CHILDREN AND THE CARS THAT WATCH THEM

Nila Bala*

* * *

Parents are turning to autonomous vehicles (AVs) to shuttle their children around, seeing them as a safe and convenient option. AVs promise increased mobility for children but bring with them unparalleled surveillance risks. As parents embrace in-cabin monitoring and location tracking to enhance safety, they also—often unknowingly—authorize the mass collection, retention, and potential disclosure of their children's most intimate data.

This Essay presents the first case study of children's privacy in AVs, serving as a lens to critique the prevailing reliance on parental notice and choice as the cornerstone of children's data protection. Drawing on privacy theory, surveillance studies, and child development literature, the Essay argues that the notice-and-choice framework fails to account for children's distinct privacy interests, particularly when the data collected may be retained indefinitely, repurposed by law enforcement, or sold to data brokers. The Essay calls for real limits on data collection, meaningful restrictions on sharing, and mandatory deletion rules. These principles extend beyond AVs to the technological ecosystem now shaping childhood in the digital age.

Introduction

The San Francisco Standard reported that Chris's fifteen-year-old daughter has a new way of getting around: Waymo robotaxis. Chris and his wife describe it as the "best thing that's ever happened" to them: "It was instantly awesome," remarked Chris, who used only his first name so that his Waymo account would not be banned. "We don't have to worry about her getting home, ever."

Chris is not alone. Parents all over San Francisco are skirting the rules, using Waymo's driverless cars to shuttle kids solo, despite company policy forbidding the practice.[1] Some parents prefer

---

* Acting Professor of Law (tenure track), UC Davis School of Law. The author thanks Khalid Albutairi, Elizabeth Brandt, Simone Montgomery, Madeline Reed, and Lauren Yi for their assistance.

[1] "Passengers 17 and under can ride as your guests. For our little passengers under 8 years old, you'll need to bring a car or booster seat and secure it in the back seat according to the manufacturer's installation instructions. Children under the age of 8 cannot sit in the front. Learn more in our Help Center."

autonomous vehicles (AVs) to public transportation, feeling a robot chauffeur is safer. Many parents like that they can track its location at all times. Additionally, robotaxis have cameras inside to record what is happening at all times, and Waymo support staff sometimes intervene when they see unsafe behavior. These cameras address a key concern for parents: Parents generally support AV use by their children, with a caveat. They want video surveillance that they can access at all times. While minors are not yet permitted to travel alone in Waymo vehicles, that policy is likely to change in the near future. Waymo has just announced the launch of a program for teen passengers, and there are parents who would welcome Waymo allowing even younger passengers.

This Essay considers the unique privacy issues that emerge based on the normalization of child ridership in AVs. As many scholars have argued, cars are not simply cars. They are used as spaces to have conversations, to engage in intimate activities, and even as homes. Cars are especially important as private spaces for adolescents as they develop their identities.

Cars are also not simply cars in an additional way: They are a computer on wheels, collecting highly revealing location information. Following *Dobbs v. Jackson Women's Health Organization* (2021), minors face unprecedented restrictions on reproductive and gender-affirming healthcare access, car trips to access care could now carry potential criminal implications. In this environment, aggregating location information to clinics and medical facilities raises the danger of prosecutions. As the Supreme Court articulated in *Carpenter v. United States* (2017), knowledge of an individual's movements over "public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales" can paint an extraordinarily detailed and intimate picture of their lives. The Court was talking about cell site location data, but today's vehicles can provide much of the same.

Data collection is ubiquitous, and children are at particular risk. AVs (and smart vehicles in general) can collect and retain massive amounts of data, subjecting children to "dataveillance" without their knowledge. This information—the child's location, actions, statements, imagery, and videos, can be shared with various parties, including law enforcement. AVs are part of a larger story of "always-on" devices that constantly collect data from users, often without their knowledge or consent. The relentless data collection raises concerns about equity. Not all children will be subjected to privacy risks equally—those from marginalized communities with fewer transportation choices may suffer disproportionate surveillance.

This Essay presents the first case study examining AV technology and children's privacy. Its central scholarly contribution, however, extends far beyond the intersection of cars and children. This work advances a fundamental critique of parental notice-and-choice frameworks as adequate mechanisms for protecting children's data privacy in the digital era.

Under privacy law's dominant approach of notice-and-choice, companies must notify individuals about their data collection and obtain consent before collection. When applied to children, this regime defers to parental consent, a model that assumes parents can make informed privacy decisions on behalf of their children after receiving adequate information. This model fails for two reasons. First, current privacy law's reliance on parental consent disregards children's independent privacy interests and developmental needs. Second, relying on parental notice-and-choice inherits and amplifies the well-documented problems of the notice-and-choice model—already widely recognized as inadequate for protecting adult privacy.

These two failures reveal that meaningful privacy protection for children cannot be achieved through procedural reforms to notice-and-choice mechanisms. Instead, such protections require substantive legal safeguards that operate independently of parental authorization. By examining how AV surveillance systems threaten children's privacy, this work develops principles with broad applicability across various technologies that collect children's data.

My argument proceeds in three parts. Part I of this Essay provides a descriptive account of the current state of AVs generally. It is the first article to consider the use by children specifically, alongside the existing laws governing the field. Part II will consider the costs and benefits of surveillance on children, with attention to how its negative effects may be distributed inequitably. Surveillance is no longer peripheral to childhood. Children are watched at home, on the streets, and in schools—and this pervasive observation is reshaping the experience of growing up. Drawing upon surveillance studies and child development literature, the Essay is the first to discuss the social impacts specifically of monitoring children in vehicles. The focus of children's privacy law has been to focus upon third-party predators, placing parents as children's protectors, assuming a complete unity of interest. But in the AV context, parents are one of the largest proponents for increased surveillance. With surveillance comes the real potential for increased criminalization.

Finally, Part III proposes reforms to better protect children's intimate privacy when they ride in AVs. Instead of continuing to regulate AVs through a notice-and-choice (also called notice-and-

consent) model to collect data, this Essay urges substantive protections to limit the use of minors' data. The reforms proposed will guide meaningful privacy protections that go far beyond just AVs to other devices children use in the modern, connected age.

I. Children and Cars

A. AV Development

Self-driving cars have long captivated the world's imagination. They were the stuff of dreams, but they are now a reality. Vehicles with some level of automation, namely some basic safety features like cruise control, have been available for the last fifty years. But higher levels of automation are a new phenomenon. SAE International, formerly the Society of Automotive Engineers, has created a taxonomy for defining these various levels of automation, from level 0 (no driving automation) up to level 5 (full driving automation). Only recently have manufacturers been able to make level 3 and 4 vehicles. Level 4, exemplified by Waymo, allows for something closer to full autonomy.

Advanced automation means much higher amounts of data collection and storage by AVs. AVs rely on more than a dozen cameras and sensors strategically positioned around the car. Today's AVs collect approximately one hundred times more data than a personal smartphone. While the primary purpose of this data collection is to enable safe and efficient autonomous driving, it inevitably captures personal information about individuals in the vehicle's vicinity. Cameras can potentially record identifiable faces, license plates, and even activities inside nearby buildings or homes. This footage could be placed through facial recognition software and could also be stored in perpetuity.

The privacy implications of AVs extend beyond personal ownership. Especially while the technology is still nascent, most people are likely to encounter AVs through ridesharing and rentals, making these contexts the most likely sites of data collection. AV fleets, such as Waymo, and more traditional models that may incorporate AVs in the future, like Uber and Lyft, track not just pickup and dropoff locations but also entire route histories and other personal information. Rented AVs are likely to collect similar information but tend to engage in greater integration with users' smart devices, absorbing demographic details, entertainment preferences, and contact lists. Additionally, AVs might employ biometric systems for vehicle access, adding another layer of sensitive data collection.

The initial collection of personal information—what we might term "primary use"—represents only the beginning of privacy

concerns. Primary use refers to data collected for the express purpose of enabling the core function of the technology. But data rarely stays confined to its original purpose. Consider a vehicle company collecting information that allows their cars to safely and effectively transport passengers. However, this information is shared and sold to third parties, either directly or through data brokers, exposing passengers to secondary uses. Similarly, in the AV context, car companies might share behavioral data with third-party advertisers–for example, that an individual goes to a health clinic once a month. It is no surprise modern vehicles have been categorized as "the worst performing product category for privacy protections."

In sum, the expansion of AVs, and the vast amounts of data they collect, raise urgent questions about the adequacy of existing privacy laws to protect consumers.

B. Existing AV Laws

AV regulations are limited at both the federal and state level, in a way that parallels the general inertia of legal responses to technological advances. This section first examines AV-specific legislation, followed by broader privacy laws relevant to the data AVs collect. Roughly thirty-five states have legislation responsive to current AV technology; however, most of these statutes focus mainly on safety, rather than privacy. Only a single state, Utah, has proposed legislation mentioning children. In 2020, the state tried to enact provisions regarding transporting minors in AVs for-hire, mainly around safety. In a similar vein, the state tried to establish a working group the following year on unaccompanied minors and AVs but failed.

At the federal level, statutes or regulations are absent. In both 2017 and 2018, Congress failed to pass AV START, a bill aimed at regulating the safety and development of AVs. To date Congress has never passed legislation specific to automated driving. The National Highway Traffic Safety Administration (NHTSA) has issued guidance on cybersecurity best practices for AVs, which serve as recommendations for the industry but lack the force of law. Although broad privacy laws might provide some protection, they are not equipped to handle the data practices of AVs. For example, Children's Online Privacy Protection Act (COPPA), a federal law enacted in the 1990s to protect children who use online services, has a number of deficiencies. It protects only children under thirteen and relies upon notice and choice of parents. COPPA also may not cover data collected from AVs, since it is focused on personal information collected by websites and online services.

Similarly, the Driver's Privacy Protection Act (DPPA) is focused on the driver's data and requires state agencies to obtain a driver's express consent before releasing any personal information obtained in connection with a motor vehicle record. However, the DPPA contains several exceptions that would seem to allow in-cabin monitoring to take place. These include legitimate needs by any government agency in carrying out its functions, and when there is a "use in connection with matters of motor vehicle or driver safety and theft" and "motor vehicle market research activities." In-cabin recordings might also not be considered a "motor vehicle record" in the first place, thus evading the DPPA's protections altogether. And like COPPA, express consent continues to function as a broad permission slip to disclosure.

There are a number of relevant state laws, though these too have limitations. California is one of the few states that provides consumers with limited protections around the personal information their vehicle is gathering about them. In 2023, the California Privacy Rights Act (CPRA) took effect and included geolocation within the definition of "sensitive personal information," opening up the possibility the CPRA could regulate AV data collection. Notably, the California Privacy Protection Agency has announced a review of data privacy practices of "connected" vehicles, which have features like location sharing, smartphone integration, and cameras, signaling regulatory interest in this area. Another relevant California state law is the California Invasion of Privacy Act (CIPA), an anti-wiretapping and anti-eavesdropping statute that prohibits unauthorized interceptions of communications in order to protect the right of privacy. While CIPA offers protections against unauthorized recordings, its practical impact is limited in the AV context, in which parental consent has ostensibly been obtained.

Several states—Virginia, Colorado, Connecticut, and Utah—also have general data protection laws that require companies to get consent for processing sensitive data, including geolocation, and set modest limits on data flows. In addition, companies that also operate in the European Union must comply with the General Data Protection Regulation (GDPR) requirements that set standards for the collection, processing, and storing of personal data by AVs. These laws were not written specifically with AVs in mind, so regulatory gaps remain.

C. Children and AVs

For children, the elderly, and individuals with disabilities, AVs represent a revolution in mobility options. Over 40% of persons with disabilities rely on others for transportation and 70% limit their travel

altogether. Given that children cannot drive, they face an even greater dependency on the adults in their life to travel. This dependency is particularly acute for children from low-income households, who often struggle to access school, extracurriculars, medical appointments, and social events. Transportation access thus represents more than convenience—it constitutes a prerequisite for educational mobility and social participation.

As AVs edge closer to widespread adoption, a number of public interest groups have begun to look at the unique challenges associated with child passengers. In 2018, the organization Safe Kids Worldwide created a Blue Ribbon Panel, Children in Autonomous Vehicles. The calls to action include increased safety standards, usability testing for families, inclusive design, appropriate supervision, and marketing safe transportation using restraints. Significantly, all of the Blue Ribbon Panel's recommendations focus on child safety rather than privacy. This narrow focus on physical safety is mirrored in much of the emerging literature, which tends to look at parents' attitudes and beliefs around AV safety for their children. Parents in particular have highlighted the need for *more* surveillance within the vehicle's cabin, including that a camera and microphone are requirements to their children to both monitor and communicate with their children. However, few studies have looked at children's attitudes, and none have focused specifically on children's privacy.

As AVs evolve, children are likely to use them not only for transit, but as temporary extensions of home, school, and social life. For children commuting alone or spending significant time in transit, AVs may become spaces where they complete homework, communicate with friends, nap, change clothes for extracurriculars, or process personal emotions. Survey data reveals that individuals already regularly engage in a wide range of intimate activities within their vehicles—from routine behaviors like eating and communicating to more private activities such as sleeping, changing clothes, and engaging in sexual activities. AVs will only amplify this trend, and make cars even more dwelling-like by freeing up passengers from tasks related to driving. This shift toward treating vehicles as personal living spaces heightens the need for privacy protections. Privacy concerns affect all vehicle occupants, but they become particularly acute for children, whose developmental stage makes them especially vulnerable to privacy intrusions. The next section takes up that concern.

II. Children's Privacy

As young people start to be alone in cars, safety concerns naturally arise for parents, car manufacturers, insurance companies, and government regulators. These concerns are legitimate. Some forms of in-cabin monitoring may not only be desirable, but necessary. For children who are unattended passengers, surveillance could assist in emergencies; for example, if the vehicle broke down and the child needed to call for help or was facing a medical emergency. Additionally, if a child is unattended, surveillance may help determine if the child is properly restrained during the journey. Surveillance could allow for automatic adjustment of safety systems based on passenger size and position and ensure the use of child safety restraints when appropriate.

In some cases, the impetus for surveillance extends beyond child-specific concerns. In-cabin monitoring can serve broader interests—to protect companies from vandalism, misuse, and other misbehavior by occupants. Surveillance may help mitigate these risks. Yet any safety benefits must be weighed against developmental costs. Adolescence is a critical period of identity formation and growing independence, historically supported by private spaces, and undermined by constant monitoring. Part II of this Essay explores two distinct but related surveillance dynamics: The first section of this Part addresses the harms of parental surveillance, while the second section considers harms beyond parents—harms from law enforcement and other third parties monitoring children. While treated separately here, parental and third-party surveillance are closely linked. As I have argued in previous work, parental surveillance—and parental consent to surveillance—can facilitate and legitimize third-party monitoring of children.

A. Risks from Surveillance

AV surveillance does not just implicate spatial autonomy for youth, but control over their inner worlds–their thoughts and choices. Surveillance harms children's self-development during a time when they are particularly vulnerable. Yet today's young people face unprecedented surveillance across all domains of their lives. Unlike the past, when children could explore ideas in books and libraries without online tracking, today's surveillance denies children the ability to develop and express themselves without shame or judgment.

The role of parents as key contributors to this surveillance often goes unnoticed. Surveillance technology companies have masterfully positioned their products as essential markers of responsible parenting in the digital age. Through their marketing, they promote the notion

that constant monitoring—from nanny cams to location trackers—represents the gold standard of caring, attentive parenting. While the primary purpose of AV monitoring systems is ostensibly for operational oversight and safety, parental demand for these monitoring capabilities is undeniable and may even be a condition for parents allowing their child to use AVs. So while systems might be installed by the AV company, an intended market is parents. Any evaluation of in-cabin surveillance must take seriously parental interests in monitoring and the uses—and misuses—of the data they access.

Increasingly, good parenting equals perpetual surveillance. Companies capitalize on parental anxieties about safety and success, suggesting that parents who don't embrace comprehensive monitoring technologies are somehow falling short of their duties, even though our children are not in greater danger, and in fact are far safer, than past generations. The marketing narrative transforms surveillance from an option into an obligation, reimagining the parent-child relationship through a lens of constant observation and data collection.

Constant monitoring of young people undermines developmental processes that require freedom from observation. These developmental processes include identity exploration, role experimentation, and the formation of a coherent self-concept. Privacy plays a crucial role in this process, as it provides adolescents with the space to experiment with different self-presentations and develop their unique identity away from constant adult scrutiny. This experimentation involves gradually taking on more responsibilities and making choices about their future, which requires a degree of freedom from parental control and often a shift in attachment to peers. Unfortunately, current research on teen technology often takes a misguided "risk-centric" approach. But restricting children's participation in an effort to protect them may, ironically, lead to greater long-term risks. For children, surveillance instills a sense of mistrust and suspicion, conditions that can ultimately breed the very misbehavior that authorities are seeking to prevent. Children, feeling pre-judged as potential wrongdoers, may act out in rebellion against the very system meant to "improve" their behavior.

Even before AVs, truly private spaces were rare for teenagers. The car provided a unique refuge. As one young woman told sociologist Amy Best, getting a driver's license meant feeling "liberated"—primarily from constant parental presence. This liberation opened doors to relationships beyond the family unit. Professors Ann Dailey and Laura Rosenbury have highlighted this critical issue: children's right to a life beyond their parents. In the car, young people could have a space away from adults. In the car, children could participate in

social life more freely and develop more relationships and be exposed to ideas beyond those mediated by their parents. Vehicles, if constantly monitored, risk eliminating one of the few remaining private spaces available to young people. The loss of these moments—whether brief drives or extended road trips—could fundamentally alter how teenagers develop independence and process life's challenges.

The car is also a conduit to spaces that children may not have parental support to access. Specifically, vehicles may be the way young people access reproductive and gender-affirming healthcare. For children in the LGBTQ+ community, transportation may be a lifeline to finding communities where they can find acceptance and support. As Professor Danielle Citron explains, children's intimate privacy—defined as control over access to their "bodies, minds, health, sex, sexual orientation, gender identity, and close relationships"—is fundamental to their ability to thrive. In this context, vehicles function not merely as transportation, but as tools of empowerment toward intimate privacy and resistance against oppressive circumstances.

The loss of private space in vehicles not only undermines adolescents' development, it also opens the door to something more insidious: the systemic repurposing of children's data. Surveillance in AVs does not end with the gaze of a parent or the car company simply collecting information for safety; it becomes part of a larger infrastructure in which intimate details about a child's behavior, location, and associations can be retained, shared, and used in ways far removed from the original purpose. Monitoring for safety has its risks, but the harms go beyond these to policing, profiling, and punishment—especially for those who are already at the margins.

B. Beyond Primary Use

Information collected to ensure child safety in AVs and maintain AV performance will inevitably find its way to secondary uses—a pattern well established across digital domains. Nearly every automaker is already selling driver behavioral data, including where, when, and how fast individuals drive. AV-generated data, and specifically in-cabin monitoring, will almost certainly follow this same trajectory.

The consequences of surveillance creep will not fall equally across society. Black and Brown children, poor children, and disabled youth may be the most likely to be surveilled, with their data more frequently channeled to law enforcement. Easy access to digital evidence could create a net-widening effect of youth entering the carceral system. Even seemingly innocuous location data can create prosecutorial evidence for establishing patterns and documenting

minor infractions that might otherwise go unnoticed. Contact with the system can actually make young people more likely to reoffend. The data demonstrates that over-criminalization of typical teenage behavior is harmful and made all the easier by surveillance technology.

Surveillance could also be used for new crimes that have emerged in the wake of *Dobbs*. Now, minors face increasing restrictions in accessing reproductive and gender-affirming health care. Location data from reproductive healthcare clinics has been targeted and sold by multiple data brokers. Law enforcement can bypass legal requirements and buy personal data in bulk from data brokers, regardless of any evidence of a crime. This practice allows police to circumvent the need for gathering evidence and obtaining a warrant based on probable cause, which is typically required to access such data.

For police and the government, in-cabin monitoring in AVs is a surveillance opportunity. With storage costs plummeting, there's little incentive to delete anything. Information can be aggregated and stored in a database in perpetuity. We have already seen how surveillance databases, like those tracking alleged gang members, become powerful tools wielded against minority communities. It is likely that law enforcement use of AV surveillance will replicate this trend.

Once car companies generate this data, it develops a life of its own. The Supreme Court's decision in *Carpenter v. United States,* which has been interpreted narrowly by lower courts, offers little protection. In *Carpenter*, 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. 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. 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.

Carpenter's impact has been limited, with courts resolving a shockingly high rate of cases based on the "good faith exception" to the exclusion rule and denying Fourth Amendment protections in 82.6% of post-*Carpenter* cases. Policing agencies continue to defend third-party data access on the grounds that people have consented to third-party access by using these apps. Some courts have supported this logic, drawing the line between voluntary, affirmative acts and automatically generated information. When parents affirmatively consent to in-cabin surveillance to ease their anxiety, they likely

trigger the third-party doctrine. Though few parents intend for third parties or police to access their children's information, this may be the inevitable cost of their desire to monitor their own children. This legal framework allows government access to surveillance data, even if it was created for entirely different purposes.

III. Why Parental Consent Doesn't Work and What to Do About It

The notice-and-choice paradigm has dominated privacy regulation. These rules operate under the premise that collecting, distributing, and retaining personal information is permissible as long as reasonable notice is provided and consent is obtained. However, this model has been subject to extensive criticism. According to the American Law Institute's Data Privacy project, "[t]he overwhelming majority of commentary, scholarship, and empirical evidence suggests that traditional notice does not work." This failure stems from several practical and structural shortcomings in how notice and choice is implemented.

Privacy notices are often incomprehensible and lengthy, making it unrealistic to expect individuals to read them. Most individuals experience "consent fatigue": They mechanically accept terms without real engagement. The cognitive burden imposed by notice-and-choice exceeds what individuals can actually take in, rendering consent ineffective. Additionally, the "choice" offered is often illusory. Privacy decisions are typically presented in take-it-or-leave-it terms for essential services.

In some ways, the criticisms of notice-and-choice frameworks in privacy law mirror longstanding critiques of consent doctrine in Fourth Amendment jurisprudence. People often don't understand what they are consenting to, and the power imbalance with law enforcement can make refusal feel illusory, especially for members of minority communities. The dynamics of consent become even more complicated when children are involved. In the criminal legal context, courts have increasingly recognized that there are certain constitutional rights of which a parent cannot consent to the waiver on behalf of the child, particularly once the child enters the juvenile legal system. A similar skepticism should inform our view of parental consent in the data privacy context—especially when the data in question is intimate, long retained, and potentially accessible to third parties, including the government. If courts are beginning to recognize the limits of parental decision-making in the criminal legal system, we should ask how those

limits apply beyond the courtroom—especially within the data privacy context.

Notice-and-choice frameworks, especially within families, create deep concerns that mirror the conflicts of interest we see in the criminal context. As scholars like Helen Nissenbaum have argued, privacy is not just individual but contextual and relational, and a notice-and-choice model ignores how data practices affect groups and social structures. Individual adults already demonstrate poor privacy decision-making for themselves–routinely accepting lengthy terms without reading them, misunderstanding the scope of the agreement, and consenting to arrangements they would reject if fully informed. Yet we rely on the parental control model that delegates children's privacy protections to parents, instead of creating substantive protections for children. As Professors Danielle Citron and Ari Waldman observe, "no parent can meaningfully curtail corporate data collection, either for themselves or their children."

Even setting aside structural issues, there's a deeper problem with notice and choice: the assumption that parents' privacy choices necessarily reflect the best interests of their children. As Professors Dailey and Rosenbury have highlighted, the law—in general—constructs the parent and child as a unified entity, focusing primarily on external threats and largely ignoring the possibility of intra-family conflicts. But parents and children may not actually be aligned. In the AV context, "close supervision" might undermine a young person's exploration and attempts to develop independence. Perfect surveillance can also mean perfect evidence: AV surveillance creates complete evidence trails that may lead parents to report children's misbehavior or minor offenses to authorities—whether intending to "scare them straight," avoid personal liability, or simply responding to situations they feel ill-equipped to handle independently. At the opposite extreme, "unfettered access" might leave children with minimal oversight, their data routinely transferred to third parties and data brokers through parents' completely uninformed consent. Neither approach might be in the child's interest.

Existing legal frameworks are inadequate to these concerns–they operate on a notice and choice basis, and rarely, if ever, consider how third parties can acquire children's data from AVs. Even if parents are well meaning, parental consent can become a vehicle for privacy violations rather than protection, exploited by corporations seeking to access children's data through parental permission and by law enforcement officers who obtain parental consent to gather evidence subsequently used to prosecute those same children.

The Children's Online Privacy Protection Act (COPPA) exemplifies these limitations. Although COPPA imposes a parental consent requirement for children under thirteen, it adopts the conventional notice-and-choice approach—despite widespread evidence that such notices are just clicked through by parents. If most Americans accept online terms of service without reading them, the percentage is likely even higher among time-constrained parents. Similarly, in the educational arena, scholars like Professor Zahra Takhshid advocate moving away from the parental consent apparatus toward more robust privacy protections for children for these reasons. For educational technology, parents often face a false choice: consent to data collection or impede their child's educational access. AVs present parallel concerns—when the choice lies between vehicle access for essential activities or no access at all, meaningful consent regarding data collection does not exist.

A. A Way Forward

Rejecting surveillance altogether isn't realistic—or even desirable. As discussed at the outset of Part II, AVs need some monitoring in order to operate safely. The external cameras are integral to making sure the AV avoids collisions, and the internal surveillance can also be justified for safety, for example, making sure individuals are restrained. But we should ask ourselves seriously: What surveillance do we really need? What can we do without? And even for data that we need, how can we mitigate long-term harms?

So far, we've relied on notice and choice. As long as individuals consent, companies are free to collect whatever they want. Some reformers have proposed improving this process—providing consumers more notice, creating friction before proceeding, making privacy notices more concise. These incremental changes miss the fundamental issue: Every stakeholder in the child surveillance ecosystem—from car manufacturers to government agencies to parents—faces strong incentives to collect more data, not less. It's a one-way ratchet to full surveillance of children.

And while the child is a stakeholder, children lack representation. This makes them uniquely vulnerable to privacy infringements. Unlike adults who can vote, lobby, or organize to protect their interests, children depend entirely on others to advocate for their rights. This dependence becomes an issue when their privacy conflicts with an adult protecting their own interests. As Professor Aliza Hochman-Bloom has argued in the context of curfews, it is unlikely that parents will oppose curfews, even when they are harmful to children. Few parents will publicly argue that children should be allowed out alone at night, and just as few will argue that children

deserve privacy from AV monitoring because doing so suggests inadequate parenting. It is simply not popular to argue that children need more freedom, should take more risks, should be watched less, especially with the popularity of intensive parenting.

Additionally, companies and government agencies are unlikely to embrace restraint in collecting and sharing only necessary data. Ride patterns hold tremendous value, not just for marketing to individuals, but for analyzing broader behavioral trends. Dozens of data brokers admit to selling minors' data, including reproductive health care and geolocation information. Children's data holds special value to data brokers (estimated in the hundreds of billion dollars in the United States alone). Given these financial incentives, it's unrealistic to expect companies to care about children's privacy in the absence of regulation.

The notice-and-choice framework has failed children. We need substantive limits on what data companies can collect about kids and how they use it. In this section, I propose three concrete reforms: (1) robust data minimization, particularly with regard to in-cabin surveillance recordings; (2) strict limitations on the sale and sharing of data with third parties, including data brokers and law enforcement; and (3) clear statutory data retention and deletion requirements. Though this Essay focuses on AVs, these reforms have implications for all surveillance systems that touch children's lives.

1. Reimagining Data Minimization for Surveillance Technologies.

Data minimization is a core principle of modern privacy law, yet implementation in the United States remains frustratingly incomplete. The GDPR, for example, requires that data collection be "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed." But in the United States, there is no justification required to process personal data. Still, consent is ostensibly required for data to be collected and processed, and the American Law Institute's Data Privacy Principles—seizing upon existing U.S. law—recommend greater limits on collecting and processing data unrelated to the initial aim.

While these principles are seldom codified into binding obligations under U.S. law, they should be. Current industry practices permit continuous, high-resolution video recording of minor passengers with minimal justification. This approach inverts appropriate privacy baselines: Comprehensive surveillance becomes the default rather than the exception. Legal frameworks should instead establish a presumption against full-time recording unless companies can

demonstrate compelling safety interests that cannot be satisfied through less invasive means.

In-cabin video is marketed as essential to ensure rider safety, prevent misuse, and enable remote customer support. However, these safety objectives might be achievable through less invasive means. Alternative approaches could include audio-only monitoring, on-demand surveillance systems that only activate during an emergency, or simple physical sensor technology (to verify compliance with things like seatbelt usage). Part of data minimization is collecting information for vehicle safety without a default of sharing it with third parties, including parents. These policies limit unnecessary data collection while still fulfilling safety functions.

2. Confronting the Third-Party Data Sharing Crisis.

The commodification of children's personal information through secondary data markets is one of the most urgent threats to children's digital privacy. The data broker ecosystem has institutionalized what scholars term "surveillance capitalism": the systematic extraction and monetization of behavioral data that deepens existing inequalities and exploits vulnerable populations, including children. In the AV context, the data that companies collect can easily enter these secondary markets. Recent investigations confirm that data brokers frequently traffic in this kind of sensitive information and even purposely create design tools to hide privacy violations—playing a "cat and mouse" game to get the most sensitive information possible.

What's worse, many data brokers are unregistered and operate with near-complete opacity. Regulation is needed to protect children—and all individuals—from having their data sold and resold at industrial scale. Ideally, data brokers would be regulated at the federal level. Several states have made efforts to regulate data brokers: In California, Vermont, Texas, and Oregon, data brokers must register annually, but the regulations fall short of substantively protecting customers. They maintain opt-out frameworks that place unrealistic burdens on individuals.

Law enforcement agencies also increasingly bypass warrant requirements by purchasing data directly from companies or data brokers, circumventing constitutional protections. In 2025, Montana became the first state to close this loophole by requiring warrants before government agencies can purchase electronic communications or other sensitive data. Such measures are the first step to protecting children's intimate privacy from exploitative secondary markets.

3. Data Retention and Deletion.

Most privacy scholars focus on access and control of data, but retention and deletion are important elements as well. Even when AV companies collect data for legitimate safety purposes, retention of that data poses a serious threat to children's privacy. The longer intimate data is stored, the more opportunities exist for abuse, theft, and misuse. There is the threat of hacking, often revealing very private information about individuals. Additionally, sharing a child's data with police presents separate dangers that I have thoroughly documented in previous work. Given these harms, regulations should require that companies delete in-cabin recordings, location histories, and other sensitive information related to child passengers as soon as the immediate operational purpose has been served.

Short retention limits are also key to prevent law enforcement abuses. Data for criminal investigations can be perpetually retained under current laws, with previously innocuous information revealing new insights in the future. This state of permanence stands in contrast to juvenile justice principles: While all states mandate juvenile record expungement or sealing, digital search data can persist indefinitely on law enforcement servers because most agencies lack data deletion policies. Without meaningful deletion policies, children face the risk of perpetual exposure, undermining their right to second chances and clean slates.

Conclusion

The rise of AVs offers unprecedented mobility for children, yet it also brings the potential for unprecedented surveillance. In-cabin monitoring, location tracking, and the sale of all that data combine to create a digital dossier of children's lives. Young people cannot understand, opt-out, or meaningfully control the AV data collected about them. Our legal frameworks fail to keep pace—not just because of legislative inertia, but because the privacy laws we do have are built on a flawed foundation: the notice-and-choice paradigm and parental consent.

This Essay challenges that foundation. Children are not just extensions of their parents. Their privacy interests may be different. Surveillance, even when well intentioned, can undermine their developmental needs, chill exploration, and curb appropriate risk-taking. For marginalized youth in particular, these risks are compounded by inequities that make surveillance not just invasive but punitive.

AVs give us an opportunity—a chance to develop privacy protections for children before the harms become normalized.

Meaningful reform requires more than marginal improvements to notice or better design of consent forms. The reforms proposed here—data minimization, strict limits on third-party sharing, and robust retention and deletion mandates—are essential not just for AVs, but for the entire digital infrastructure surrounding children today.

We must reorient privacy law to protect children as rights-holders in their own right. Until then, the cars that carry our children will continue to watch them—and worse, expose them—in ways they may not understand but will nonetheless feel.

* * *

Nila Bala is an Acting Professor of Law (tenure track) at UC Davis School of Law.