrants to specify a narrower scope.[224]

Despite agency efforts to downplay access to this technology, a recent records request by the nonprofit Upturn found that at least 2,000 agencies have purchased these tools, often utilizing federal grant funding.[225] Those agencies that do not own their own MDFTs often have easy access to them thanks to partnerships and sharing agreements with other agencies.[226] This covert adoption has occurred without public awareness or governing policies.[227]

Law enforcement agencies justify MDFT use for serious crime. However, records reveal a routine deployment of this technology in relatively mundane cases—"graffiti, shoplifting, marijuana possession, prostitution, vandalism, car crashes, parole violations, petty theft, public intoxication, and the full gamut of drug-related offenses"—offenses often associated with youth.[228] At least one case noted by Upturn was a cellphone search of a minor, for allegedly violating the terms of his electronic home monitoring.[229] Searches for digital evidence may also be undertaken in cases where police are not investigating a case at all.[230] Under the Fourth Amendment, all that is required is "consent."

To assess administrative safeguards beyond the Fourth Amendment, I conducted a comprehensive survey of California law enforcement agencies' policies regarding consensual digital searches of minors. California was an

222. *Id.* at 27–30; *See also* Jonathan Kerr, *Riding on Horseback to the Moon: Consent Searches in the Age of Smartphones and Digital Tracking*, 82 WASH. & LEE L. REV. 491, 526–27 (2025).

223. KOEPKE ET AL., *supra* note 221, at 53 (suggesting databases are possible).

224. MDFTs can recover logs about when apps were installed, when a device was locked, when a message was viewed, when Bluetooth was connected, and what apps were open at a certain time. *Id.* at 22; *see also* Jennifer Lynch, *New Federal and State Court Rulings Show Courts Are Divided on the Scope of Cell Phone Searches Post*-Riley, ELEC. FRONTIER FOUND. (Oct. 4, 2022), https://www.eff.org/deeplinks/2022/10/new-federal-and-state-court-rulings-show-courts-are-divided-scope-cell-phone [https://perma.cc/V45S-53CL].

225. KOEPKE ET AL., *supra* note 221, at 4; Victor Cooper, *Uncovering the "Who-Done-It" Truth: How Digital Forensics Empowered Lee County Sheriff's Office in Homicide Investigations*, CELLEBRITE (July 31, 2023), https://cellebrite.com/en/uncovering-the-who-done-it-truth-how-digital-forensics-empowered-lee-county-sheriffs-office-in-homicide-investigations/ [https://perma.cc/SX2X-HTSE].

226. KOEPKE ET AL., *supra* note 221, at 39.

227. *Id.* at 49, 55.

228. *Id.* at 42.

229. *Id.* at 44.

230. Unlike warrants, suspicionless consent searches need no cause, leading to more biased assessments. *See* Sommers & Bohns, *supra* note 18, at 1967 n.8.

ideal research setting for several reasons. First, state law mandates public online access to law enforcement policy manuals.[231] Second, California's reputation for progressive legislation and privacy protection suggested its agencies might be more likely to have developed policies around MDFT use with minors.[232] Of the 412 law enforcement agencies surveyed, 75 responded. Not a single responding department had established specific policies governing consent searches of minors' digital devices. [233] The absence of administrative guidelines has an important implication: It leaves officers with unfettered discretion to conduct these searches.[234] This discretion has historically translated into racialized policing, with Black and brown children facing disproportionately high rates of law enforcement encounters.[235] And without policy constraints, detectives routinely employ interrogation-like techniques to gain consent, methods that have been highly criticized—especially when used on young people.[236]

2. Indirect Methods to Obtain Children's Data

This Section addresses indirect methods to obtain children's data, through (1) commercial sources (including data brokers) and (2) schools. As noted above, *Carpenter* suggests that third-party disclosure would not automatically negate privacy expectations, but its narrow scope likely offers little protection for children's digital data.[237] These indirect pathways remain largely unregulated, offering law enforcement ready access to extensive information about young people's lives.

a. Commercial Third Parties

Policing agencies increasingly work with private sector actors to purchase data, avoiding subpoenas, court orders, and/or warrants.[238] This

231. CAL. PENAL CODE § 13650 (West 2025).

232. *See* CAL. CIV. CODE §§ 1798.100–99.100 (West 2025) (California Privacy Rights Act). CA has also created a Privacy Protection Agency. *See* CAL. BUS. & PROF. CODE §§ 22580–82 (West 2025) (Privacy Rights for California Minors in the Digital World Act).

233. California Survey of Police Department's Consent Search Policies Regarding Minor's Digital Devices (unpublished table) (on file with author).

234. Rachel A. Harmon, *The Problem of Policing*, 110 MICH. L. REV. 761, 762 (2012) (describing the immense authority police are granted by the state to impose harm).

235. Henning, *supra* note 130, at 1541.

236. Stacy Dewald, *"So, You Can Let Me Look at Your Phone?": Detectives Obtaining Consent to Search Cell Phones*, 5 J. CRIM. JUST. & L. (2022); *see, e.g.*, Ariel Spierer, *The Right to Remain a Child: The Impermissibility of the Reid Technique in Juvenile Interrogations*, 92 N.Y.U. L. REV. 1719 (2017).

237. *Id.*

238. Barry Friedman & Danielle Citron, *Indiscriminate Data Surveillance*, 110 VA. L. REV. 1351, 1364 (2024).

includes information on whom children associate with, where they go, what they read and search, and their medical data.[239] The personal data sold can range from data sets with anonymized trends to precise location data on specific individuals.[240] Equipped with artificial intelligence tools, law enforcement can procure immense amounts of data, organize it, and store it.[241]

Dozens of data brokers admit to selling minors' data—including reproductive health care and geolocation information.[242] Children's data holds special value to data brokers (estimated in the hundreds of billion dollars in the US alone).[243] This lucrative information is fed into algorithms to keep children hooked on platforms.[244] In addition, when agencies can buy their way around the Fourth Amendment, they often do so in a way that exacerbates existing biases in policing practices.[245]

Parents are data producers in this ecosystem. Surveillance technology companies aggressively market parental control apps as necessary to modern-day parenting, a social marker of responsible and loving parents.[246] To these companies, part of being a good parent is watching your children—always.

Along with phones, a wide range of other devices exist to surveil children. The non-removable AngelSense tracker device allows parents to "listen-in" to their child's day anytime, and see what the child has been up

239. *Id.*

240. Anonymizing data does little to protect it: researchers were able to correctly identify 99.8 percent of Americans from the data points. Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye, *Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models*, 10 NAT. COMMC'NS., 2019, art. no. 3069, at 1, https://www.nature.com/articles/s41467-019-10933-3 [https://perma.cc/9QWH-E3HL].

241. *See* Friedman & Citron, *supra* note 238, at 1356.

242. Suzanne Smalley, *Dozens of Data Brokers Disclose Selling Reproductive Healthcare Info, Precise Geolocation and Data Belonging to Minors*, THE RECORD (Mar. 8, 2024), https://therecord.media/dozens-of-data-brokers-disclose-selling-info-on-kids-geolocation-data-reproductive-health [https://perma.cc/J4FE-BM79].

243. Tehila Minkus, Kelvin Liu & Keith W. Ross, *Children Seen but Not Heard: When Parents Compromise Children's Online Privacy*, PROC. 24TH INT'L CONF. ON WORLD WIDE WEB (May 18, 2015).

244. Press Release, House Comm. on Energy & Com., Protecting Kids' Privacy with a National Data Privacy and Security Standard (May 8, 2023), https://energycommerce.house.gov/posts/protecting-kids-privacy-with-a-national-data-privacy-and-security-standard [https://perma.cc/8MY7-DW5Q].

245. *See* EMILE AYOUB & ELIZABETH GOITEIN, BRENNAN CTR. FOR JUST., CLOSING THE DATA BROKER LOOPHOLE (2024), https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole [https://perma.cc/68M2-9UTU].

246. Gary T. Marx & Valerie Steeves, *From the Beginning: Children as Subjects and Agents of Surveillance*, 7 SURVEILLANCE & SOC'Y 192 (2010), https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/4152/4155 [https://perma.cc/PCR8-ZAAV].

to with diary logs that input data every thirty seconds.[247] Parents might have their teens install the "Drive Safe & Save App" to collect data on their driving and save money on auto insurance, or monitor their teen's driving habits with a dashcam marketed as a "constant observer," creating responsible driving "because there's always an eye on them."[248] Many parents purchase parent control phones and other devices with genuine concern for their child's well-being and safety.[249] At the same time, parents report unease with these decisions. Due to cell phones' compact size and the tendency to carry them around all the time, parents find smartphones (as compared to televisions or computers) particularly difficult to monitor.[250]

It is no surprise that family protection apps, like Life360, are extremely popular. Life360 allows family members to share their locations, messages, and monitor family members' movements.[251] As of November 2024, Life360 had 76.9 million active users, a sixty-four percent increase from the previous year.[252] More than ten percent of Americans have used the app.[253] Life360 has sold children's data, with nearly twenty percent of their annual revenue coming from data sales.[254] Data brokers then readily share this information with law enforcement.[255]

247. Katie McEntire & Cathy Habas, *Best GPS Trackers and Tracking Devices for Kids in 2025*, SAFEWISE (Mar. 26, 2024), https://www.safewise.com/resources/wearable-gps-tracking-devices-for-kids-guide/ [https://perma.cc/68ZB-6KZQ].

248. *Teen Cams: What are the Benefits of Dashcams for Teenage Drivers and Parents?*, VANTRUE (Nov. 6, 2023), https://www.vantrue.com/blogs/news/dashcams-for-teens [https://perma.cc/6RQS-A235]; Matthew Collister, *State Farm Drive Safe and Save Review*, TIME (Oct. 14, 2024), https://time.com/personal-finance/article/state-farm-drive-safe-and-save-review/ [https://perma.cc/X4XT-QVYA] ("An opportunity for teen drivers or those with poor credit to save money on their car insurance").

249. Press Release, Ipsos, Over Four in Five Parents Cite Safety and Peace of Mind as the Top Reasons for Parents Allowing Children to Have Cell Phones (Aug. 17, 2010), https://www.ipsos.com/en-us/over-four-five-parents-cite-safety-and-peace-mind-top-reasons-parents-allowing-children-have-cell [https://perma.cc/4WSU-RPKQ].

250. Jörg Matthes, Marina F. Thomas, Anja Stevic & Desirée Schmuck, *Fighting Over Smartphones? Parents' Excessive Smartphone Use, Lack of Control Over Children's Use, and Conflict,* 116 COMPUTS. HUM. BEHAV., 2021, art. no. 106618.

251. *What Does Life360 Do?* LIFE360, https://www.life360.com/learn/what-does-life360-do/ [https://perma.cc/SY4L-VLYL].

252. Press Release, Life360, Life360 Reports Record Q3 2024 Results (Nov. 12, 2024), https://investors.life360.com/news-releases/news-release-details/life360-reports-record-q3-2024-results [https://perma.cc/ GUC7-2JT2].

253. Chloe Taylor, *Gen Z's Latest Tech Craze Is Tracking Each Other's Exact Whereabouts: 'It's Exploded into a Cool Thing to Do'*, FORTUNE (Sept. 12, 2023, 4:51 AM), https://fortune.com/2023/09/12/gen-z-find-my-friends-life360-location-tracking-privacy-safety/ [https://perma.cc/EJW3-6KFM].

254. Jon Keegan & Alfred Ng, *The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users*, THE MARKUP (Dec. 6, 2021, 8:00 AM), https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user [https://perma.cc/X5YQ-E2X2].

255. *See* Friedman & Citron, *supra* note 238, at 1355.

Against this backdrop, numerous states are taking up the issue of child online safety, requiring platforms to incorporate parental surveillance into tech platforms as a solution.[256] These bipartisan proposals, in Maryland, California, and Utah (which has passed its bill into law) include parental access to the content and interactions of children's accounts.[257] Thus, both social pressures and legislation are acting together to normalize, and even require surveillance over children online.

The private architecture of parents surveilling children is multifaceted.[258] While critiques abound, sharing data between parents and children in its most positive form may create freedom, convenience, safety, and even connection within the relationship.[259] Some evidence suggests parental monitoring is associated with less sexual risk and substance use, and better mental health.[260] Children's views on parental surveillance vary.[261] However, what is increasingly clear is that these tools, intended by parents for use within their own home and their private relationship with their child, inadvertently provide information to third parties, and thus, the state as well.

256. Alfred Ng, *Where Parental Snooping Is Becoming the Law,* POLITICO (Apr. 11, 2023, 1:50 PM), https://www.politico.com/news/2023/04/11/social-media-privacy-parents-kids-00091400 [https://perma.cc/GX6E-BDJX].

257. Similar proposals have been introduced at the federal level. *See, e.g.*, Kids Online Safety Act, S. 1409, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/senate-bill/1409/text [https://perma.cc/X2BE-JHRF]; Kids Off Social Media Act, S. 278, 119th Cong. (2025), https://www.congress.gov/119/bills/s278/BILLS-119s278rs.xml [https://perma.cc/M7H9-3ZRC].

258. These are issues I hope to fully explore in future work.

259. *See, e.g.*, DAVID S. BICKHAM, ELIZABETH HUNT, KRISTELLE LAVALLEE COLLINS & JILL R. KAVANAUGH, BOS. CHILD.'S DIGIT. WELLNESS LAB, CHILDREN'S FIRST CELL PHONES: PARENTS' PERSPECTIVES ON RISKS AND BENEFITS (2021), https://digitalwellnesslab.org/pulse-surveys/childrens-first-cell-phones-parents-perspectives-on-risks-and-benefits/ [https://perma.cc/MA46-47WX] (reporting connection and safety as primary motivators for child cell phones).

260. *See Parental Monitoring*, CTR. FOR DISEASE CONTROL (Nov. 22, 2024), https://www.cdc.gov/healthy-youth-parent-resources/positive-parental-practices/parental-monitoring.html [https://perma.cc/K56Y-N7JJ].

261. *See* The Learning Network, *What Students Are Saying About Parental Surveillance, Living Without Wi-Fi and Vibrant Youth*, N.Y. TIMES (Mar. 19, 2020), https://www.nytimes.com/2020/03/19/learning/what-students-are-saying-about-parental-surveillance-living-without-wi-fi-and-vibrant-youth.html [https://perma.cc/8R42-44JF]. For a more negative take from children on mobile apps for parental control, see Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J. LaViola Jr. & Pamela J. Wisniewski, *Safety vs. Surveillance: What Children Have to Say about Mobile Apps for Parental Control*, CHI CONF. ON HUM. FACTORS COMPUTING SYS., Apr. 2018, at 1–14, https://www.eecs.ucf.edu/~jjl/pubs/pn1838-ghoshA.pdf [https://perma.cc/VW5A-6BU3].

b. School Surveillance

Most students today receive school-provided laptops or tablets, another source of surveillance of young people.[262] These devices have third party commercial software installed that (1) alerts school officials when students access objectionable materials and (2) constantly monitors students' online activities, even when they are at home and on the weekends.[263] Danielle Citron calls such continuous monitoring "security theater," fostering an illusion of protection, without actual evidence of increased safety.[264] And while schools carry out the surveillance, the direct transmission of information from schools to law enforcement, and the sale of student's data to data brokers, both contribute to the policing of children's data.

Generally, parents are given little notice or opportunity to object to surveillance tools.[265] Those who try to opt out face many hurdles that effectively compel families to agree to devices loaded with third party EdTech services.[266] Although the Family Educational Rights and Privacy Act (FERPA) forbids schools from disclosing student information without parental consent, there are exceptions that can be exploited—including characterizing EdTech services as "school officials" to allow sharing student information with them directly.[267] Schools can also freely send information to law enforcement, which when characterized as a "law enforcement record," is explicitly excluded from the definition of education records under FERPA.[268]

EdTech companies employ content moderators to track students' activities. These content moderators usually contact school officials. But particularly outside school hours, moderators directly alert law enforcement.[269] These alerts can trigger a cascade of disciplinary events, from suspension to criminal legal system involvement, particularly

262. *School Pulse Panel: Surveying High-Priority, Education-Related Topics*, NAT'L CTR. FOR EDUC. STATISTICS (2025), https://nces.ed.gov/surveys/spp/results.asp [https://perma.cc/2P9X-9YC8] (choose "Technology" dropdown; then choose "2023–2024") (In the 2023–24 school year, ninety-five percent of public schools provide digital devices (laptops, tablets, etc.) to students who need them).

263. *See* Citron, *supra* note 7, at 1451–52.

264. *Id.* at 1465.

265. *Id.* at 1453.

266. *Id.* at 1454.

267. *Id.* at 1467; *see also* Fanna Gamal, *The Private Life of Education*, 75 STAN. L. REV. 1315, 1318 (2023).

268. 34 C.F.R. § 99.8(b)(1) (2025). Law enforcement unit records are not protected by FERPA because they are specifically excluded from the definition of "education records."

269. Priya Anand & Mark Bergen, *Big Teacher Is Watching: How AI Spyware Took Over Schools*, BLOOMBERG: BUSINESSWEEK (Oct. 28, 2021, 4:00 AM), https://www.bloomberg.com/news/features/2021-10-28/how-goguardian-ai-spyware-took-over-schools-student-devices-during-covid [https://perma.cc/SJL6-X4S7].

affecting students of color.[270] These monitoring systems also may "out" LGBTQ+, undocumented, and pregnant individuals—groups facing increasing criminalization post-*Dobbs*. Students from marginalized groups may not have personal devices to use. Their school issued device may be their only connection to online health and educational resources. EdTech data creates an indirect route for law enforcement to obtain student data, legitimized through parental consent.[271]

B. Harms of Data Collection

The state justifies consensual searches initiated by law enforcement through the public interest in solving crimes. Indeed, the Supreme Court in *Schneckloth v. Bustamonte* believed that results of consent searches can "yield [the] necessary evidence for the solution and prosecution of crime;" so, the Court held, individuals do not need to be explicitly informed of their right to refuse a search.[272] However, consent searches fall short of the Court's promises of producing "important and reliable evidence," and instead cause the following harms.[273]

1. Decreased Public Safety

Consent searches may not increase public safety or yield useful crime-solving information. Studies across multiple jurisdictions reveal that these searches rarely yield useful evidence or lead to arrests, despite law enforcement's anecdotal claims to the contrary.[274] The low hit rate from

---

270. *See* Michael Heise & Jason P. Nance, *To Report or Not to Report: Data on School Law Enforcement, Student Discipline, Race, and the "School-to-Prison Pipeline*,*"* 55 U.C. DAVIS L. REV. 209, 212 (2021).

271. Aaron X. Sobel, Note, *End-Running Warrants: Purchasing Data Under the Fourth Amendment and the State Action Problem*, 42 YALE L. & POL'Y REV. 176, 177 (2023) (noting that this violation of children's privacy is likely not cognizable under the Fourth Amendment because data brokers' purchases are considered action by a private entity, not government action).

272. Schneckloth v. Bustamonte, 412 U.S. 218, 243 (1973).

273. *Id.* at 227.

274. A recent study in five states found no discernible relationship between consent searches and crime during automobile stops. *See* Megan Dias, Derek A. Epp, Marcel Roman & Hannah L. Walker, *Consent Searches: Evaluating the Usefulness of a Common and Highly Discretionary Police Practice*, 21 J. EMPIRICAL LEGAL STUD. 35, 35 (2024). A study in D.C. of the Metropolitan Police Department found that only 9.5 percent of consent searches during an eighteen-month period retrieved any evidence of a crime, and only 2.3 percent resulted in seizure of a gun. *See* D.C. POLICE REFORM COMM'N, DECENTERING POLICE TO IMPROVE PUBLIC SAFETY: A REPORT OF THE DC POLICE REFORM COMMISSION 105 (2021), https://dccouncil.gov/wp-content/uploads/2021/04/Police-Reform-Commission-Full-Report.pdf [https://perma.cc/N5SB-AYGL]. Similar studies in Nashville and California also found traffic stops to rarely yield evidence of serious crimes. *See* N.Y.U. POLICING PROJECT, AN ASSESSMENT OF TRAFFIC STOPS AND POLICING STRATEGIES IN NASHVILLE 10,

consent searches means that agencies using this strategy do not find more contraband or make more arrests than agencies that do not.[275] Even if digital consent searches proved more effective than traditional consent searches—a proposition unsupported by current evidence and unlikely given the broader pattern of consent searches—the substantial harms would still outweigh any potential benefits. These so-called consent searches increase distrust between police and communities they serve and can be dangerous for officers and drivers alike.[276] The impact falls disproportionately on Black and brown individuals, who face the highest rates of stops and consent searches—leading scholars to characterize the consent doctrine as "the handmaiden of racial profiling."[277] For young people, who are still forming their views of law enforcement, the coercive techniques used to obtain consent particularly undermine procedural justice and trust.[278]

2. Increased Criminalization of Children

Easy access to digital evidence could create a net-widening effect of youth entering the carceral system. Casual searches of phones may lead to criminal consequences for minor infractions, like violating curfew, skipping school, and running away from home.[279] Location data, pictures, and text messages provide powerful evidence to prove minor offenses. These minor

https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5bf2d18d562fa747a554f6b0/1542640014294/Policing+Project+Nashville+Report.pdf [https://perma.cc/J6VV-6CMP]; *see also* Magnus Lofstrom, Alexandria Gumbs & Brandon Martin, *Racial Disparities in California Law Enforcement Stops*, PUB. POL'Y INST. OF CAL. (Dec. 3, 2020), https://www.ppic.org/blog/racial-disparities-in-california-law-enforcement-stops [https://perma.cc/ FMK6-UT4D].

275. Derek Epp, Hannah L. Walker, Megan Dias & Marcel Roman, *'Consent' Searches Don't Stop Drug Trafficking. They Threaten Privacy Rights*, SCI. AM. (Feb. 29, 2024), https://www.scientificamerican.com/article/consent-searches-dont-stop-drug-trafficking-they-threaten-privacy-rights/ [https://perma.cc/6XXZ-6ANZ].

276. *Why Limit Pretextual Stops?*, N.Y.U. POLICING PROJECT, https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/645b9ea85e3f9a7712b2b810/1683725992612/Why+Limit+Pretextual+Stops.pdf [https://perma.cc/5URS-7KXU]. I was one of the authors of this document while employed as the Director of Legislative Initiatives at the Policing Project.

277. Emma Pierson et al., *A Large-Scale Analysis of Racial Disparities in Police Stops Across the United States*, 4 NATURE HUM. BEHAV. 736, 736, 742, 744–45 (2020), https://www.nature.com/articles/s41562-020-0858-1 [https://perma.cc/7WTP-4RGA]; George C. Thomas III, *Terrorism, Race and a New Approach to Consent Searches*, 73 MISS. L.J. 525, 542 (2003).

278. Jacinta M. Gau, *Consent Searches as a Threat to Procedural Justice and Police Legitimacy: An Analysis of Consent Requests During Traffic Stops*, 24 CRIM. JUST. POL'Y REV. 759, 759–77 (2012); *see* OFF. OF JUV. JUST. & DELINQ. PREVENTION, INTERACTIONS BETWEEN YOUTH AND LAW ENFORCEMENT 12 (2018), [https://perma.cc/QM6S-EEM9] (available at archived link only).

279. *Just Kids: When Misbehaving Is a Crime*, VERA (Aug. 2017), https://www.vera.org/when-misbehaving-is-a-crime [https://perma.cc/X8EA-JZNE].

offenses pose little to no risk to public safety but push more children into the system.[280]

An intersectional lens reveals children of color are more vulnerable to harms of policing and punishment.[281] They are more likely to be searched.[282] They are more likely to be included in digital registries.[283] Additionally, normal adolescent behavior by children of color is more likely to be characterized as a criminal offense.[284] Cellphone extractions are frequently conducted for drug crimes, an offense exhibiting some of the most extreme racial disparities in enforcement.[285] It is likely digital evidence will be weaponized at higher rates against Black, Latinx, and Native children.

3. Developmental Harms to Privacy

Policing children's devices harms children's self-development during a time when they are particularly vulnerable. As Danielle Citron has written, children require intimate privacy, "the extent to which others have access to and information about [their] bodies, minds, health, sex, sexual orientation, gender identity, and close relationships."[286] Intimate privacy is "especially important for children" to thrive as they navigate the path to adulthood.[287]

Unlike the past, when children could explore ideas in books and libraries without online tracking, today's youth face unrelenting surveillance that

280. *See id.* ("[T]he very experience of being in court increases the likelihood that kids will engage in future criminal activity.").

281. *See, e.g.*, Ana Lilia Campos-Menzo, Marisol Flores, Denise Perez, Zoe Halpert & Kevin Zevallos, *Unjustified: Youth of Color Navigating Police Presence Across Sociospatial Environments*, 10 RACE & JUS. 297, 297 (2020) ("Hyper-surveillance in marginalized communities places Brown and Black boys at a high risk of involuntary police contact.").

282. *See*, *e.g.*, IAN AYRES & JONATHAN BOROWSKY, ACLU OF S. CAL., A STUDY OF RACIALLY DISPARATE OUTCOMES IN THE LOS ANGELES POLICE DEPARTMENT 5–9, 16–18 (2008), http://www.scribd.com/doc/99227597/A-Study-of-Racially-Disparate-Outcomes-in-the-Los-Angeles-Police-Department [https://perma.cc/6TPV-GK8H] (finding that African Americans and Hispanics are more likely to be stopped and searched by the Los Angeles Police Department but these searches are less likely to yield evidence than searches of whites); *see also* Andy Alford & Tony Plohetski, *Traffic Stop Data Hint at Racial Bias: Austin Police Numbers Show Minorities More Likely to Be Searched, Whites More Likely to Have Contraband,* AUSTIN AM.-STATESMEN, Mar. 16, 2003 at A1; ALEXANDER WEISS & DENNIS P. ROSENBAUM, UNIV. OF ILL. AT CHIC. CTR. FOR RSRCH. IN L. & JUS., ILLINOIS TRAFFIC STOPS STATISTICS STUDY: 2008 ANNUAL REPORT 2 (2009), http://www.dot.state.il.us/travelstats/ITSS%202008%CC20Annual%20Report.pdf [https://perma.cc/C2ZZ-WQX4].

283. *See, e.g.*, YOUTH JUST. COAL., TRACKED AND TRAPPED: YOUTH OF COLOR, GANG DATABASES AND GANG INJUNCTIONS 8 (2012), https://youthjusticela.org/wp-content/uploads/2012/12/TrackedandTrapped.pdf [https://perma.cc/3SU3-WGYY] (explaining 86 percent of CalGang is Black and Latino individuals).

284. Kristin Henning, *Criminalizing Normal Adolescent Behavior in Communities of Color: The Role of Prosecutors in Juvenile Justice Reform*, 98 CORNELL L. REV. 383, 403–04 (2013).

285. *See* KOEPKE ET AL., *supra* note 221, at 45.

286. Citron, *supra* note 7, at 1444.

287. *Id.*

chills their ability to develop and express themselves without shame or judgment. Critics may contend that modern adolescents do not care about privacy.[288] In reality, there are numerous indications young people do care about privacy. Survey data shows that younger respondents value privacy at similar rates to older respondents, though their conceptualization of privacy differs slightly from adults. [289] This is because privacy enables identity formation, creative expression, and autonomy.[290]

In contrast, ongoing surveillance chills activity, stifles curiosity, and leads to self-censorship. For children, surveillance instills a sense of mistrust and suspicion, conditions that can ultimately bred the very misbehavior that authorities are seeking to prevent.[291] When children feel their every move is watched and judged, they may choose to act out as a form of rebellion against being "treated like they are doing [it] anyway."[292] These chilling effects extend beyond the surveilled child to their peer relationships. A phone search exposes not just the target child's data but also their friends' activities, messages, and photos—potentially deterring peers from associating with each other. Police search and seizure of a phone represents one of the greatest intrusions that can take place.

4. Permanent Records

The virtually unlimited data retention capabilities of modern storage systems enable law enforcement to conduct searches with permanent consequences. This permanence presents special risks for children, whose digital footprints may persist long into adulthood. Our legal system recognizes that children are vulnerable, can change, and deserve a clean slate. Children are different from adults: This principle echoes throughout the Court's jurisprudence on juveniles, starting with *Roper v. Simmons*.[293]

288. *See* State v. Gutierrez, 482 P.3d 700, 709 (N.M. 2020) (arguing marital privilege is no longer necessary because privacy is no longer an esteemed value).

289. Jay Stanley, *Do Young People Care About Privacy?*, ACLU (Apr. 29, 2013), https://www.aclu.org/news/privacy-technology/do-young-people-care-about-privacy [https://perma.cc/A9H8-GM98]; Benjamin Shmueli & Ayelet Blecher-Prigat, *Privacy for Children*, 42 COLUM. HUM. RTS. L. REV. 759, 761 (2011).

290. *See* Shmueli & Blecher-Prigat, *supra* note 289, at 772.

291. Emmeline Taylor, *I Spy with My Little Eye: The Use of CCTV in Schools and the Impact on Privacy*, 58 SOCIO. REV. 381 (2010).

292. *Id.* at 392.

293. 543 U.S. 551, 569 (2005) (recognizing adolescents' heightened susceptibility to external influences, particularly from peers); *see also* Graham v. Florida, 560 U.S. 48, 48–49 (2010) (affirming the reasoning found in *Roper*); J.D.B. v. North Carolina, 564 U.S. 261, 262 (2011) ("A child's age is far 'more than a chronological fact.'" (quoting Eddings v. Oklahoma, 455 U.S. 104, 115 (1982))); Miller v. Alabama, 567 U.S. 460, 461 (2012) (asserting that previous rulings have established a constitutional distinction between juveniles and adults).

This recognition explains key protections in the system, including closed hearings and record sealing policies.[294]

But rather than engage in narrow, particularized searches, police who search phones often "dump" them, capturing the entirety of the device's contents.[295] Comprehensive dossiers documenting every interaction, location, and relationship, fundamentally undermine these core philosophical ideals of providing rehabilitative chances and a clean slate. It is one thing for a parent or school to have oversight of a child's device. Even this surveillance can impact a child, with costs to free expression, well-being, and equality.[296]

But it metamorphosizes into an entirely different harm when law enforcement receives data, leading to criminal consequences. Digital information can be stored forever without degradation, with previously innocuous information revealing new insights in the future. Paradoxically, while all states have procedures for juvenile record expungement or sealing, digital search data can persist indefinitely on law enforcement servers, as most agencies lack data deletion policies.[297] Perpetual searches with permanent retention cause enduring harms for children.

5. Databases

An additional harm results when individual data is aggregated, creating databases. Law enforcement has long gathered and stored data to thwart crime. But MDFTs and other modern technologies mean agencies can now seamlessly catalog a child's contacts and movements and connect it with information from other children and adults.

Databasing children can have a chilling effect on their speech and movement that are particularly severe given their stage of emotional and intellectual development.[298] Compounding this issue, these databases have

294. *Automatic Expungement of Juvenile Records*, NAT'L CONF. OF STATE LEGIS. (Jan. 4, 2024), https://www.ncsl.org/civil-and-criminal-justice/automatic-expungement-of-juvenile-records [https://perma.cc/LW8N-FEFM].

295. Dewald, *supra* note 236, at 11; *see also* Taylor Applegate, Note, *Mobile Device Forensic Tools: A Help or a Hindrance to Constitutional Cellphone Searches?*, 35 STAN. L. & POL'Y REV. 284, 288 (2024) (discussing how the plain view doctrine has been interpreted to allow authorities to "rummage" through a mobile device).

296. *See* Citron, *supra* note 7 at 1456.

297. Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773, 804 (2015) (big data analytics and bulk data collection techniques have led to the government's impulse to collect everything and keep it forever).

298. *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013) (explaining how surveillance chills the exercise of civil liberties); Lindsey Barrett, *Ban Facial Recognition Technologies for Children—and for Everyone Else*, 26 B.U. J. SCI. & TECH. L. 223, 280 (2020) (describing the particularized effects of surveillance on children).

historically been riddled with errors and questionable information, often lacking auditing procedures. Even with access restrictions in place, the potential for abuse remains high: Officers have misused their privileges in the past.[299] Perhaps most concerning is that historically the police power to label and database individuals has been wielded to surveil, repress, and persecute vulnerable communities and dissenting voices.[300]

Digital consent searches cause great harm with few, if any, benefits. These searches significantly harm children's development and privacy. Neither the Fourth Amendment nor parental authority protect children from consensual digital searches. In Part III, this Article provides legal tools for mitigating the harms described above.

III. LEGAL TOOLS FOR MITIGATION

This Article has advanced two key arguments regarding digital searches of children's devices. First, law enforcement too often relies on a child's consent, despite significant concerns regarding its voluntariness. Second, relying on parental consent on behalf of children is problematic as well. Parents are subject to coercive pressures from law enforcement and may have significant conflicts of interest. Additionally, current doctrine permits parental consent to override a child's objection to the search. This view stems at least partly from outdated notions of child coverture, which constructed children as mere extensions of their parents. It is a concept increasingly at odds with our modern understanding of children's autonomy and privacy interests.

To address these issues, this Article proposes both legal arguments and legislative reforms. First, the analysis turns to existing case law to argue against parental and child consent for searches of children's data. The Article then proposes three policy recommendations to better protect children's digital privacy. The first recommendation, generally abolishing digital consent searches of minors, responds to the harms of direct searches. The second, regulating third party collection of data, focuses on the indirect methods law enforcement use to collect children's data. Finally, the third recommendation to create comprehensive policies around data use, retention, and expungement, applies to both methods of collection.

---

299. *Police Sometimes Misuse Confidential Work Databases for Personal Gain*: *AP*, CBS (Sept. 30, 2016, 8:59 AM), https://www.cbsnews.com/news/police-sometimes-misuse-confidential-work-databases-for-personal-gain-ap/ [https://perma.cc/XS6L-YS5G].

300. Jessica Brandt, *When Democracies Employ Repressive Technology, What are the Repercussions?*, GLOB. POL'Y J. (May 10, 2023), https://www.globalpolicyjournal.com/blog/10/05/2023/when-democracies-employ-repressive-technology-what-are-repercussions [https://perma.cc/D3M9-JAG5].

A. Legal Argument

In light of the unique privacy concerns surrounding digital evidence, defense attorneys should consider a new approach when challenging device searches based on consent. This Section develops two complementary constitutional arguments: First, courts should apply heightened scrutiny to a minor's direct consent to digital searches, borrowing from Fifth Amendment voluntariness principles; second, parental consent should be deemed insufficient to authorize searches of a child's digital information under Fourth Amendment protections.

When evaluating a child's consent to digital searches, courts should apply a more rigorous voluntariness analysis—one informed by their own approach to custodial interrogation.[301] In that context, courts have long acknowledged that children's developmental immaturity can render them especially vulnerable to coercion. Yet in the consent context, courts often relegate age to a box to be checked, rather than grappling with its full significance. A youth-centered framework would correct this imbalance by placing adolescents' cognitive and emotional differences at the heart of the inquiry. This reform would bring consent doctrine in line with the Supreme Court's recognition in *J.D.B. v. North Carolina* that children are more susceptible to outside pressures than adults—a principle that logically applies with equal force when officers request access to a child's digital life as when they question a child about suspected wrongdoing.[302] A youth-centered consent framework would recalibrate voluntariness by explicitly considering the coercive weight of authority from the reasonable youth's perspective, creating a strong presumption against voluntary consent by minors.

Even when children don't consent directly, law enforcement often circumvents this issue by obtaining parental permission instead. However, this alternate pathway deserves equal constitutional scrutiny. The challenge to parental consent builds upon existing Fourth Amendment precedent establishing digital devices as constitutionally unique. The Court has already made clear that cellphones and digital evidence are fundamentally different from other types of evidence, creating a special categorical exception to the search-incident-to-arrest rule. In *Riley,* the Court placed cell phones on unique constitutional footing because "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person" and "ha[ve] several interrelated consequences

301. *See supra* note 132 and accompanying text.
302. *See* 564 U.S 261, 272 (2011).

for privacy."[303] The *Riley* court found even an arrest is insufficient to justify probing into the contents of the individual's phone because of the privacy interest at hand.[304]

Based on the cell phone's unique status already established in the law, the court should consider a categorical exception limiting parental consent for searches of children's digital information. Precedent exists for creating an exception in this context: Limitations to parental consent have been recognized for highly personal evidence, including a child's body and their DNA.[305] A similar exception should be extended to children's digital information given the unique privacy concerns and highly personal nature of the information.

This approach finds support in case law. For instance, in a case of first impression, the Oregon Court of Appeals reasoned that the Fourth Amendment does not permit the warrantless DNA search of the body of a child based on parental consent, even if the child acquiesces.[306] The state, citing *Randolph*, argued that because parents can consent to searches of their child's room and property, they can consent to a DNA search.

The court acknowledged the rationale of *Randolph's* dicta, that "valid third-party consent depends either on the third party's common authority over the property based on her or his own property interest, or, alternatively, on the application of agency principles," but squarely rejected such reasoning, finding that "a child is not the property of her or his parents (or anyone else), and we are aware of no cases holding that a parent has a property interest in a child."[307]

Extending the rationale from *In re H.K.D.S.*, the digital device should be conceptualized to be more like the child's body or DNA and less like a bedroom or backpack. Searches of digital devices share many qualities with the intrusiveness of the search of the body. This notion has found traction in case law, with courts drawing parallels between digital and body searches. The Ninth Circuit in *United States v. Cotterman* equated a forensic search of an electronic device to a "computer strip search."[308] The Court reasoned that "[s]uch a thorough and detailed search of the most intimate details of one's life is a substantial intrusion upon personal privacy and

303. *See* Riley v. California, 573 U.S. 373, 393–94 (2014).

304. *Id.* at 373.

305. RESTATEMENT OF CHILDREN AND THE LAW § 12.11 (AM. L. INST., Tentative Draft No. 3, 2021); *In re* H.K.D.S., 469 P.3d 770 (Or. Ct. App. 2020) (parental consent with child acquiescence does not amount to voluntary consent); Bala, *supra* note 22, at 489.

306. *See H.K.D.S.*, 469 P.3d at 774.

307. *Id.* at 776 (quoting State v. Bonilla, 366 P.3d 331 (Or. 2015)).

308. 709 F.3d 952, 966 (9th Cir. 2013).

dignity."[309] The Court in *Riley* similarly recognized digital evidence as fundamentally different from any other ordinary physical item.[310] And at least one court in the context of a border search has argued that a cell phone search is *even more intrusive* than a body search.[311]

Comparing the digital device to the body will be increasingly relevant in the modern age: Scholars have written of "digital persons" and "digital subjects"—entities constructed from the vast amounts of data available about each of us.[312] The emerging "Internet of Bodies" (IoB) technology will meld digital data and human bodies together, where separating the two may become impossible.[313] Cell phones and similar devices may become inseparable from the body, with data trails from the body eventually becoming a search of the body itself.[314] But even with today's technology, we must recognize cell phones are not mere containers or pieces of property, but instead an extension of the self—a perspective many adolescents already adopt.[315] This shift in understanding of smart devices more accurately recognizes the privacy and dignity interests at hand.

DNA, like cell phone data, enables police officers to reconstruct "the sum of an individual's private life."[316] And just as parental consent has been found to be insufficient to search the child's body or DNA, it should not be sufficient to justify the search of a cell phone.[317]

These judicial approaches offer several advantages: They require no legislative action, can adapt to evolving understandings of adolescent

309. *Id.*; *see also* N.Y. Bar Ass'n Comm. on Pro. Ethics, Formal Op. 2017-5 (2017) (discussing the protection of confidential client information when crossing the border).

310. *See* Riley v. California, 573 U.S. 373, 393 (2014).

311. *See* United States v. Smith, 673 F. Supp. 3d 381, 387 (S.D.N.Y. 2023).

312. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004); Olga Goriunova, *The Digital Subject: People as Data as Persons*, 36 THEORY, CULTURE & SOC'Y 125, 126 (2019).

313. *See, e.g.*, United States v. Sultanov, 42 F. Supp. 3d 258, 286 (E.D.N.Y. 2024) ("Until technology that can 'translate people's brain activity — like the unspoken thoughts swirling through our minds— into actual speech' meaningfully advances, reviewing the information in a person's cell phone is the best approximation government officials have for mindreading."); *see also* Maria Gomez De Sicart & Cristy Garratt, *The Next Generation of the 'Internet of Bodies' Could Meld Tech and Human Bodies Together,* CNBC TECH (Jun. 1, 2024, 09:40 AM), https://www.cnbc.com/2024/06/01/internet-of-bodies-could-meld-tech-and-human-bodies-together.html [https://perma.cc/4MTA-H5SH].

314. Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 589–592 (2017).

315. Coriena Davel, The Mobile Phone as an Extension of the Self: A Study Among Adolescents in a Secondary School (Feb. 2017) (Ph.D dissertation, University of South Africa), https://core.ac.uk/download/pdf/85157464.pdf [https://perma.cc/N9VK-UQRM]; Isabela Granic, Hiromitsu Morita & Hanneke Scholten, *Beyond Screen Time: Identity Development in the Digital Age*, 31 PSYCH. INQUIRY 195, 195–96 (2020) ("[Y]oung people—having grown up with tablets in their cribs and phones in their highchairs—no longer experience much of their digital, online interactions and physical, offline interactions as functionally distinct.").

316. Riley v. California, 573 U.S. 373, 394 (2014).

317. *See In re* H.K.D.S., 469 P.3d 770, 744 (Or. Ct. App. 2020).

development, and build on existing jurisprudence. Courts have already recognized children's diminished capacity in interrogation contexts and could logically extend this reasoning to searches.[318] However, judicial reforms face significant obstacles: Courts have historically been reluctant to create bright-line rules in Fourth Amendment cases, preferring "totality of circumstances" tests that often undervalue youth.[319] Additionally, the process is incremental and jurisdiction-specific, and courts may defer to police expertise in investigative matters despite developmental science.

Nevertheless, the constitutional principles and precedents already exist to support this more protective framework for children's digital privacy. Defense attorneys should aggressively advance both prongs of this approach, challenging both direct and parental consent as insufficient bases for digital searches of minors.

B. Legislative Reforms

The following recommendations both look to recognize children's data privacy, while also balancing legitimate safety concerns. Both Jane's story and J.P's case raise issues that cannot be easily dismissed. The creation of nude photographs put Jane at risk.[320] Similarly, the alleged bomb threat in J.P.'s case may have put many other students in danger.[321] Their cases highlight the challenges of navigating adolescent privacy against broader safety concerns.

This Article argues, however, that safety can be maintained, and indeed might be enhanced, without resorting to consent searches of minors' digital devices. The proposed recommendations take into account parents' roles in overseeing their children's safety, recognizing that parental mediation is sometimes sufficient to address many of the issues teenagers face while growing up. Thus, the recommendations below regulate third party and law enforcement access to children's data, rather than regulating parents directly.

These recommendations also recognize there may be times law enforcement should search a digital device. MDFTs are valuable tools in genuine emergencies and where the government has established probable

318. *See supra* note 132.

319. Ohio v. Robinette, 519 U.S. 33, 39 (1996) ("Reasonableness, in turn, is measured in objective terms by examining the totality of the circumstances. In applying this test we have consistently eschewed bright-line rules . . . ."); *see also* Georgia v. Randolph, 547 U.S. 103, 125 (2006) (Breyer, J., concurring) (suggesting that the Fourth Amendment uses the word "unreasonable" because bright-line rules do not "capture the ever changing complexity of human life").

320. *See* Willard, *supra* note 1.

321. *In re* J.P., 2018 WI App 66, ¶¶ 5–12, 384 Wis. 2d 415, 921 N.W.2d 529.

cause. They can be instrumental in solving serious crimes and exonerating individuals.[322] This proposal focuses on eliminating exploratory searches that are fishing expeditions to get information from innocent youth. It does not eliminate recognized exceptions to the Fourth Amendment, such as exigent circumstances, nor does it interfere with law enforcement's ability to seek and obtain a warrant.[323] Searches would remain permissible, but only after a warrant is obtained or a non-waivable consultation between the young person and an attorney takes place.

1. Generally Abolish Digital Consent Searches of Minors

Consent searches are notoriously bad at yielding evidence of serious crimes.[324] They carry significant harms, particularly when performed on minors.[325] Given the asymmetries of power and the dynamics between law enforcement and marginalized communities, it is a "simple truism that many people, if not most, will always feel coerced by police 'requests' to search."[326] Coercion undermines the validity of all types of searches; a more comprehensive reform would curb consent searches more broadly.

Legislative reform might present a more direct pathway to reform. Children and online privacy are currently experiencing a news moment, and reforms protecting children often have bipartisan, bicameral support.[327] Reforms initially proposed for children may create a chain of further reforms affecting the adult system as well.[328] This reform is a starting point,

322. In the process of regulating MDFTs and implementing safeguards against data retention, we must also recognize that public defenders also need access to MDFTs, but suffer from severe resource disadvantages. Kashmir Hill, *Imagine Being on Trial. With Exonerating Evidence Trapped on Your Phone.* N.Y. TIMES (Nov. 22, 2019), https://www.nytimes.com/2019/11/22/business/law-enforcement-public-defender-technology-gap.html [https://perma.cc/U2KQ-J5MD].

323. We should take Nathaniel Mensah's concerns seriously that traditional warrants do not do enough to protect individuals from digital searches, and there should be greater attorney involvement. *See* Mensah, *supra* note 203, at 1160–62; *see also* Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 1, 4 (2015) (arguing for use restrictions on non-responsive data seized during a digital search).

324. *See* Tokson, *supra*, note 122 at 1803, 1823.

325. *See* discussion *supra* Section I.B.

326. Marcy Strauss, *Reconstructing Consent*, 92 J. CRIM. L. & CRIMINOLOGY 211, 221 (2001).

327. Owen Tedford, *Federal and State Governments' Spotlight on Children's Online Privacy*, FORBES (Feb. 21, 2024, 8:35 PM), https://www.forbes.com/sites/owentedford/2024/02/21/childrens-online-privacy-in-the-spotlight/ [https://perma.cc/4CSM-JCLH].

328. Recognizing that the Court's jurisprudence has also made clear children are fundamentally different from adults, reforms often start with children. *Roper v. Simmons* abolished the death penalty for juveniles in 2005. 543 U.S. 551 (2005). Subsequent years have seen lessening use of the death penalty for adults, with only five states conducting executions and seven imposing new death sentences in 2023, the lowest number in twenty years. DEATH PENALTY INFO. CTR., THE DEATH PENALTY IN 2023: YEAR END REPORT (2023), https://deathpenaltyinfo.org/facts-and-research/dpic-reports/dpic-year-end-reports

and targets searches that cause greater and longer-lasting harms, as compared to traditional physical searches.

One legislative pathway is for states to eliminate consent-based digital searches of minors altogether, instead requiring officers to obtain warrants. This would follow the lead of jurisdictions that have already limited police authority to conduct consent searches during traffic stops and pedestrian encounters.[329] A categorical warrant requirement would recognize several realities: first, that minors are especially vulnerable to coercion, second, consent searches are often executed in a racially disparate fashion and yield limited evidence, and third, that digital searches contain incredibly intimate information. While the warrant process is not without its flaws—scholars have rightly criticized how easy they are to obtain—warrants nonetheless provide a procedural hurdle. Requiring a warrant could ensure that only searches officers deem necessary are carried out. Importantly, it would eliminate reliance on parents, which is not an adequate safeguard.

A second legislative pathway provides more flexibility for minors, particularly in cases where they are victims seeking help. Even in these cases, procedural safeguards are essential. Cases like Jane's illustrate that information initially obtained through consent, ostensibly to protect a minor, may later be used to prosecute that same individual.[330] An attorney consultation can help prevent such harms and protect the integrity of a child's consent.

Such a proposal aligns with a larger movement advocating for early access to counsel.[331] Precedent for employing this approach exists in California, where Senate Bills 395 and 203 mandate attorney consultation

---

/the-death-penalty-in-2023-year-end-report [https://perma.cc/PH2A-PQUF]. Restorative justice practices more palatable to pilot in the juvenile legal system have demonstrated efficacy when applied to adults as well. MARTIN WRIGHT & BURT GALAWAY, MEDIATION AND CRIMINAL JUSTICE: VICTIMS, OFFENDERS AND COMMUNITY 14–16 (1989) (describing the beginnings of the victim offender reconciliation movement in Kitchener, Ontario with young teenagers). Similarly, D.C.'s Incarceration Reduction Amendment Act, passed based on *Roper*, allows for resentencing for people who committed crimes before they were twenty-five. D.C. CODE § 24-403.03 (2024); *see The Second Look Amendment Act*, D.C. PUB. DEF. SERV., https://www.pdsdc.org/resources/client-resources/second-look-amendment [https://perma.cc/4V9Z-X548].

329. R.I. GEN. LAWS § 31-21.2-5(b) (2024) ("No operator or owner-passenger of a motor vehicle shall be requested to consent to a search . . . unless there exists reasonable suspicion or probable cause of criminal activity."); S.B. 429, 80th Legis. Assemb., Reg. Sess. (Or. 2019) (must be informed of right to refuse search). *Accord* COLO. REV. STAT. § 16-3-310 (2024); MINNEAPOLIS POLICE DEP'T, POLICY AND PROCEDURE MANUAL: § 9-202 WARRANTLESS SEARCHES (2024), https://www.minneapolismn.gov/media/-www-content-assets/documents/police/policies-pdfs/9-202-Warrantless-Searches.pdf [https://perma.cc/SMU6-S3CZ].

330. *See* Willard, *supra* note 1.

331. BRETT FISCHER, JOHANNA LACOE & STEVEN RAPHAEL, CAL. POL'Y LAB, PROVIDING EARLY LEGAL COUNSEL REDUCES JAIL TIME AND IMPROVES CASE OUTCOMES (2023), https://www.capolicylab.org/wp-content/uploads/2023/06/Providing-Early-Legal-Counsel-Improves-Outcomes.pdf [https://perma.cc/44AG-4CRD].

for minors before a custodial interrogation. An early research report studying implementation found a number of perceived benefits, without any negative impacts.[332] Some of these benefits included youth better understanding their rights, increased trust among youth and counsel, and better outcomes at detention hearings for the youth.[333] Notably, those surveyed also reported that police initiated fewer interrogations, as law enforcement decided that it was not worth their time to question youth since most were silent after consulting with an attorney.[334]

Requiring counsel before consensual searches might yield similar results to those observed in pre-interrogation attorney consultations. It may reduce the number of searches to those that are genuinely necessary. In instances where minors do want to consent, guidance from an attorney is beneficial in providing more informed decision-making regarding the long-term risks of the digital search.[335]

Rather than relying on parents as the "interested adult," a role research suggests may paradoxically increase the waiver of rights, supporting youth with early access to counsel empowers them to resist unwarranted law enforcement requests. Additionally, mandating counsel before a consensual search, rather than relying on parents' consent, would also address the problematic implications of the dicta in *Randolph*, which allows a child's explicit objection to a search to be overridden by the parent. The policy acknowledges that children have interests different from their parents, and those interests matter.

Extending the benefits of counsel to the search context also recognizes the police pressure that minors face goes beyond the context of custodial interrogations. The adult legal system's reliance on waiver and consent permeates criminal procedure, far beyond the spaces scholars have recognized thus far.[336] For children, the waiver of rights is often improperly legitimized through their parent's consent. Requiring a conversation with counsel instead is a crucial first step toward critically examining other ostensibly "voluntary choices" that the legal system currently relies upon parents to legitimize.

---

332. GENEVIEVE CITRIN RAY & JEANETTE HUSSEMANN, NORC, UNIV. OF CHI., EARLY ACCESS TO LEGAL COUNSEL FOR YOUTH: AN IMPLEMENTATION STUDY OF CALIFORNIA SENATE BILLS 395 AND 203, at 2 (Nov. 2023), https://www.defendyouthrights.org/wp-content/uploads/Early-Access-to-Legal-Counsel-for-Youth-Implementation-Study.pdf [https://perma.cc/ZXH2-966M].

333. *Id.*

334. *Id.* at 7.

335. *Id.* at 12.

336. Weisburd, *supra* note 149, at 1.

2. Regulate Third Party Collection of Data

Children's data is extremely vulnerable within the data brokerage ecosystem.[337] Commercial entities and EdTech companies sell children's information, and there is evidence schools are directly selling student data as well.[338] The public is generally unaware of these practices and the impact that data brokers can have on their lives.[339] All of this is exacerbated when law enforcement agencies obtain this data, compounding the privacy risks and civil liberties concerns for children.

The sale of data operates without sufficient oversight. Existing regulations includes a patchwork of statutes at the federal and state levels, as well as some voluntary industry self-regulation.[340] Since technology companies and law enforcement agencies operate across state lines, the solutions below will primarily focus on the deficiencies in current federal regulations, as they have the broadest impact on interstate data practices.[341]

At the federal level, FERPA and COPPA govern children's data privacy.[342] As noted in Part I, FERPA forbids schools from disclosing student information without parental consent. However, it has exceptions that can be easily exploited. School officials can be expansively defined to include EdTech companies, as student data can be disclosed to certified contractors without prior consent.[343] And once a record is classified as a law enforcement record, FERPA does not apply at all.[344] Similarly, COPPA requires companies to obtain "verifiable parental consent" before collecting

337. Pieter Arntz, *Data Brokers Admit They're Selling Information on Precise Location, Kids, and Reproductive Healthcare*, MALWAREBYTES LABS (Mar. 11, 2024), https://www.malwarebytes.com/blog/news/2024/03/data-brokers-admit-theyre-selling-information-on-precise-location-kids-and-reproductive-healthcare [https://perma.cc/9CZ5-YN7L] (children are more vulnerable and less aware of the potential risks associated with data processing).

338. ALISTAIR SIMMONS, DUKE SANFORD CYBER POL'Y PROGRAM, DATA BROKERS AND THE SALE OF STUDENTS' DATA: PRIVACY AND POLICY IMPLICATIONS—AND HOW STUDENTS FEEL ABOUT IT (2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/07/Data-Brokers-and-the-Sale-of-Students-Data-Simmons-2023.pdf [https://perma.cc/LX9K-QCCY].

339. Press Release, F.T.C., FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 18, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data [https://perma.cc/X5HA-KRJA].

340. *See generally* Florencia Marotta-Wurgler, *Self-Regulation and Competition in Privacy Policies*, 45 J. LEGAL STUD. S13 (2016). Industry self-regulation had been mainly in the form of the now-retired Student Privacy Pledge, which was not a law, but was legally enforceable by the Federal Trade Commission against its over 300 signatories. The Pledge also contained many loopholes preventing it from offering meaningful protection. *About the Pledge*, STUDENT PRIVACY PLEDGE (Apr. 25, 2025), https://studentprivacypledge.org/ [https://perma.cc/C5U2-S6PQ].

341. This is not to discount state efforts that do make a difference.

342. See *supra* Section II.A.2.b for problems flagged with FERPA, including the broad definition of school official and the exemption for law enforcement record.

343. 34 C.F.R. § 99.31 (2025).

344. *Id.* § 99.31(9)(ii)(B).

personal information from children under thirteen for commercial purposes.[345] Again, a number of loopholes have emerged—if the information is collected for a school purpose, COPPA would not apply.[346] If the child is over thirteen, COPPA also does not apply.[347] And of course, law enforcement use is an exception to COPPA.[348]

Notably, both of these federal statutes give parents full control over the governance of children's data. However, parent consent as a guardrail has been heavily criticized with regard to COPPA.[349] Parents are unlikely to understand or read boilerplate waivers and notice and consent forms.[350] As Zahra Takhshid argues, "new privacy initiatives at the federal level should also not rely primarily on parental consent but instead offer privacy protection laws that limit the overreach of EdTech companies."[351] Similarly, parent tracking apps count on parents not reading the terms and conditions.[352] These companies have enormous financial incentives to sell children's data.[353] In most cases, parents simply don't know this practice is occurring.

A number of federal proposals miss the mark in this way, focusing on providing more notice and choice.[354] For example, the American Privacy Rights Act would create a registry so the public can identify and track data brokers sharing.[355] However, as the American Law Institute identifies, most "commentary, scholarship, and empirical evidence suggests that traditional notice does not work."[356] If parents (and the American public in general) are

345. 15 U.S.C. § 6502(b)(1)(A)(ii).

346. *Id.* § 6502; Lesley Fair, *Testing, Testing: A Review Session on COPPA and Schools*, Federal Trade Commission Business Blog (Jan. 23, 2015), https://www.ftc.gov/business-guidance/blog/2015/01/testing-testing-review-session-coppa-schools [https://perma.cc/69L2-FYBA] (schools are not commercial operators).

347. 15 U.S.C. § 6501(1).

348. *Id.* § 6502(2)(E)(iv).

349. *See* Takhshid, *supra* note 20, at 1420; *see also* John Palfrey, Danah Boyd & Urs Gasser*How the COPPA, as Implemented, is Misinterpreted by the Public: A Research Perspective*, BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y (Apr. 28, 2011), https://cyber.harvard.edu/publications/2010/COPPA_Implemented_Is_Misinterpreted_by_Public [https://perma.cc/SGL2-TXSV].

350. *See* Takhshid, *supra* note 20, at 1421.

351. *Id.* at 1420.

352. Privacy Pillar, *Parental Surveillance Apps: Who's Tracking Whom?*, LINKEDIN (July 14, 2022), https://www.linkedin.com/pulse/parental-surveillance-apps-whos-tracking-whom-adzapier/ [https://perma.cc/V2CH-LS2R].

353. F.T.C., DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/HDW6-LTAW].

354. Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 36–38 (2021) (arguing that placing the onus of privacy protection solely on individuals is ineffective and unfair).

355. American Privacy Rights Act of 2024, H.R. 8818, 118th Cong. (2024), https://www.congress.gov/bill/118th-congress/house-bill/8818/text [https://perma.cc/DKY8-7V2T].

356. PRINCIPLES OF THE L.: DATA PRIVACY § 3 cmt. a (AM. L. INST. 2020).

not reading terms and conditions, requiring more of them will not solve the problem.

Instead, we should both strengthen COPPA and FERPA and actually regulate data brokers, with the goal of closing gaps in the law that allow schools and companies to aggregate and sell children's data. We should also eliminate the data broker loophole that allows government agencies, including law enforcement, to purchase children's data and avoid the requirements of the Fourth Amendment.

3. Enact Policies Around Data Use, Retention, and Expungement

Most law enforcement agencies operate without any restrictions to conducting digital data searches.[357] Without clear data use and retention policies, agencies have unchecked power to hold onto information indefinitely. Agencies can use this data to fuel police surveillance and build databases with aggregated information. Furthermore, federal and state laws often carve out exemptions or create shields, allowing surveillance technologies and databases to proceed in secret.[358] As a foundational principle, data protection policies need to exist and need to be public.[359]

Critically, the first step must be to limit the scope of how data is used. Instances of data sharing between agencies (e.g. between the juvenile legal system, family regulation system, immigration, etc.) heightens the chances that information collected can later be used against the child in unforeseen ways.[360] Combined with the current state of cloud-based data retention, existing without limits, data can be used as a tool to punish the child who is the subject of that information forever.

Data use and retention policies are especially important for children positioned as victims. When children and their parents consent to a search of their phone based on an assumption that the child is a victim, future data violations may thwart expectations as to how the data will be used.[361] Thwarted expectations erode autonomy "because [they] result[] in people's

357. This is a broader concern with government surveillance in general, which often operates secretly and without public knowledge or input. *See* Barry Friedman, *Lawless Surveillance*, 97 N.Y.U. L. REV. 1143, 1147 (2022) (arguing surveillance is without public transparency and is in need of legislative action).

358. Christina Koningisor, *Police Secrecy Exceptionalism*, 123 COLUM. L. REV. 615, 644–46 (2023).

359. Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827, 1827 (2015) ("Although police departments have internal rules, these rules are rarely made public or publicly debated.").

360. *See e.g.*, Washington, *Fammigration Web*, *supra* note 183, at 125 (noting the deep connections between the family regulation and immigration systems).

361. *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 849–53 (2022) (identifying thwarted expectations as a frequent symptom of privacy violations).

inability to make choices in accordance with their preferences." Consent for one purpose is not consent for another, despite courts' acceptance of consent even when individuals do not understand the full scope of what they are agreeing to.[362]

A number of examples demonstrate how data has been repurposed and subject to misuse. For example, in 2022, news broke that the San Francisco Police Department had used a woman's DNA—collected as part of a rape examination—to arrest her, positioning her as a defendant.[363] This practice of searching crime victims' DNA in unrelated criminal cases had reportedly been going on for seven years.[364] In a related disturbing trend, law enforcement agencies exploited newborn DNA—collected and databased to test for metabolic disorders at birth—for unrelated criminal investigations.[365] Not only do such actions violate autonomy interests, they also cause chilling effects, decreasing individual's participation in sexual assault reporting and public health programs respectively.[366]

These concerns transcend DNA to digital data, especially in teenage sexting cases, where categories of victim and defendant can blur. Children are particularly vulnerable to not understanding the long-term consequences of consenting to a data search. They, or their parents, come to law

362. *See* Richards & Hartzog, *supra* note 175, at 1478. Richards and Hartzog note that unwitting consent "can take at least three forms, including not understanding the legal agreement, not understanding the technology being agreed to, or not understanding the practical consequences or risks of agreement," which are all concerns with data collection by police. *Id.* at 1466; *see, e.g.*, State v. Rejholec, 2021 WI App 45, 398 Wis. 2d 729, 963 N.W.2d 121 (evidence supported finding that defendant's statements to police officer were voluntary, despite officer's use of false evidence, lies); United States v. Crawford, 372 F.3d 1048, 1060 (9th Cir. 2004) ("Trickery, deceit, even impersonation do not render a confession inadmissible.").

363. *See, e.g.*, Azi Paybarah, *Victim's Rape Kit Was Used to Identify Her as a Suspect in Another Case*, N.Y. TIMES (Feb. 15, 2022), https://www.nytimes.com/2022/02/15/us/san-francisco-police-rape-kit-dna.html [https://perma.cc/7Q82-H9H7].

364. *See* Tami Abdollah, *Rape Survivors, Child Victims, Consensual Sex Partners: San Francisco Police Have Used DNA from All of Them for 7 Years*, USA TODAY (Feb. 25, 2022, 1:58 PM), https://www.usatoday.com/story/news/nation/2022/02/23/san-francisco-police-rape-kit-dna-controversy/6854467001 [https://perma.cc/4KYW-PNBP].

365. *See* Verified Complaint, N.J. Off. of the Pub. Def. v. N.J. Dep't of Health, No. MER-L-001210-22 (N.J. Super. Ct. Law Div. July 11, 2022); Emily Mullin, *Police Used a Baby's DNA to Investigate Its Father for a Crime*, WIRED (Aug. 15, 2022, 7:00 AM), https://www.wired.com/story/police-used-a-babys-dna-to-investigate-its-father-for-a-crime/ [https://perma.cc/MY32-ZWQX].

366. Christina Del Greco, *Establish Data Standards to Protect Newborn DNA Privacy by Developing Data Storage Standards for Newborn Screening Samples*, FED'N OF AM. SCIENTISTS (Nov. 18, 2024), https://fas.org/publication/protecting-newborn-dna-privacy/ [https://perma.cc/HD6H-X278] (subpoenaing newborn screening data "may also erode trust in the health system"). In addition, research in the sexually transmitted disease context shows concerns about privacy and data sharing can significantly decrease people's willingness to participate in public health initiatives. *See* Heather Pederson et. al., *A Cross-Sectional Survey Exploring Attitudes Towards Provincial Electronic Health Record Implementation Among Clients Attending the Provincial Sexually Transmitted Infections Clinic in British Columbia*, 91 SEXUALLY TRANSMITTED INFECTIONS 44 (2015).

enforcement, seeking help, not knowing their data may be repurposed in unforeseen ways. While these young people may consent to data collection as a victim, this consent shouldn't count for unrelated purposes.

Generally abolishing digital consensual searches by law enforcement can minimize data misuse. After all, fewer searches decrease opportunities for abuse. However, effective data control hinges on robust data policies. These are currently lacking.

If digital consensual searches are to remain, the data collected should be used only for the objective at hand. Consent-to-search forms should limit searches to "responsive data," echoing Orin Kerr's proposal for executing digital warrants to collect only the specific information that is relevant to the defined scope of the search.[367] To ensure compliance, legislation should require audit logs with automatic screen recording, providing a record of the precise steps law enforcement used to search the phone.[368]

Irrespective of whether data is collected via a consensual search, warrant, exigency, or other means, states should limit the data that is retained, and mandate destruction for most data. Electronic data deletion and sealing statutes in New Mexico, Utah, and California—among the first of their kind—serve as legislative models.[369] Juvenile expungement and sealing statutes could also serve as useful benchmarks for retention and deletion. Some common sense provisions include immediately deleting data when charges are dismissed or fail to result in an adjudication or conviction.[370] Even with a conviction or adjudication, data deemed relevant should be sealed at the conclusion of the case, with a few exceptions.[371] Effective

367. *See* Kerr, *supra* note 22, at 4 (arguing to impose a use restriction on nonresponsive files seized during the execution of a warrant for digital evidence). The American Law Institute's section on consent searches also advocates for controlling the scope of searches. PRINCIPLES OF THE L.: POLICING, § 4.06 (AM. L. INST. 2023).

368. *See* KOEPKE ET AL., *supra* note 221, at 64.

369. I focus here on New Mexico, Utah, and California, because most states do not have comprehensive, specific statutes requiring law enforcement agencies to limit electronic data retention and provide for deletion. San Francisco has a local policy of note as well. *See Record Retention & Destruction Policy*, S.F. DEP'T OF POLICE ACCOUNTABILITY, https://www.sf.gov/file/department-police-accountability-record-retention-destruction-policy [https://perma.cc/NF75-Q7TH]. Note that all three of these state statutes govern data obtained because of a warrant. Electronic Communications Privacy Act, N.M. STAT. ANN. § 10-16F-3 (2024); Electronic Information Privacy Act, UTAH CODE ANN. §§ 77-23c–101.2 to -105 (LexisNexis 2024); Electronic Communications Privacy Act, CAL. PENAL CODE § 1546.1(d)(2), (e)(2) (West 2024).

370. Around half of states have laws that automatically seal or expunge juvenile records in certain circumstances. *See* NAT'L CONF. OF STATE LEGIS., *supra* note 294.

371. Similar to the recommendation with regard to generally abolishing digital consent searches, the sealing process should still permit defenders to access exonerating evidence. Additionally, Professor Eve Rips persuasively argues that there are ways to preserve the information for data and research, so we can understand the history and disparities present in criminalizing children. *See* Eve Rips, *Off the Record: Preserving Statistical Information After Juvenile Expungement*, 72 AM. U. L. REV. 587, 587 (2023).

policies can safeguard against mission creep, the creation of aggregated databases for broad surveillance, and unjustified and continuous data storage of large swaths of the population.

CONCLUSION

The digital age presents unprecedented challenges to children's data privacy, with law enforcement access posing acute risks. This Article explores the historical and legal foundations of one particular challenge, parental consent serving as a carte blanche to law enforcement access, tracing it back to the concept of child coverture.

The collection of children's data, facilitated through parental consent, can reshape the very meaning of childhood. It harms young people in permanent and stigmatizing ways, with impacts most felt by minority youth. This information also feeds databases and chills youth associating with one another, creating community-wide effects. Continued reliance on parental consent, even over the objection of their children, is a relic of coverture and must be reimagined.

This Article proposes a multi-prong approach to reform, one that depends less on parental decision-making, and more on regulating state and third-party actions. It provides advocates with a vehicle to argue that digital searches are different, and more akin to a search of the child's mind itself. Legislative reforms, like abolishing digital consent searches of minors, regulating third-party data collection, and implementing comprehensive data policies, are also necessary. With these steps, we can begin to build a framework that truly protects children's digital privacy.

Ultimately, this Article calls for a theoretical shift in how we conceive of children, as beings who are not simply extensions of their parents. Instead, it advocates for affirmative measures to protect their data. This vision places children's interests at the forefront, recognizing their right to information and privacy.