The Vehicle Monitoring and Collection Technology Era

Stacy-Ann Elvy[*]

ABSTRACT: Vehicle monitoring and collection ("VMC") technology, including starter interrupt devices that remotely disable vehicles, and other GPS tracking devices are used in consumer vehicle agreements in subprime transactions. Subscription-based models supported by VMC features, such as over-the-air software updates that remotely disable or enable vehicular functions, have also appeared in the non-subprime automobile context as well. This Article contends that the rise in VMC technology and features raises several alarming privacy, electronic subjugation, and cybersecurity risks. The Article makes an express link between the consumer risks and harms associated with the use of VMC technology in subprime lending transactions and the broader technological shift towards a subscription-based service model supported by VMC features in non-subprime vehicle transactions. The Article's evaluation and critique of VMC technology and features is conducted simultaneously through the lens of commercial law, state VMC technology statutes, state privacy laws, such as the California Consumer Privacy Act ("CCPA"), and federal frameworks governing transactions involving consumer vehicles. I argue that these legal regimes do not consistently protect consumer interests and are insufficient to comprehensively meet the challenges associated with the VMC age. The Article concludes by offering a detailed path forward.

[*] Professor of Law and Martin Luther King Jr. Hall Research Scholar, University of California, Davis School of Law (J.D., Harvard Law School; B.S., Cornell University). For helpful feedback, conversations, comments, or insights, I am grateful to Juliet Moringiello. I am also indebted to my research assistant, Nicholas Takton, for his invaluable help on this project. This article was supported by research grants from the University of California, Davis and the National Science Foundation ("NSF") Grant No. 2245373. The statements contained herein do not reflect the views or opinions of the NSF.

Introduction

> A car, to its driver, can feel like a sanctuary. A place to sing favorite songs off key, to cry, to vent or to drive somewhere no one knows you're going. But in truth, there are few places in our lives less private. . . . Once you've bought a car and you find it is bad at privacy, what are you supposed to do?[1]

> I felt like even though I made my payments and was never late under my contract, these people could do whatever they wanted, . . . and there was nothing I could do to stop them.[2]

> The idea is simple: We'll sell you a car with a dashcam, or that can be driven hands-free, or that can coach you with telematics data to be a better driver. But if you actually want to *use* any of the new toys, you'll have to pay extra.[3]

Imagine that you are driving in your vehicle on an isolated local road in a small town at night during a cross-country road trip to visit family for the holidays. You stop at a local convenience store or gas station. Once you have purchased snacks and gas, you get back in your vehicle, but the

1. Kashmir Hill, *Your Car Is Tracking You. Abusive Partners May Be, Too.*, N.Y. Times (Dec. 31, 2023), https://www.nytimes.com/2023/12/31/technology/car-trackers-gps-abuse.html (on file with the *Iowa Law Review*).

2. Michael Corkery & Jessica Silver-Greenberg, *Miss a Payment? Good Luck Moving That Car*, N.Y. Times: Dealbook (Sept. 24, 2014, 9:33 PM), https://archive.nytimes.com/dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car (on file with the *Iowa Law Review*).

3. Aarian Marshall, *With Subscriptions, Automakers Mimic Netflix's Playbook*, Wired (Oct. 12, 2021, 7:00 AM), https://www.wired.com/story/subscriptions-automakers-mimic-netflix [https://perma.cc/539C-TZMC].

vehicle will not start despite your best efforts, leaving you stranded. The tow truck company and mechanic that you contacted eventually identify the problem—a vehicle monitoring and collection ("VMC") technology[4] device installed in your vehicle as a condition of loan approval to purchase the vehicle. You learn that the VMC technology device has either malfunctioned or your lender (or a third party) remotely activated the device to disable your vehicle.

This is the 2022 story of a Georgia consumer whose vehicle contained a starter interrupt device ("SID"), a type of VMC technology that allows a lender to remotely disable and enable a vehicle's ignition.[5] The consumer alleged that, two years before the incident, he paid off the entirety of his loan balance and, therefore, fully owned the vehicle.[6] In describing his experience of being "stranded at night in a strange place," the consumer stated, "I'm past freaking out. I just felt helpless you know. I'm a big man and everything, but being in a strange place is kind of nerve-racking."[7]

This Georgia consumer's experience is not unique. VMC technology, including SIDs, and other GPS tracking devices are frequently used in vehicle agreements in subprime transactions. The vice president of one SID provider estimates that "up to [seventy] percent" of subprime borrowers' vehicles utilize VMC technology.[8] Like the Georgia consumer mentioned earlier, other consumers have claimed that their vehicles were remotely disabled despite making timely payments.[9] In one report, a lender used VMC technology to track and locate the vehicle "of a woman who had fled to a shelter to escape her abusive husband."[10] By moving to the shelter, the domestic violence victim allegedly violated a provision in her loan agreement that confined her driving movements to a specified "four-county radius."[11]

---

4. I use the term VMC technology in this Article to refer to the use of devices, computer programs, and associate systems to protect businesses' rights and support and guarantee loan payments in subprime lending transactions. Examples of VMC technology include starer interrupt devices, GPS tracking devices and computer programs, and smart Internet of Things systems that monitor users' vehicular activities or facilitate remote disablement of a vehicle's ignition or operations. Legal Action Chi., Comment Letter on Notice of Proposed Rulemaking, Motor Vehicle Dealers Trade Regulation Rule 2 (Sept. 12, 2022) [hereinafter Legal Action Chicago Comment Letter], https://downloads.regulations.gov/FTC-2022-0046-8097/attachment_2.pdf [https://perma.cc/NNG8-QPJS] (discussing various devices with kill switch capabilities, such as fuel line shutoff valves that "prevent fuel from flowing into the engine" and car battery disconnect switches that "prevent electricity from reaching the engine").

5. Harry Samler & Lindsey Basye, *Ga. Man Stranded After He Says Dealer's GPS Device Disabled His Car*, ATLANTA NEWS FIRST (Mar. 14, 2022, 10:50 AM), https://www.atlantanewsfirst.com/2022/03/14/he-paid-off-his-car-two-years-later-he-says-gps-device-left-him-stranded [https://perma.cc/J3KD-VQWU].

6. *Id.*

7. *Id.*

8. Jaeah Lee, *Wait, Banks Can Shut Off My Car?*, MOTHER JONES (Apr. 2016), https://www.motherjones.com/politics/2016/04/subprime-car-loans-starter-interrupt [https://perma.cc/UB78-H25G].

9. *Id.*

10. Corkery & Silver-Greenberg, *supra* note 2.

11. *Id.*

The woman feared that her allegedly abusive partner could determine her location from the tow-truck company who repossessed her vehicle.[12] At least one consumer has alleged that a lender remotely disabled their vehicle while driving on a highway using VMC technology.[13]

Increasingly, subscription-based models supported by VMC features,[14] such as over-the-air software updates that remotely disable or enable vehicular functions, have appeared in the non-subprime automobile context. Automobile companies have already implemented in connected vehicles subscription-based models with annual or monthly payments for vehicle options, such as optimal acceleration, heated seats, "adaptive cruise control," "semi-autonomous system[s]," "[a]utomatic crash notification" to emergency services, vehicle health updates, oil change notifications, and stolen vehicle notifications.[15]

---

12. *Id.*

13. *Id.*; *see also* Sean Patrick Farrell, *The Remote Repo Man*, N.Y. TIMES (Sept. 24, 2014), https://www.nytimes.com/video/business/100000003095109/the-remote-repo-man.html (on file with the *Iowa Law Review*) (describing these practices).

14. I use the term "VMC features" to describe vehicles that are accompanied by technology that remotely enables and disables select vehicular functions in connected (internet of things) vehicles to facilitate subscription business models in the non-subprime lending context. These features may share similarities with VMC technology in the subprime context but with respect to their impact may not be wholly identical to traditional SID and other kill switch devices used in the subprime context. For instance, a subscription for heated seats in a vehicle supported by VMC features may use technology, such as over-the-air software updates, to disable only a vehicle's heated seats for nonpayment while a traditional kill switch device in the subprime context may be installed directly in the vehicle and disable or enable the vehicle's engine and prevent a vehicle from starting and possibly negatively impact other vehicular functions. Historically, in subprime vehicular transactions with VMC technology "the debtor received a code every time she made a payment and the code enabled her to start the car until the next payment was due." Juliet M. Moringiello, *Automating Repossession*, 22 NEV. L.J. 563, 568 (2022). Modern VMC technology devices in subprime transactions can be accompanied by over-the-air firmware upgrades and "are able to disable a car remotely using GPS technology." *Id.*

15. Andrew J. Hawkins, *The Future of Cars Is a Subscription Nightmare*, VERGE (July 13, 2022, 12:31 PM), https://www.theverge.com/2022/7/13/23206999/car-subscription-nightmare-heated-seats-remote-start [https://perma.cc/8R7K-5ZHM] (driving optimization features); Aarian Marshall, Lauren Goode & Michael Calore, *Your Car's Future Is Loaded with Subscriptions*, WIRED: GADGET LAB (Apr. 6, 2023, 8:00 AM), https://www.wired.com/story/gadget-lab-podcast-593 [https://perma.cc/VEL3-VP5D] (driving optimization features, heated seats); Alistair Charlton, *BMW Wants to Charge You a Subscription for Your Heated Seats*, FORBES (July 2, 2020, 1:18 PM), https://www.forbes.com/sites/alistaircharlton/2020/07/02/bmw-wants-to-charge-you-a-subscription-for-your-heated-seats (on file with the *Iowa Law Review*) (heated seats); Mary DellaValle, *Vehicle Subscription Models Put a Twist on Consumer Choice*, TIRE REV. (May 17, 2021), https://www.tirerevieww.com/vehicle-subscription-consumer-choice [https://perma.cc/KBJ5-GRVP] (cruise control, semi-autonomous systems); Kim Komando, *Carmakers Are Charging for a Lifesaving Feature*, KOMANDO (Feb. 10, 2024), https://www.komando.com/money/car-subscription-services [https://perma.cc/9J6J-7ANH] (notifications to emergency services); Charlie Langton & David Komer, *Customers of Some New GM Cars Will Be Forced to Buy OnStar*, FOX 29 PHILA. (Aug. 10, 2022, 8:32 PM), https://www.fox29.com/news/customers-of-some-new-gm-cars-will-be-forced-to-buy-onstar [https://perma.cc/UH4T-A3LL] (vehicle health, oil changes, and stolen vehicle notifications). For a list of the companies deploying the novel business idea of having consumers use cars on a subscription-basis, as an alternative to leasing and renting a vehicle, see Clifford Atiyeh, *Car Subscription Services: A Complete Guide to Lease and Rental Alternatives*, FORBES: WHEELS (May 18, 2023), https://www.forbes.com/wheels/advice/car-subscription-services [https://perma.cc/2V

This business model contrasts with the traditional vehicle purchase setting in which consumers chose, at the time of sale, to purchase specific permanent vehicle options. Historically, these fixed consumer preselected options remained with a vehicle, even if the initial consumer resold the vehicle to a subsequent owner.[16] Subscription-based pricing may eventually be embraced in the used vehicle market.[17] Used vehicles are also sold in the subprime auto lending industry.[18] These subscription models and supporting technologies share notable similarities with VMC technology in the subprime lending context. For example, an individual who misses a subscription payment could find that the vehicle manufacturer has remotely disabled the associated vehicular features, such as auto-pilot or enhanced acceleration systems.

Admittedly, VMC technology may provide some benefits to consumers, vehicle dealers, and lenders. This technology could, in theory, decrease repossession costs, allow borrowers to quickly cure defaults, and perhaps increase borrowers' access to credit. In the non-subprime context, vehicles with VMC features could protect vehicles from theft by third parties, analyze drivers' behaviors to improve their driving, and improve product safety.[19] Despite these potential benefits, this Article contends that the rise in VMC

5N-MFDU]; Andrew Beckford, *All the Car Subscription Services Offered in the United States*, MOTORTREND (Aug. 31, 2023), https://www.motortrend.com/features/car-subscription-services-in-united-states [https://perma.cc/9KVL-BHMD].

16. Keith Barry, *Why You Might Need to Subscribe to Get Certain Features on Your Next Car*, CONSUMER REPS. (Dec. 15, 2021), https://www.consumerreports.org/cars/automotive-industry/why-you-might-need-to-subscribe-to-get-certain-features-on-your-next-car-a6575794430 [https://perma.cc/BW5C-4SLY]; Hawkins, *supra* note 15; Stephen Piepgrass & Daniel Waltz, *Regulators Likely to Focus on Hybrid Transactions and IoT Devices*, JDSUPRA (Apr. 2, 2021), https://www.jdsupra.com/legalnews/regulators-likely-to-focus-on-hybrid-1890321 [https://perma.cc/254X-TD4V].

17. Marshall et al., *supra* note 15 ("[A]utomakers adopted the subscription model where drivers pay to unlock features, and . . . the used car market will embrace it too."); Aarian Marshall, *Your Used Car May Soon Come with Subscription Fees*, WIRED (Apr. 6, 2023, 8:00 AM), https://www.wired.com/story/automakers-subscription-revenue-used-car-owners [https://perma.cc/T873-WV8D] ("Automakers' latest target in the subscriptions push—or shakedown, depending where and how comfortably you're sitting—is used car owners.").

18. Till v. SCS Credit Corp., 541 U.S. 465, 481 (2004) ("[S]everal considerations suggest that the subprime market is not, in fact, perfectly competitive. To begin with, used vehicles are regularly sold by means of tie-in transactions, in which the price of the vehicle is the subject of negotiation, while the terms of the financing are dictated by the seller."); Jessica Silver-Greenberg & Michael Corkery, *In a Subprime Bubble for Used Cars, Borrowers Pay Sky-High Rates*, N.Y. TIMES: DEALBOOK (July 19, 2014, 12:36 PM), https://archive.nytimes.com/dealbook.nytimes.com/2014/07/19/in-a-subprime-bubble-for-used-cars-unfit-borrowers-pay-sky-high-rates (on file with the *Iowa Law Review*) (discussing a review of "more than [one-hundred] bankruptcy court cases, [and] dozens of civil lawsuits against lenders," which found that "subprime auto loans can come with interest rates that can exceed [twenty-three] percent [and that] loans were typically at least twice the size of the value of the used cars purchased, including dozens of battered vehicles with mechanical defects hidden from borrowers").

19. *See* Annalise Frank, *Thieves Across America Are Stealing Hyundais and Kias in Seconds*, AXIOS (Aug. 27, 2022), https://www.axios.com/2022/08/27/kia-hyundai-thefts-stolen-usb-immobilizer-tiktok [https://perma.cc/9JPS-7NMM]; Jason Knowles & Ann Pistone, *Carjacking Tech: How Police Are Using GPS Products to Track Down Stolen Cars*, ABC 7 CHI. (Feb. 5, 2021), https://abc7chicago.com/carjacking-prevention-carjackings-chicago-stolen-car-gps-tracking/10316715 [https://perma.cc/UD4Y-3H8A].

technology and features, in both subprime and non-subprime consumer automobile transactions, raises several alarming privacy, electronic subjugation, and cybersecurity risks. It also raises practical concerns, such as who should bear responsibility for removing or permanently disabling such technology upon satisfaction of loan obligations.

Several academics and commentators have evaluated the commercial and consumer protection implications of VMC technology in subprime automobile lending transactions.[20] This Article is unique in the following four ways: First, this Article contributes to the existing body of scholarship in this area by conducting an in-depth exploration of the privacy, electronic subjugation, and cybersecurity risks associated with VMC technology. Second, this Article makes an express link between the consumer risks and harms associated with the use of VMC technology in subprime lending transactions and the broader technological shift towards a subscription-based service model supported by VMC features in non-subprime connected vehicle transactions. Third, this Article's evaluation and critique of VMC technology and features is conducted simultaneously through the lens of commercial law, state VMC technology laws, state privacy laws, such as the California Consumer Privacy Act of 2018 ("CCPA"),[21] and federal frameworks governing transactions involving consumer vehicles. I argue that these legal regimes do not consistently protect consumer interests and are insufficient to comprehensively meet the challenges associated with the VMC age. Fourth, this Article is also the first legal scholarship to evaluate in-depth the efficacy and potential impact of the Federal Trade Commission's ("FTC") Combating Auto Retail Scams Trade Regulation Rule ("CARS Rule") in remedying the consumer harms that flow

20. *See, e.g.*, Juliet M. Moringiello, *Electronic Issues in Secured Financing*, *in* RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW 285, 297–303 (John A. Rothchild ed., 2016) (discussing the impact that electronic communications, such as SIDs, have had on secured transactions law); STACY-ANN ELVY, A COMMERCIAL LAW OF PRIVACY & SECURITY FOR THE INTERNET OF THINGS 196–243 (2021) (exploring the rise of asset collection technology); Moringiello, *supra* note 14, 568–70 (discussing whether creditors have the right to remotely disable collateral upon a debtor's default); Rebecca Crootof, *The Internet of Torts: Expanding Civil Liability Standards to Address Corporate Remote Interference*, 69 DUKE L.J. 583, 646–66 (2019) (discussing how to expand legal liability for remotely disabling a vehicle and other such capabilities); Kwesi D. Atta-Krah, Note, *Preventing a Boom from Turning Bust: Regulators Should Turn Their Attention to Starter Interrupt Devices Before the Subprime Auto Lending Bubble Bursts*, 101 IOWA L. REV. 1187, 1209–12 (2016) (discussing why subprime lenders should refrain from using SIDs in their underwriting); Laura Harper, Note, *Did the Repo Man Just Ghost Me? Technology's Contribution to Vehicle Repossession and How It Impacts the UCC*, 38 REV. LITIG. 373, 377–84 (2019) (discussing how SIDs and similar technology impacts the Uniform Commercial Code ("UCC")); Charles Seby, Comment, *Securing Transactions with Technology: Revising Article 9 to Address Remote Electronic Default Remedies*, 58 JURIMETRICS 459, 472–77 (2018) (arguing that Article 9 of the UCC should be revised in light of these new technologies); Erica N. Sweeting, Comment, *Disabling Devices: Adopting Parameters for Addressing a Predatory Auto-Lending Technique on Subprime Borrowers*, 59 HOW. L.J. 817, 845–46 (2016) (arguing for stricter regulations of devices capable of remotely disabling vehicles).

21. CAL. CIV. CODE §§ 1798.100–.199.100 (West 2022).

from VMC technology.[22] The CARS Rule is currently the subject of an ongoing legal challenge from the National Automobile Dealers Association and the Texas Automobile Dealers Association.[23] If the CARS Rule survives this challenge, it is expected to impact not just automobile dealers but also ancillary entities, such as "banks, finance companies affiliated with original equipment manufacturers, and other nonbank auto finance companies."[24]

This Article offers a detailed path forward to remedy concerns associated with the rise of VMC technology and features, including amending existing sources of law to impose restrictions on the use of such technology. For instance, in 2021, Illinois proposed a bill that would have prohibited the activation of SIDs "in any vehicle solely as a means to secure payment on the vehicle."[25] Other alternative solutions include enhancing state law governing VMC technology by imposing limits on data collection, use, and retention, and restricting companies' ability to condition lending arrangements on the installation of VMC technology. When applicable, state secured lending laws can also provide that remote disablement of consumer vehicles via VMC technology constitutes a constructive repossession subject to existing breach of the peace limitations. Given the public, societal and collective value of privacy, the critical role it plays in our democracy, and the impact a single individual's privacy choices may have on others and society,[26] courts can also consider privacy harms in determining whether a breach of the peace has occurred as part of a repossession or disablement conducted via VMC technology. Beyond the secured lending context, federal legislation, such as an omnibus privacy statute that restricts the power and timing of consent and

22. *See generally* Combating Auto Retail Scams Trade Regulation Rule, 89 Fed. Reg. 590 (Jan. 4, 2024) (to be codified at 16 C.F.R. pt. 463) (although the CARS Rule was initially set to become effective on July 30, 2024, its enactment remains delayed until further notice because of a pending legal challenge).

23. Petitioners' Opposed Motion for Stay of Final Rule and for Expedited Consideration at 1, Nat'l Auto. Dealers Ass'n v. FTC, No. 24-60013 (5th Cir. Jan. 8, 2024); Combating Auto Retail Scams Trade Regulation Rule, 89 Fed. Reg. 13267 (Feb. 22, 2024) (to be codified at 16 C.F.R. pt. 463) ("Because of a pending legal challenge, this document announces that the effective date of the [Combating Auto Retail Scams Trade Regulation Rule] is delayed until further notice."); *see also* Fed. Trade Comm'n, Order Postponing Effective Date of Final Rule Pending Judicial Review 1 (Jan. 18, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/P204800CARSExtensionOrder.pdf [https://perma.cc/E3BD-C3YF] (postponing the effective date of the rule); Daniel Savrin, David Monteiro & Allen Denson, *What FTC CARS Rule Means for Auto Dealers and Lenders*, LAW360 (Jan. 16, 2024, 4:55 PM), https://www.law360.com/articles/1785264/what-ftc-cars-rule-means-for-auto-dealers-and-lenders (on file with the *Iowa Law Review*) (describing the case and delay).

24. Savrin et al., *supra* note 23; Jeff Greenbaum, *FTC Releases New "Combating Auto Retail Scams Rule,"* LEXOLOGY (Dec. 13, 2023), https://www.lexology.com/library/detail.aspx?g=4d4b8b2d-0814-4a06-bc26-7072020a977d&utm [https://perma.cc/S8UL-UVVH] ("The CARS Rule applies to the sale of most self-propelled motor vehicles, but doesn't generally cover boats, motorcycles, scooters, electric bicycles, motor homes, and golf carts.").

25. H.B. 3216, 102d Gen. Assemb., Reg. Sess. (Ill. 2021).

26. *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY xv–xvi, 225 (1995) ("[P]rivacy is a common value in that it is shared by individuals, a public value in that it has value to the democratic political system, and a collective value in that technology and market forces make it increasingly difficult for any one person to have privacy unless everyone has a similar minimum level of privacy.").

imposes limits on permissible and impermissible data practices, could help address the attendant privacy and cybersecurity concerns. Congress could also evaluate recent calls for the imposition of various fiduciary duties, such as a duty of loyalty and a duty to avoid unreasonable risks.[27] Congress, states, and existing regulatory bodies with authority can provide guidance on subscription-based models in the connected vehicle context. State privacy laws can move beyond a rights-based and notice-and-choice approach to better address privacy and electronic subjugation risks by more adequately addressing data discrimination and enforcing existing obligations, such as data minimization.

The privacy concerns raised by VMC technology in subprime lending transactions includes the increased risk of monitoring by lenders and other third parties who can obtain access to data about individuals' daily vehicular activities. There is also the risk of data aggregation and resulting analysis that facilitates both expected and unexpected data uses. Secondary use of data collected by VMC technology for purposes other than those initially approved by drivers is a concerning privacy risk.[28] Without sufficient restrictions, data collected by VMC technology can be combined with other sources of data about individuals to reveal important insights about individuals. Specifically, VMC data can reveal highly sensitive information about an individual, including his or her precise location, frequently visited places, political preferences, and health status. There are also concerns associated with the risk of exclusion and worsening existing discrimination. As is the case in other settings, hacking incidents, data leaks, and other instances of improper storage may also occur in the VMC context. There are also electronic subjugation concerns associated with VMC technology to the extent that consumers have significantly less control over their vehicles' operations in comparison to transactions in which such devices or features are not used.

Non-subprime consumer transactions involving subscription services enhanced by VMC features in connected vehicles also raise similar privacy and cybersecurity concerns. Connected vehicles increasingly collect large quantities of data about drivers and their behaviors, thereby raising privacy concerns. Modern connected vehicles can collect information about fluctuations in drivers' weight, how fast they drive, how many children they have, and their financial information, among other things.[29] Connected vehicles can also

27. *See, e.g.*, Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1206 (2016) ("Although professional malpractice and professional breach of duty normally arise out of a contract, courts regularly enforce tort duties that do not have to be spelled out in a contract or explicitly agreed to by the parties; they also award tort damages. That is also true with respect to duties about information." (footnote omitted)); Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593, 632–37 (2024) [hereinafter Solove, *Murky Consent*] (discussing various possible duties, including that of loyalty).

28. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 490–91, 507, 515, 520–22 (2006) [hereinafter Solove, *A Taxonomy of Privacy*] (listing surveillance, aggregation, secondary use, and insecurity, among others, as privacy risks).

29. Bill Hanvey, Opinion, *Your Car Knows When You Gain Weight*, N.Y. TIMES (May 20, 2019), https://www.nytimes.com/2019/05/20/opinion/car-repair-data-privacy.html (on file with the *Iowa Law Review*).

track drivers' eye movements and detect their heartbeats.[30] This data collection increases once a driver connects their smartphone to their vehicle.[31] It is estimated that connected vehicles collect "as much as [twenty-five] gigabytes of data per hour."[32]

Automobile manufacturers have revealed plans to deploy VMC features in ways that are similar to the use of VMC technology in subprime transactions. Thus, even consumers with excellent credit scores may face similar risks. The preexisting risks associated with connected vehicles may be exacerbated by subscription vehicle services associated with VMC features. Ford Motor Company applied for a patent that would "enable a computer to disable a vehicle or component of a vehicle over delinquent car payments and could lead to cars self-driving themselves to repossession lots."[33] The patent application also notes that the vehicle's camera could determine if the consumer attempts to hinder virtual repossession efforts and transmit the vehicle's GPS location to the police department to stop such efforts.[34] Although not all patent applications are approved, if implemented this technology could lead police to make unwarranted stops based on the incorrect assumption that a vehicle is stolen.[35] This risk is particularly alarming for members of historically over-policed groups.

Beyond the Ford patent example, it is also possible that automobile manufacturers will more widely incorporate technology with remote disablement capabilities in new vehicles in the next few years. In accordance with the Infrastructure Investment and Jobs Act, the National Highway Traffic Safety Administration has begun rulemaking proceedings to issue standards mandating the potential inclusion of "advanced drunk and impaired driving prevention technology" in new vehicles to "prevent or limit motor vehicle operation if an

30. Jen Caltrider, Misha Rykov & Zoë MacDonald, *What Data Does My Car Collect About Me and Where Does It Go?*, MOZILLA: PRIV. NOT INCLUDED (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go [https://perma.cc/F4GT-EASU]; *see also* Letter from Edward J. Markey, U.S. Sen., to James D. Farley, Jr., President & CEO, Ford Motor Co. 1 (Nov. 30, 2023) [hereinafter Markey Letter], https://www.markey.senate.gov/imo/media/doc/senator_markey_letter_to_automakers_on_privacy.pdf [https://perma.cc/PKT5-6N2H] (referring to the 2023 Mozilla report).

31. Hanvey, *supra* note 29.

32. *Id.*

33. Michael Sainato, *Ford Seeks to Remotely Repossess Cars After Missed Payments in US Patent*, GUARDIAN (Mar. 3, 2023, 12:35 PM), https://www.theguardian.com/business/2023/mar/03/ford-reposses-patent-remote-lock [https://perma.cc/JB7M-WKW5]; Tim Cushing, *Ford Submits a Patent That Would Allow Cars to Repossess Themselves*, TECHDIRT (Mar. 6, 2023, 1:40 PM), https://www.techdirt.com/2023/03/06/ford-submits-a-patent-that-would-allow-cars-to-repossess-themselves [https://perma.cc/5W7Q-KBW2]. For the actual application, see U.S. Patent Application Pub. No. 2023/0055958 A1 (filed Aug. 20, 2021) [hereinafter Ford Patent Application], https://image-ppubs.uspto.gov/dirsearch-public/print/downloadPdf/20230055958 [https://perma.cc/WM54-GQE2].

34. Ford Patent Application, *supra* note 33, at 10 (discussed at [0049]).

35. Cushing, *supra* note 33.

impairment is detected."[36] While this potential technology seeks primarily to address drunk driving concerns, given its proposed ability to remotely disable motor vehicle operations upon detecting drunk driving, this technology may eventually share some similarities with the kill switch or remote disablement features of VMC technology in subprime settings. Regardless of the context, connected vehicles with remote disablement capabilities raise significant concerns about unnecessary data collection, uncontrolled monitoring, cybersecurity, and problematic monetization concerns. The last set of concerns include the potential sale of collected data and the aggregation of such data with other sources of information about drivers to generate significant insights about a person's activities.

With respect to subscription-based services supported by VMC features, one car manufacturer previously implemented an eighteen dollar per month subscription program for heated seats, and also offers subscriptions for other vehicle features.[37] Another vehicle manufacturer has charged drivers a monthly subscription fee "to remotely start vehicles using a key fob — a feature that had previously been free."[38] Other automobile companies have used subscription model pricing for select vehicle options as well.[39] In some cases, as alluded to above, these vehicle options were previously offered to consumers for free.[40] It is estimated that in 2021 General Motors ("GM")

36. Infrastructure Investment and Jobs Act, Pub. L. No. 117–58, 135 Stat. 429 § 24220 (2021); Advanced Impaired Driving Prevention Technology, 89 Fed. Reg. 830, 830–31 (proposed Jan. 5, 2024) (to be codified at 49 C.F.R. pt. 571) ("The Infrastructure Investment and Jobs Act (Bipartisan Infrastructure Law or BIL) directs NHTSA to issue a final rule establishing a Federal Motor Vehicle Safety Standard (FMVSS) that requires new passenger vehicles to have 'advanced drunk and impaired driving prevention technology' by 2024."); *see also* Press Release, Nat'l Highway Traffic Safety Admin., NHTSA Takes First Step Toward Impaired Driving Prevention Standard to Save Lives, Launches Holiday Drive Sober Campaign (Dec. 12, 2023), https://www.nhtsa.gov/press-releases/drive-sober-campaign-launch-winter-2023 [https://perma.cc/4W9E-NN6S] (announcing the program); Ian Duncan, *Car Safety Agency Takes Step Toward Requiring Anti-Drunk Driving Tech*, WASH. POST (Dec. 12, 2023, 2:59 PM), https://www.washingtonpost.com/transportation/2023/12/12/nhtsa-drunk-driving-technology-mandate (on file with the *Iowa Law Review*) (describing the program).

37. Hawkins, *supra* note 15; Chris Morris, *BMW Jumps into Microtransactions: Begins Selling Heated Seat Subscriptions in South Korea*, FORTUNE (July 12, 2022, 10:44 AM), https://fortune.com/2022/07/12/bmw-heated-seats-subscription-microtransactions-south-korea/amp [https://perma.cc/6C4E-Q5DF] (discussing the BMW heated seat feature and noting that the "features are activated (and deactivated) via an over-the-air software update between the vehicle and a BMW app"); Sean Tucker, *BMW Quietly Launches In-Car Subscriptions in U.S.*, KELLEY BLUE BOOK (Jan. 9, 2023, 8:21 AM), https://www.kbb.com/car-news/bmw-quietly-launches-in-car-subscriptions-in-u-s [https://perma.cc/E3CZ-H7BV] (discussing BMW vehicle subscriptions, including heated seats, remote engine start, driver recorder, parking assistant, and others).

38. Theo Wayt, *Auto Giants Like BMW, GM and Toyota Make Drivers 'Subscribe' for Basic Features*, N.Y. POST (Aug. 21, 2022, 1:49 PM), https://nypost.com/2022/08/21/auto-giants-like-bmw-gm-and-toyota-make-drivers-subscribe-for-basic-features [https://perma.cc/8URU-9TC2].

39. Hawkins, *supra* note 15 ("Volkswagen, Toyota, Audi, Cadillac, Porsche, and Tesla have all dabbled in subscription models for certain options.").

40. H. Dennis Beaver, *Automakers' Added Subscription Fees Raise Legal Questions*, KIPLINGER (Jan. 2, 2024), https://www.kiplinger.com/personal-finance/automakers-added-subscription-fees-raise-legal-questions [https://perma.cc/8754-BMJV] ("Other automakers — Audi, Cadillac, Porsche,

earned more than "$2 billion in in-car subscription service revenue" and the company hopes that, by 2031, that number will increase to $25 billion, which "would essentially put GM in the same league as Netflix, Spotify, and Peloton."[41]

Tesla reportedly remotely disabled the auto-pilot system in an individual's vehicle for nonpayment and then subsequently re-enabled the features after its actions became public.[42] Consider that, in 2023, reports indicated that Volkswagen refused to reactivate connected emergency service on a customer's stolen vehicle without payment of a $150 subscription fee despite police requests.[43] As a result, police had to resort to other means to rescue the child left inside the vehicle.[44]

While the discontinuation or remote disablement of heated seats and other nonessential vehicle options may have minor implications, other types of subscription-based pricing attached to more essential vehicle functions, or the safety features of a vehicle, such as automatic breaking, may present more significant concerns. For instance, in 2022 Mercedes announced plans to implement an "Acceleration Increase" subscription service in which vehicle owners must pay an annual $1,200 fee to increase motor performance.[45] The service boosts torque and output from the vehicle's motor by twenty to twenty-four percent and shaves nearly a second "off [zero to sixty mile per

---

Tesla and Volvo — are instituting a subscription model for certain options where a customer would pay a monthly or annual fee for such features as active driving assistance or voice recognition, even though they are already built into the car and, in some cases, have been free to use for years.").

41. Hawkins, *supra* note 15; *see also* Langton & Komer, *supra* note 15 ("General Motors is bumping up the sticker price on many of its new vehicles adding a mandatory OnStar subscription, whether you want it or not" and the $1,500 price "will be tacked on to the purchase price which gets you three years of access to OnStar— and then, after the three years, you start paying monthly or the device will be dropped."); Jamie L. LaReau, *OnStar Faces Firestorm over Baby in Locked Car, Tries to Explain What Happened*, DET. FREE PRESS (Aug. 15, 2019, 9:22 AM), https://www.freep.com/story/money/cars/general-motors/2019/08/14/onstar-baby-car-gm/2009929001 [https://perma.cc/5ESA-GH86] (discussing GM's OnStar subscription service and reporting that OnStar services nowadays work as follows: "[O]nce an OnStar plan expires or is cancelled, the OnStar system is deactivated and our connection to the vehicle is removed.").

42. Sean O'Kane, *Tesla Owner Says Remotely Disabled Autopilot Features Have Been Restored*, VERGE (Feb. 13, 2020, 4:24 PM), https://www.theverge.com/2020/2/13/21136699/tesla-autopilot-used-model-s-owner-restored-assistance-features [https://perma.cc/XNC2-UG5L]. *But see* Nick Statt, *Tesla Remotely Disables Autopilot on Used Model S After It Was Sold*, VERGE (Feb. 6, 2020, 7:03 PM), https://www.theverge.com/2020/2/6/21127243/tesla-model-s-autopilot-disabled-remotely-used-car-update [https://perma.cc/7GZ9-TWCD] (discussing how Tesla, in another case, maintained the deactivation of features once purchased by a third-party, stating that the new owner had not paid for them).

43. Jon Fingas, *VW's Connected Emergency Service Is Free for 5 Years After Botched Carjacking Response*, ENGADGET (Mar. 8, 2023), https://www.engadget.com/vws-connected-emergency-service-is-free-for-5-years-after-botched-carjacking-response-144502763.html [https://perma.cc/XP3X-9D6F].

44. *Id.* (noting, in addition, that in response to concerns, the company made its connected emergency services free for a five-year period on select vehicles).

45. Jess Weatherbed, *Mercedes Locks Faster Acceleration Behind a $1,200 Annual Paywall*, VERGE (Nov. 23, 2022, 7:24 AM), https://www.theverge.com/2022/11/23/23474969/mercedes-car-subscription-faster-acceleration-feature-price [https://perma.cc/R9VG-58V5].

hour] acceleration."[46] A vehicle's acceleration relates to vehicle safety and functionality.[47] Somewhat similarly, Tesla charged customers a $3,250 fee to unlock "the full battery capacity" of older model Teslas.[48] It is certainly possible that, in the near future, automobile manufacturers could offer subscription services to "unlock extra range for road trips" or make vehicles more efficient.[49] A 2022 proposed bill in New Jersey would have restricted automobile firms' ability to engage in this practice.[50] There was a similar proposal in Pennsylvania in 2023.[51]

Automobile manufacturers increasingly use VMC features to facilitate limiting the full functionality of factory equipped vehicle hardware to enable software-supported subscription services to increase revenue streams post-transaction, even though they may, traditionally, already factor the price of the hardware into the overall purchase price.[52] In this context, electronic subjugation potentially occurs through a series of microtransactions under a subscription-based model. Even a driver who has paid off their loan balance and has title to a vehicle may need to continue making monthly payments to use existing hardware in the vehicle.

The increasing shift to a subscription model supported by VMC features in the automobile industry presents risks akin to the use of VMC technology

---

46. *Id.*; *see also* Jon Fingas, *Mercedes' New EV Innovation Is a Paywall on Your Car's Performance*, ENGADGET (Nov. 23, 2022), https://www.engadget.com/mercedes-acceleration-increase-ev-subscription-230058550.html [https://perma.cc/FVL8-MWKJ] (detailing what is included in the paid subscription service).

47. *See, e.g.*, Bob Fredericks & Post Wires, *Toyota to Pay $1.2B Settlement in Vehicle Acceleration Lawsuit*, N.Y. POST (Mar. 19, 2014, 9:19 AM), https://nypost.com/2014/03/19/toyota-to-pay-1-2b-settlement-in-vehicle-acceleration-lawsuit [https://perma.cc/VU8E-22B5] (discussing a lawsuit involving safety issues associated with vehicle acceleration features).

48. Jordan Golson, *The Refreshed Tesla Model S 70 Lets You Pay to 'Unlock' a Bigger Battery*, VERGE (May 5, 2016, 9:13 AM), https://www.theverge.com/2016/5/5/11597508/tesla-model-s-70-battery-upgrade-pay-unlock-battery [https://perma.cc/G6SR-BWR2].

49. Tim Levin, *Car Companies Want to Make Billions by Charging Monthly Fees for Features Like Heated Seats, but Buyers Won't Pay Up*, BUS. INSIDER (Nov. 21, 2022, 9:54 AM), https://www.businessinsider.com/car-feature-subscriptions-add-ons-bmw-ford-toyota-gm-2022-2 (on file with the *Iowa Law Review*).

50. S.B. 3271, 220th Leg., Reg. Sess. (N.J. 2022) ("This bill prohibits a motor vehicle dealer or manufacturer of motor vehicles sold in this State from offering to a consumer a subscription service for any motor vehicle feature that (1) utilizes components and hardware already installed on the motor vehicle at the time of the vehicle's purchase or lease; and (2) would function after activation without ongoing expense to the dealer, manufacturer, or third-party service provider.").

51. *See* Memorandum from Pa. Sen. Marty Flynn to the Members of the Pa. Sen. (Mar. 21, 2023), https://www.legis.state.pa.us/cfdocs/Legis/CSM/showMemoPublic.cfm?chamber=S&SPick=20230&cosponId=40247 [https://perma.cc/ZT43-9TUP].

52. *See* Hawkins, *supra* note 15. With the dip in global sales for new cars in recent years, "car manufacturers have pivoted toward selling software updates and features as subscriptions to generate a continuous revenue stream long after a car has been purchased." Weatherbed, *supra* note 45. The paywalling by Mercedes of its vehicles' performance "is part of an emerging, more loathsome trend that sees auto brands restricting the capabilities of hardware that already comes factory-equipped with the vehicle." *Id.*; *see also* Tom Gerken, *Mercedes-Benz to Introduce Acceleration Subscription Fee*, BBC (Nov. 24, 2022), https://www.bbc.com/news/technology-63743597 [https://perma.cc/MZT6-JPW7] (discussing the fee).

in subprime consumer lending transactions and may worsen concerns associated with connected vehicles. Both VMC technology and subscription model arrangements in connected vehicles with VMC features highlight a broader technological and societal shift in which consumers have significantly less control over the modern-day goods they purchase. Indeed, in today's world, device manufacturers, lenders, and other entities increasingly retain electronic control of modern goods post-transaction. The digital subjugation power of these entities continues to grow exponentially. As Professor Joshua Fairfield has argued, with the rise of Internet of Things ("IoT") technology and associated smart systems, "[w]e risk becoming digital peasants, owned by software and advertising companies, not to mention overarching governments."[53]

Admittedly, subscription-based pricing has dominated the IoT space for several years. For instance, the Nest Learning Thermostat, which uses some level of artificial intelligence to understand consumers' preferences and adjusts the temperature and energy use in homes based on those preferences, is accompanied by a video and cloud subscription service.[54] Subscription models are also in use in music and movie streaming services. However, the growing use of this model in the automobile industry in connected vehicles, which are part of the IoT, is relatively more nascent and raises distinct concerns for consumers. A vehicle plays a different but essential role in consumers' lives, particularly in comparison to an IoT camera, thermostat, or streaming service operating on a subscription model. Thus, the extent of digital subjugation post-transaction is particularly alarming in the vehicular context. Subscription-based models combined with VMC features also raise additional questions, such as whether the scope of basic vehicle warranties will be sufficient to extend to vehicle parts connected to subscription services.

The remainder of this Article proceeds as follows: Part I conducts an in-depth exploration of the consumer risks associated with VMC technology in subprime transactions as well as those associated with VMC features that enable subscription services in non-subprime connected vehicle transactions.

---

53. JOSHUA A.T. FAIRFIELD, OWNED: PROPERTY, PRIVACY, AND THE NEW DIGITAL SERFDOM i (2017); *see also* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET–AND HOW TO STOP IT 106 (2008) (contending that the connected goods are no longer the static physical objects that have dominated the consumer marketplace, and which, "once placed with an individual, belong[] to that person").

54. *Nest Learning Thermostat*, GOOGLE STORE, https://store.google.com/product/nest_learning_thermostat_3rd_gen?hl=en-US [https://perma.cc/55KF-2K5N] (showcasing features that necessitate a subscription); *see also* Daniel Faggella, *Artificial Intelligence Plus the Internet of Things (IoT) - 3 Examples Worth Learning From*, EMERJ (Oct. 23, 2019), https://emerj.com/ai-sector-overviews/artificial-intelligence-the-internet-of-things-iot-3-examples-worth-learning-from [https://perma.cc/99ZZ-2MXM] ("Nest's device 'learns' the regular temperature preferences of it's [sic] users, and also adapts to the work schedule of it's [sic] users by turning down energy use."); Corinne Iozzio, *Artificially Intelligent Thermostat Automatically Creates a Climate Schedule for You*, POPULAR SCI. (Jan. 21, 2012, 12:36 AM), http://www.popsci.com/gadgets/article/2011-12/artificially-intelligent-thermostats-learns-adapt-automatically [https://perma.cc/WC5V-ATYZ] (describing the Nest thermostat as an "[a]rtificially [i]ntelligent [t]hermostat"); Steven Levy, *How Nest Is Creating the Conscious Home, One Smart Device at a Time*, WIRED (Dec. 17, 2013, 9:01 AM), https://www.wired.com/story/where-there-is-smoke (on file with the *Iowa Law Review*) (discussing the Nest thermostat's use of artificial intelligence).

This Part argues that VMC technology and features raise monitoring, data aggregation, subsequent use, exclusion, cybersecurity, and electronic domination risks. This technology may also worsen existing concerns about discrimination. Part II evaluates some of the legal frameworks potentially applicable to VMC technology and features, including Article 9 of the Uniform Commercial Code ("UCC"), state statutes directly regulating VMC technology, comprehensive state privacy laws, and some federal frameworks, such as the FTC's CARS Rule and the Equal Credit Opportunity Act. This Part posits that these existing frameworks often do not consistently address the concerns highlighted in Part I.

Part III offers concrete solutions to the privacy, electronic subjugation, and cybersecurity risks identified in Part I. These solutions include enhancing restrictions in various sources of law on VMC technology and subscription-based services supported by VMC features. For instance, to the extent that they do not already, state laws can restrict companies' ability to collect data about consumers using VMC technology by limiting data collection and surveillance to the period after a default. Likewise, Article 9 of the UCC could provide that a remote disablement qualifies as a constructive repossession that is subject to breach of the peace limitations and impose data use and disclosure restrictions. Article 9 could also make clear that the breach of the peace standard applies to remote disablements in consumer transactions. Courts might elect to consider privacy and other types of harms when determining whether a secured party has breached the peace. More broadly, an omnibus federal privacy statute may be helpful in mitigating against harms associated with the use of VMC features in non-subprime transactions and the privacy concerns raised by connected vehicles. Congress, states, and existing regulatory bodies should provide guidance on the use of subscription-based models supported by VMC features in consumer vehicle transactions.

I. CONSUMER CONCERNS

This section exposes the various privacy risks, including monitoring, aggregation, subsequent use, data exclusion, and worsening existing discrimination that may flow from VMC technology and features. VMC technology and features in the vehicle context also expands the digital powers of corporate entities and allows them to exercise significant control over drivers post-transaction. Regardless of the context, whenever there is surveillance and data collection via connected objects, there is always the risk of cybersecurity failures. Older model vehicles and newer connected smart vehicles are no exception. All of these risks—privacy, electronic subjugation, and cybersecurity—are present in both the subprime lending context and the non-subprime setting, even though there may be differences with respect to the level of risk or invasion.

A. *PRIVACY RISKS*

By 2025, there will be 293 million IoT vehicles in use.[55] Connected vehicles accompanied by subscription services and VMC features fit squarely within the IoT. Since 2020, "most new cars sold in the United States" have "built-in Internet connections, including [one-hundred] percent of Fords, GMs and BMWs and all but one model [of] Toyota and Volkswagen [vehicles]."[56] While subprime automobile lending transactions can involve both used and new vehicles, used or older vehicles may not always have a direct internet connection.[57] However, these older vehicles can easily enter the IoT through the installation of a SID or other tracking device. The installation of VMC technology in used and older vehicles establishes a connection to external devices and systems linked to the internet (and other networks), thereby ushering these older vehicles into the IoT. Notably, even the "onboard diagnostics" ports in vehicles manufactured after 1996 can help connect older model automobiles to the IoT.[58] Eventually, more modern connected vehicles with subscription services enhanced by VMC features are likely to make their way into the used subprime vehicle lending market and older non-IoT vehicles may become obsolete. Thus, both subprime and non-subprime vehicles pose privacy risks.

---

55. Rachel Green, *Honda and AutoNavi Are Partnering on a Connected Car Platform*, BUS. INSIDER (Jan. 4, 2018), https://finance.yahoo.com/news/honda-autonavi-partnering-connected-car-160405798.html (on file with the *Iowa Law Review*).

56. Geoffrey A. Fowler, *What Does Your Car Know About You? We Hacked a Chevy to Find Out*, WASH. POST (Dec. 17, 2019, 7:00 AM), https://www.washingtonpost.com/technology/2019/12/17/what-does-your-car-know-about-you-we-hacked-chevy-find-out (on file with the *Iowa Law Review*).

57. Holly Johnson, *Everything You Need to Know About Subprime Auto Loans*, CAP. ONE AUTO NAVIGATOR (May 6, 2022), https://www.capitalone.com/cars/learn/managing-your-money-wisely/everything-you-need-to-know-about-subprime-auto-loans/1488 [https://perma.cc/A6P6-TKCH] ("[T]he average deep subprime borrower had an interest rate of 12.53% on new cars as of the fourth quarter of 2021, and the average subprime borrower paid an average rate of 9.41%. Compare that to the average rate for prime and super-prime borrowers that same quarter, which worked out to 3.51% and 2.47%, respectively. . . . [T]he average deep subprime borrower had an interest rate of 19.87% on used cars as of the fourth quarter of 2021, and the average subprime borrower paid an average rate of 15.96%. Compare that to the average rate paid by prime and super-prime borrowers for used cars that same quarter, which worked out to 5.38% and 3.61%, respectively. . . . [Y]ou can purchase a new car or look for a good deal on a used car as a subprime borrower. You'll just have to pay more interest on your auto loan to do so."); Wolf Richter, *Subprime Auto-Loan Delinquencies Hit Record, Prime Loans Are Pristine, After Easy Money Ends: The High-Risk High-Profit Business of Subprime Auto Lending*, WOLF ST. (Oct. 22, 2023), https://wolfstreet.com/2023/10/22/subprime-auto-loan-delinquencies-hit-record-prime-loans-are-pristine-after-easy-money-ends-the-high-risk-high-profit-business-of-subprime-auto-lending [https://perma.cc/2LU3-FRC6] ("Typically, subprime-rated borrowers purchase older, such as 10-year-old or older, used vehicles with those loans," often accepting interest rates higher than those of new cars, "because that's the only thing they qualify for.").

58. Liz Slocum Jensen, *Onboard Diagnostics Will Connect Cars to the Internet of Things*, VENTUREBEAT (Aug. 7, 2016, 5:13 AM), https://venturebeat.com/2016/08/07/onboard-diagnostics-will-connect-cars-to-the-internet-of-things [https://perma.cc/WN2R-UR4W]. In today's world, there exist "a variety of [onboard diagnostic, or] OBD-II dongles that plug into the diagnostics port of every car sold in the U.S. since 1996." *Id.* Leveraging data from those ports can "bring any car into the Internet of Things (IoT) and will prove valuable when merged with contextual computing." *Id.*

1. Monitoring and Data Acquisition

VMC technology could permit periodic and even continuous monitoring and tracking of consumers and their vehicles. This tracking could occur both before and after a default, a reality some describe as a "privacy tax."[59] The devices of one provider include capabilities such as "pinpoint GPS" tracking and geofencing features, "speed alerts," "[a]utomated [forty-nine]-hour tracking" and text and email alert payment reminder features.[60] Another VMC technology provider offers products with "[d]aily [d]evice [h]istory," "[v]ehicle [i]nformation," and "[e]xcessive [m]ileage" reports, and, in some cases, starter interrupt features.[61] As the Consumer Financial Protection Bureau ("CFPB") has noted, "some lenders require access to GPS locators so that they always know where a car is physically located."[62]

According to a *New York Times* investigation, one VMC technology provider allegedly lost business because it ensured that lenders could not turn on its tracking device until after a borrower defaulted.[63] This revelation suggests that perhaps some dealers or lenders may prefer VMC devices that collect data about consumers and track their driving activities before default. The investigation also uncovered that a director of collections at a credit union could "monitor the movements of about 880 subprime borrowers on a computerized map that shows the location of their cars with a red marker" and "spot drivers who [were] behind on their payments."[64]

Similar concerns extend to technologies that possess VMC features, such as remote disablement of vehicular functions, that enable subscriptions services in the non-subprime lending context. Recall that most vehicle subscription services are provided to consumers with newer model connected vehicles.[65] Connected vehicles act as both agents of surveillance and data-

59. Kashmir Hill, *People with Bad Credit Can Buy Cars, but They Are Tracked and Have Remote-Kill Switches*, FORBES (Sept. 25, 2014, 2:25 PM), https://www.forbes.com/sites/kashmirhill/2014/09/25/starter-interrupt-devices (on file with the *Iowa Law Review*).

60. *Select GPS Starter Interrupter Device*, PASSTIME GPS (2024), https://passtimegps.com/solutions/select-gps [https://perma.cc/X5XG-FPFT]; *TRAX GPS Device*, PASSTIME GPS (2024), https://passtimegps.com/solutions/trax [https://perma.cc/S7QC-U97Q] ("Every [forty-nine] hours, TRAX automatically provides the current location of the vehicle or asset and a detailed location history of that GPS device.").

61. SPIREON, GOLDSTAR PRODUCT COMPARISON 1–2 (2017), https://www.spireon.com/wp-content/uploads/GS_SalesEnablement_Tables_1217_Web-1.pdf [https://perma.cc/5VNC-D99B].

62. Ryan Kelly, Chris Kukla & Ashwin Vasan, *Rising Car Prices Means More Auto Loan Debt*, CONSUMER FIN. PROT. BUREAU (Feb. 24, 2022), https://www.consumerfinance.gov/about-us/blog/rising-car-prices-means-more-auto-loan-debt [https://perma.cc/7BG3-WWGU].

63. Corkery & Silver-Greenberg, *supra* note 2.

64. *Id.*

65. *See supra* note 15 and accompanying text; *see also* Jim Henry, *High Prices and Risky Credit May Steer Buyers to Older Used Cars; Dealers, Lenders Adjust*, FORBES (Feb. 27, 2023, 3:49 PM), https://www.forbes.com/sites/jimhenry/2023/02/27/high-prices-and-risky-credit-may-steer-buyers-to-older-used-cars-dealers-lenders-adjust (on file with the *Iowa Law Review*) (noting that "dealers and lenders are having to move with the market, to sell and to finance, respectively, older used cars than they are used to" and noting that some providers are extending their "offering[s]

harvesting machines. Although some of the data may remain solely on the vehicle, connected IoT vehicles can document drivers' everyday movements by collecting and surveilling drivers' precise location, including frequently visited locations, unique identifiers for smartphones, call lists, contact information and associated photos stored in smartphones, videos, and drivers' acceleration and brake habits.[66] Connected vehicles can "record locations once every few minutes, even when [drivers] don't use the navigation system."[67] These data can be instantly transmitted back to vehicle manufacturers and potentially other third parties.[68]

The introduction of additional subscription services enabled by VMC features amplify these surveillance and data collection concerns. In addition to already having access to information about drivers and their vehicles due to the connected nature of IoT vehicles, subscription services enabled by VMC features provide another avenue through which companies can surveil and collect more detailed data about drivers. For instance, a heated seat subscription can provide the company with additional financial payment data and detailed information about when and how a driver and passengers use the heated seat options in a vehicle. While a connected vehicle can collect copious quantities of data, individuals who do not have a paid heated seat subscription are unlikely to have this information collected and analyzed in a granular manner since this function requires a subscription payment for activation. To return to an example discussed in the introduction, the proposed Ford patent notes that a vehicle with a buyer in default could record and capture drivers' behaviors and activities during a repossession.[69] While many modern vehicles have cameras, a company's potential ability to control and initiate camera activity due solely to a driver's payment default and to capture a driver's repossession related activities is distinct from other contexts. VMC technology and features enable monitoring and recording of acts of compliance and noncompliance, such as driving outside of a predetermined radius set forth in a loan agreement or not making timely payments for a subscription vehicle service.

Individuals aware of their surveillance could not only become uncomfortable, but they could also change their behaviors based on the

---

to include up to 11-year-old used cars, up from a previous allowable ceiling of 9-year-old vehicles"); Jim Henry, *No Relief from High New Car and Truck Prices; Subprime Loans Hit Hardest*, FORBES (Sept. 9, 2022, 3:37 PM), https://www.forbes.com/sites/jimhenry/2022/09/09/no-relief-from-high-new-car-and-truck-prices-subprime-loans-hit-hardest (on file with the *Iowa Law Review*) ("Today, customers with subprime credit are already just about priced out of the new-vehicle market . . . ." (emphasis omitted)).

66. Fowler, *supra* note 56.

67. *Id.*

68. *See id.* (noting how companies may have "real-time" data collection).

69. Ford Patent Application, *supra* note 33, at 9–11 (discussed at [0041]–[0062]); Sainato, *supra* note 33.

knowledge of surveillance, leading to "inhibitory effects."[70] As Professor Jerry Kang notes, "surveillance leads to self-censorship. This is true even when the observable information would not be otherwise misused or disclosed."[71] While surveillance may not be inherently harmful, it may negatively impact freedom of choice and freedom of movement. Recall the domestic violence victim's story mentioned earlier in which her vehicle was repossessed via VMC technology because the victim moved to a domestic violence shelter and that act violated the geolocation radius limits set forth in her loan documents.

Subprime borrowers may be required to accept surveillance and data collection to qualify for a loan and obtain access to a vehicle. Thus, they may disproportionately bear the brunt of harms associated with surveillance. As Professor Daniel Solove observes, "there can be an even greater chilling effect when people are generally aware of the *possibility* of surveillance, but are never sure if they are being watched at any particular moment."[72] One might contend that VMC technology enables only surveillance of individuals' public activities, such as their location and driving speed. However, even when individuals are aware that their public activities are being surveilled, they could be "less likely to associate with certain groups, attend rallies, or speak at meetings."[73] In summation, VMC technology and features can enable surveillance and data collection.

2. Data Aggregation and Subsequent Uses

Data collected through VMC technology or features can be aggregated,[74] analyzed, and combined with other sources of information to paint a detailed picture of drivers' lives and activities. Drivers may not expect that the data collected to ensure loan or subscription payments will be reanalyzed and used for other purposes.[75]

One VMC technology provider in the vehicle industry touts that its devices and systems can have SID features and utilize "built-in artificial intelligence (AI) technology" to "recognize[] the various data types, group[] them into risk categories and display[] this actionable business intelligence in real-time via the intuitive dashboard."[76] Another company's VMC product, marketed towards buy-here-pay-here dealers, "can also predict where a vehicle

70. Solove, *A Taxonomy of Privacy*, *supra* note 28, at 493 ("Because of its inhibitory effects, surveillance is a tool of social control, enhancing the power of social norms, which work more effectively when people are being observed by others in the community.").

71. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1260 (1998) (footnote omitted).

72. Solove, *A Taxonomy of Privacy*, *supra* note 28, at 495.

73. *Id.* at 499.

74. *Id.* at 507 (defining aggregation as "the gathering together of information about a person").

75. *Id.* at 521 (defining secondary use as "the use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject's consent").

76. *Analytical Dashboard Using AI*, ADVANTAGE AUTO. ANALYTICS (Mar. 19, 2018), https://advantagegps.com/analytical-dashboard-using-ai [https://perma.cc/C3D4-UGUZ].

may be with LocationGenie."[77] VMC technology providers can use data collected by VMC devices to analyze borrowers' behaviors to aid various creditors in detecting "signs of default."[78] Their ability to do so suggests that data collected via VMC technology can be analyzed and mined before default, even if a VMC technology provider has indicated that it takes users' "privacy seriously."[79]

Stand-alone data about a driver's location or speed driving on a single day of the week may not be very telling, but once aggregated and analyzed, the resulting information may "reveal new facts about a person that she did not expect would be known about her when the original, isolated data was collected."[80] Data aggregation and subsequent secondary data uses can lead to dignity harms as they may disrupt or unsettle consumers' expectations with respect to the facts and information that may be deduced and revealed about them.[81] While historically these newly revealed facts or information may not have been consistently accurate, modern technological developments can allow companies to increase the accuracy of this information. It is possible that drivers who voluntarily sign up for subscription services with VMC features, such as remote disablement, would be unwilling to approve secondary uses or participate in subscription services if they were made aware of and understood the implications of secondary VMC data uses, aggregation, and analysis.

Once aggregated and analyzed, the VMC-generated data enables entities deploying the technology to determine if a driver does not consistently drive to their workplace during typical business hours, a development that can help corporations evaluate a borrower's propensity and likelihood of making timely payments.[82] VMC data can be unexpectedly combined with automated license plate reader technology data to provide lenders with detailed location information as well.[83]

Aggregated and analyzed location history can reveal not only employment status but other types of sensitive information as well. One could make detailed and potentially accurate inferences about drivers and their families using these data unless existing applicable laws provide otherwise. Other inferences about a driver's family members, such as children, could be gleaned from location data, including the location of child-care facilities

77. *Connected Vehicle Insights for Buy Here Pay Here Dealers*, SPIREON (2024), https://www.spireon.com/buy-here-pay-here-dealers [https://perma.cc/P4Y5-JUQB].

78. *Id.*

79. Corkery & Silver-Greenberg, *supra* note 2 ("A Spireon spokeswoman said the company takes privacy seriously and works to ensure that it complies with all state regulations.").

80. Solove, *A Taxonomy of Privacy*, *supra* note 28, at 507.

81. *See id.*

82. *Id.*

83. Steve Orr, *License Plate Data Is Big Business*, USA TODAY (Nov. 2, 2014, 5:13 PM), https://www.usatoday.com/story/news/nation/2014/11/02/license-plate-data-is-big-business/18370791 [https://perma.cc/MC3U-HGBQ]; Kaveh Waddell, *How License-Plate Readers Have Helped Police and Lenders Target the Poor*, ATLANTIC (Apr. 22, 2016), https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436 (on file with the *Iowa Law Review*).

used by a driver's children. Moreover, if aggregated and analyzed, the data can reveal a driver's sexual activities and health status,[84] "identifying race, immigration status, weight, health and even genetic information . . . [, and] what music they play."[85]

Companies may also aggregate and analyze driver data that originates from "third-party sources like Google Maps or Sirius XM and sell it to third parties."[86] One study of connected vehicles manufacturers' privacy practices found that eighty-four percent of vehicle manufacturers share or sell users' data with third parties, including data brokers[87] and insurance companies.[88]

Compiled location data can also help deduce drivers' buying and entertainment preferences, including, propensity to accelerate, and propensity to exceed or comply with speed limits. Once aggregated and analyzed, a person's frequently visited locations can reveal visits to medical providers, including access to abortion services, and eating and shopping habits. Notably, in *United States v. Jones*, concurring justices stated that "the use of longer term GPS monitoring . . . impinges on expectations of privacy."[89] In *Carpenter v. United States*, the Supreme Court acknowledged "that individuals have a reasonable expectation of privacy in the whole of their physical movements."[90] Somewhat similarly, in a 2024 case brought by the FTC against a company primarily for selling consumers' geolocation coordinates, the district court observed that such data sales "can reveal a person's political and religious affiliations, sexual orientation, medical conditions, and much more."[91] The court went on to note that the sale of consumer location data in a non-anonymized format could "invade consumers' privacy" and generate "secondary harms" including "stigma, discrimination, physical violence, and

84. Dhruv Mehrotra & Andrew Couts, *Security News This Week: Your New Car Is a Privacy Nightmare*, WIRED (Sept. 9, 2023, 9:00 AM), https://www.wired.com/story/your-new-car-privacy-nightmare (on file with the *Iowa Law Review*).

85. Konrad Fellmann, *How Cars Have Become the Biggest Threat to Privacy*, SC MEDIA (Nov. 2, 2023), https://www.scmagazine.com/perspective/how-cars-have-become-the-biggest-threat-to-privacy [https://perma.cc/E3TM-KCPF].

86. *Id.*

87. Jen Caltrider, Misha Rykov & Zoë MacDonald, *It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy*, MOZILLA: PRIV. NOT INCLUDED (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy [https://perma.cc/V5QU-A84D].

88. Kashmir Hill, *Automakers Are Sharing Consumers' Driving Behavior with Insurance Companies*, N.Y. TIMES (Mar. 13, 2024), https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html (on file with the *Iowa Law Review*); Matt Posky, *Driving Dystopia: Automakers Are Selling Your Driving Data to Insurance Companies*, TRUTHABOUTCARS.COM (Mar. 14, 2014), https://www.thetruthaboutcars.com/cars/news-blog/driving-dystopia-automakers-are-selling-your-driving-data-to-insurance-companies-44505718 [https://perma.cc/2QYC-HF49].

89. United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring).

90. Carpenter v. United States, 585 U.S. 296, 310 (2018).

91. FTC v. Kochava, Inc., No. 22-cv-00377, 2024 WL 449363, at *5 (D. Idaho Feb. 3, 2024) (denying defendant's motion to dismiss).

emotional distress."[92] In short, data collected via VMC technology and features and connected vehicles could potentially be aggregated and subsequently used in various ways. These activities raise significant privacy concerns for consumers.

3. Exclusion and Exacerbating Discrimination

The risk of exclusion involves "the failure to allow the data subject to know about the data that others have about her and participate in its handling and use."[93] A consumer who has purchased an IoT device may have some knowledge of the types of data that the device collects. For instance, a consumer may understand that a smart vacuum must collect and use data about their home's layout to properly function. In contrast, consumers may be unaware of the extent of data collection and surveillance in their own vehicles.[94] This is an important difference. Additionally, if a consumer is unhappy with the privacy features of a household IoT device, the consumer can easily elect not to use the device or return the device, which is often not the case with a vehicle.

A 2020 report by the FTC Bureau of Economics and the FTC Bureau of Consumer Protection ("BCP") detailing the experiences of consumers purchasing vehicles found that most of the respondents did not have knowledge of devices with SID and tracking features and their related paperwork did not indicate the presence of any such devices.[95] The report went on to suggest that, by the time they executed their contracts, many respondents "were mentally fatigued," which may have contributed to consumers' lack of attention to "contract line items," such as "add-ons" and "mandatory fees."[96]

Another staff report by the BCP evaluating consumers' vehicle buying experiences determined that some consumer participants reported that their finance representative reviewed the documents with them "so quickly that they had to ask them to slow down," while others described feeling either that

---

92. *Id.* at *1, *5 ("By selling that data, Kochava arguably invades consumers' privacy and exposes them to significant risks of secondary harms."); Allison Grande, *Kochava Can't Shake FTC's Location Data Privacy Suit*, LAW360 (Feb. 5, 2024, 10:55 PM), https://www.law360.com/articles/1794217 (on file with the *Iowa Law Review*) (noting that the district court found that the allegations in the complaint were sufficient "to support the commission's claims that Kochava's practices substantially harm consumers by depriving them of their privacy and exposing them to significant risks of secondary harms such as stigma, discrimination, physical violence and emotional distress").

93. Solove, *A Taxonomy of Privacy*, *supra* note 28, at 490.

94. Hanvey, *supra* note 29.

95. MARY W. SULLIVAN, MATTHEW T. JONES & CAROLE L. REYNOLDS, FED. TRADE COMM'N, THE AUTO BUYER STUDY: LESSONS FROM IN-DEPTH CONSUMER INTERVIEWS AND RELATED RESEARCH 15 (2020), https://www.ftc.gov/system/files/documents/reports/auto-buyer-study-lessons-depth-consumer-interviews-related-research/autobuyerstudyjointreport.pdf [https://perma.cc/VDP2-M3JL] ("Participants were asked whether they discussed a vehicle tracking device with the dealer, and their paperwork was checked for any indication of one. Tracking devices can include a remote shut-off mechanism to prevent use of the car in the event of missed payments. Most of the participants were not aware of any vehicle tracking device or a remote shut-off mechanism on their vehicle, nor did their paperwork suggest the presence of one.").

96. *Id.* at 17.

the dealer's representative was displeased and irritated because they had taken time to actually review and read the proposed transactional documents, or, alternatively, they felt rushed to review these documents and "forced to move the process along."[97] These reports suggest that there are potential problems with consumers' ability to review and understand important contractual documents during the vehicle buying process, including any potential disclosures regarding the handling and use of the data collected by their vehicles and VMC technology.

A similar exclusion problem is also present in the connected vehicle and subscription services context. Obscure partnerships between vehicle manufacturers and data brokers allow drivers' data collected via connected vehicles and associated subscription services to be monetized and disclosed to third-party companies.[98] These types of data collection and surveillance have occurred without drivers receiving clear and conspicuous notice regarding the collection and potential sharing and sale of their data.[99] Some drivers of connected vehicles have reported being tracked even when they do not enable smart driver features.[100]

At least one VMC provider has offered a companion mobile app that consumers can purchase from vehicle dealers and seemingly bundle it into their loan as an add-on, which, if purchased, potentially allows dealers to cover their GPS expenses.[101] The companion mobile app provides consumers with connected services often available in newer model cars, effectively bringing older vehicles into the IoT, and provides "24/7 vehicle location," "theft recovery," and "[s]mart [a]lerts . . . for [various] driving features, including a geofencing feature."[102] For those consumers who chose to purchase vehicles

97. CAROLE L. REYNOLDS & STEPHANIE E. COX, FED. TRADE COMM'N, BUCKLE UP: NAVIGATING AUTO SALES AND FINANCING 11 (2020), https://www.ftc.gov/system/files/documents/reports/buckle-navigating-auto-sales-financing/bcpstaffreportautofinancing_0.pdf [https://perma.cc/B9MJ-3WSB].

98. Caltrider et al., *supra* note 87; Hill, *supra* note 88; Posky, *supra* note 88.

99. *See* Caltrider et al., *supra* note 87; Hill, *supra* note 88.

100. Hill, *supra* note 88.

101. *Kahu by Spireon Transforms Any Car into a Connected Car*, SPIREON (Dec. 1, 2015), https://www.spireon.com/2015/12/01/kahu-by-spireon-transforms-any-car-into-a-connected-car [https://perma.cc/H7VT-XA3Z]; *see also* Auto Remarketing Staff, *Spireon Launches Connected Car Add-On for Dealers*, AUTO REMARKETING (Jan. 30, 2017, 5:00 PM), https://www.autoremarketing.com/ar/spireon-launches-connected-car-add-dealers [https://perma.cc/BVC4-URN5] (providing more information about the connected service); KAHU BY SPIREON, MAKE EVERY CAR MORE PROFITABLE: A SMARTER ADD-ON 3 (2017), https://www.spireon.com/wp-content/uploads/Kahu-Prospectus_02-20-17.compressed.pdf [https://perma.cc/87N7-SGHG] (same); David S. Wallens, *Does Your Car Contain a GPS Tracker Without Your Knowledge?*, GRASSROOTS MOTORSPORTS (Dec. 11, 2019), https://grassrootsmotorsports.com/news/Does-Your-Car-Contain-a-GPS-Tracker-Without-Your-Knowledge [https://perma.cc/APY3-49KV] (discussing privacy implications). For a product that appeals to the subprime market, see *Meet the New Goldstar*, SPIREON (May 25, 2017), https://www.spireon.com/meet-new-goldstar [https://perma.cc/9DMG-JD5J].

102. *Kahu by Spireon Transforms Any Car into a Connected Car*, *supra* note 101 (advertising a connected service). Spireon's Goldstar also offers these features. *Meet the New Goldstar*, *supra* note 101; *see also Connected Vehicle Insights for Buy Here Pay Here Dealers*, *supra* note 77 (advertising a

with the associated dealer installed device and the companion mobile app, it is not entirely clear which parties, other than the consumer and the company, have access to collected data. It also not clear whether these data can be aggregated, anonymized, and subsequently monetized or used to allow lenders to better enforce their rights in lending transactions. Anonymized and aggregated data could be de-anonymized and subsequently used to identify borrowers.[103]

Concerns of discrimination also exist, particularly with respect to add-ons, such as the VMC add-on mentioned earlier. A study from the Center for Responsible Lending on vehicle dealers' practices determined that African-American and Latino consumers were "nearly twice as likely to be sold multiple add-on products" that could increase loan costs.[104] This increase in loan costs could contribute to higher rates of delinquency. VMC add-ons may worsen existing discriminatory problems in the automobile industry since such add-ons may present additional opportunities for surveillance and discriminatory pricing and other kinds of discrimination as is the case with other types of add-ons; to this point, it is unsurprising that automobile dealerships' salespersons may also receive additional compensation or bonuses for signing consumers up for vehicle subscription services[105] and potentially

connected service); Louis Ellis, *No Subscription Vehicle Tracker: Best One-Time Purchase Options*, MOTO WATCHDOG (Apr. 6, 2024), https://www.motowatchdog.com/blog/no-subscription-vehicle-tracker-best-one-time-purchase-options-updated [https://perma.cc/F4XV-QUUQ] (comparing various connected services).

103. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1717–22 (2010) (discussing three different anonymized datasets that were "[u]ndone"); Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye, *Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models*, NATURE COMMC'NS 1, 2 (July 23, 2019), https://www.nature.com/articles/s41467-019-10933-3 [https://perma.cc/C99D-EAWQ] ("Our results reject the claims that, first, re-identification is not a practical risk and, second, sampling or releasing partial datasets provide plausible deniability."); Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703, 704 (2016) ("For years, it was widely believed that as long as data sets were 'anonymized,' they posed no risk to anyone's privacy. If data sets were anonymized, then they did not reveal the identity of individuals connected to the data. Unfortunately, the notion of perfect anonymization has been exposed as a myth. Over the past twenty years, researchers have shown that individuals can be identified in many different data sets once thought to have been 'anonymized.'"); Latanya Sweeney, *Simple Demographics Often Identify People Uniquely* 2–5 (Carnegie Mellon Univ., Working Paper No. 3, 2000) (reviewing this data).

104. DELVIN DAVIS, CTR. FOR RESPONSIBLE LENDING, NON-NEGOTIABLE: NEGOTIATION DOESN'T HELP AFRICAN AMERICANS AND LATINOS ON DEALER-FINANCED CAR LOANS 2–3 (2014), https://www.responsiblelending.org/sites/default/files/nodes/files/research-publication/CRL-Auto-Non-Neg-Report.pdf [https://perma.cc/3ZJ3-5GUP].

105. *See, e.g.*, Chris Capurso, Brooke Conkle, Lori Sommerfield, Chris Willis & Alan D. Wingfield, *FTC and Wisconsin DOJ Settle with Auto Group over Alleged Illegal Add-Ons and Discrimination Against American Indian Consumers*, TROUTMAN PEPPER (Oct. 26, 2023), https://www.consumerfinancialserviceslawmonitor.com/2023/10/ftc-and-wisconsin-doj-settle-with-auto-group-over-alleged-illegal-add-ons-and-discrimination-against-american-indian-consumers [https://perma.cc/ZH3D-FDKQ] ("In total, American Indians paid on average approximately $1,362 more for add-ons than non-Latino White customers since 2016."); Hill, *supra* note 88 (noting that "salespeople can receive bonuses for successful enrollment of customers in OnStar services, including Smart Driver, according to a company manual").

add-ons as well. The add-on problem is also compounded by discretionary dealer interest rate markups that can facilitate discrimination in violation of existing laws.[106]

Congress dismantled the CFPB's prior guidance on dealer markups.[107] The FTC has pursued companies for discriminatory practices associated with dealer markups[108] and regional Federal Reserve Banks and the National Credit Union Administration have issued their own recommendations.[109] However, at least one FTC Commissioner has urged the FTC to initiate "a rulemaking, under the Dodd-Frank Act, to regulate dealer markup[s]."[110]

---

106. CONSUMER FIN. PROT. BUREAU, CONSUMER FINANCIAL PROTECTION BUREAU TO HOLD AUTO LENDERS ACCOUNTABLE FOR ILLEGAL, DISCRIMINATORY MARKUP 1 (2013), https://files.consumerfinance.gov/f/201303_cfpb_march_-Auto-Finance-Factsheet.pdf [https://perma.cc/GA6T-FYBV] ("Often, indirect auto lenders allow the dealer to charge the consumer an interest rate that is costlier for the consumer than the rate the lender gave the dealer. This increase in rate is typically called 'dealer markup.' The lender shares part of the revenue from that increased interest rate with the dealer."). Research also indicates that "markup practices may lead to African Americans and Hispanics being charged higher markups than other, similarly situated, white consumers." *Id.*

107. S.J. Res. 57, 115th Cong. (2018) (enacted); *Bulletin Re: Indirect Auto Lending and Compliance with the Equal Credit Opportunity Act*, CONSUMER FIN. PROT. BUREAU (Mar. 21, 2013), https://www.consumerfinance.gov/compliance/supervisory-guidance/bulletin-indirect-auto-lending-compliance [https://perma.cc/6J4B-TSNS] ("On May 21, 2018, the President signed a joint resolution passed by Congress disapproving the Bulletin titled 'Indirect Auto Lending and Compliance with the Equal Credit Opportunity Act' (Bulletin), which had provided guidance about the Equal Credit Opportunity Act (ECOA) and its implementing regulation, Regulation B. Consistent with the joint resolution, the Bulletin has no force or effect. The ECOA and Regulation B are unchanged and remain in force and effect."); Kris. D. Kully, Christa L. Bieker & Elyse S. Moyer, *Congress Invalidates CFPB's Indirect Auto Lending Guidance*, MAYER BROWN (May 8, 2018), https://www.cfsreview.com/2018/05/congress-invalidates-cfpbs-indirect-auto-lending-guidance [https://perma.cc/ALE5-GV46]; *see also* Press Release, Rebecca Kelly Slaughter, Comm'r, Fed. Trade Comm'n, Statement of Commissioner Rebecca Kelly Slaughter in the Matter of Liberty Chevrolet, Inc. d/b/a Bronx Honda 1, 4 (May 27, 2020) [hereinafter Statement of Commissioner Slaughter], https://www.ftc.gov/system/files/documents/public_statements/1576006/bronx_honda_2020-5-27_bx_honda_rks_concurrence_for_publication.pdf [https://perma.cc/L93B-NV3M] ("First and foremost, the Commission can start by initiating a rulemaking, under the Dodd-Frank Act, to regulate dealer markup. . . . Despite the obvious flaw of the Dodd-Frank Act's exemption from the jurisdiction of the CFPB for auto dealers, the Act had a saving grace: The Federal Trade Commission is empowered to write rules, under the Administrative Procedure Act, to regulate auto dealers. *See* 12 U.S.C. § 5519(d).").

108. *See, e.g.*, Stipulated Order for Permanent Injunction, Monetary Judgment, and Other Relief at 13, FTC v. N. Am. Auto. Servs., Inc., No. 22-cv-01690 (N.D. Ill. Mar. 31, 2022) (resolving a lawsuit against North American Automotive Services, among others).

109. Adam J. Levitin, *The Fast and the Usurious: Putting the Brakes on Auto Lending Abuses*, 108 GEO. L.J. 1257, 1298–99 (2020); *see also* CONSUMER FIN. PROT. BUREAU, CFPB BULL. 2013-02, INDIRECT AUTO LENDING AND COMPLIANCE WITH THE EQUAL CREDIT OPPORTUNITY ACT 4 (2013) (discussing ongoing review processes); Statement of Commissioner Slaughter, *supra* note 107, at 4 (same).

110. Statement of Commissioner Slaughter, *supra* note 107, at 1; *see also* Press Release, Rohit Chopra, Comm'r, Fed. Trade Comm'n, Statement of Commissioner Rohit Chopra in the Matter of Liberty Chevrolet, Inc. d/b/a Bronx Honda 1 (May 27, 2020), https://www.ftc.gov/system/files/documents/public_statements/1576002/bronx_honda_final_rchopra_bronx_honda_statement.pdf [https://perma.cc/JPN5-SKSE] (discussing dealer markups and arguing that "[a] decade ago, [in 2010,] Congress gave the FTC additional tools in the auto market. Given growing concerns and abuses, we should use this authority").

One study of the CFPB's enforcement actions on dealer markups found that the agency's efforts "led to a [sixty percent] decrease in the additional interest that minorities pay on auto loans."[111] A CFPB report on subprime auto lending suggests that subprime lending borrowers who obtain financing from dealers who charge higher interests rates are more likely to be delinquent on their loans.[112] Subprime borrowers from historically marginalized groups who may already have a higher chance of experiencing discrimination in the lending process may also have to contend with the possible privacy harms raised by creditors' use of VMC technology.

Unless clearly prohibited by existing law, it is possible that data obtained from connected vehicles and VMC technology could be used to negatively impact and influence the future opportunities borrowers receive in unrelated transactions, which may include unexpected subsequent uses of VMC and connected vehicle data. A 2024 report by the Electronic Privacy Information Center ("EPIC") notes that "the massive collection of data in the hands of data brokers means that consumers are sorted and scored in discriminatory ways" including discriminatory pricing.[113] Recall that connected vehicle data and VMC data can be sold to third-party companies, including data brokers, to discriminatorily advertise to drivers based on where they "live, work or frequently travel."[114]

B. ELECTRONIC SUBJUGATION RISKS

VMC technology and subscription services supported by VMC features allow corporate actors to extend their electronic dominance over drivers' activities and vehicles post-transaction. Prior to the advent of VMC technology and the IoT, lenders seeking to repossess a vehicle had less knowledge of and ability to observe and collect information about drivers' behaviors and whereabouts. Lenders, dealers, and vehicle manufacturers now have the ability to obtain real-time data about vehicle performance and drivers' activities.[115] Recall that connected vehicles can collect and disclose data about how hard drivers brake and turn and how frequently they drive late at night, among other things.[116] Also, recall that these vehicles can also be connected directly to third-party apps that can enable further data collection by third-party entities.[117]

---

111. Alexander W. Butler, Erik J. Mayer & James P. Weston, *Racial Disparities in the Auto Loan Market*, 36 REV. FIN. STUD. 1, 39 (2023).

112. *See generally* JASPER CLARKBERG, JACK GARDNER & DAVID LOW, CONSUMER FIN. PROT. BUREAU, DATA POINT 2021-10, DATA POINT: SUBPRIME AUTO LOAN OUTCOMES BY LENDER TYPE (2021) (detailing differences in auto loans among different lenders).

113. CAITRIONA FITZGERALD, KARA WILLIAMS & R.J. CROSS, ELEC. PRIV. INFO. CTR., THE STATE OF PRIVACY: HOW STATE "PRIVACY" LAWS FAIL TO PROTECT PRIVACY AND WHAT THEY CAN DO BETTER 10 (2024), https://epic.org/wp-content/uploads/2024/01/EPIC-USPIRG-State-of-Privacy.pdf [https://perma.cc/WR5D-3KLU].

114. Hanvey, *supra* note 29.

115. Fowler, *supra* note 56.

116. *Id.*

117. *Id.*

Subprime borrowers are particularly at risk for electronic subjugation because they must consent to the installation of VMC technology in their vehicles to obtain financing. Some providers of VMC technology contend that they protect borrowers' privacy and design their devices to only collect location data once the subprime borrower is in default.[118] However, VMC technology advertised by some providers can provide and obtain a vehicle's location "on demand" and generate detailed location history that exposes "where the vehicle was and more importantly, where it's going to be."[119] One model SID disclosure form notes that the lender may use the GPS functionality of an SID device to "periodically" check the location of the automobile "to verify that it has not been permanently moved to another location without [the lender's] knowledge, and to confirm that the [d]evice continues to operate as intended, has not been tampered with, and has not be[en] disengaged [or] removed from the [v]ehicle."[120]

Once VMC technology, such as a SID, is installed in a vehicle, a creditor can remotely and easily disable the vehicle.[121] Remote disablement typically happens after a buyer has defaulted on a loan payment.[122] However, as I have highlighted in other sections of this Article, remote disablement can still occur even after a driver has paid off the loan balance in its entirety and even if a buyer has made timely payments. Historically, to disable a vehicle and then subsequently repossess it, a lender had to do so in person via its agents. Through VMC technology, a lender can digitally restrain a driver's daily activities with a simple click of a button. The *New York Times* reported that a lender's representative stated that "he could monitor a vehicle's whereabouts on his smartphone" and used SID technology connected to his smartphone to disable an individual's car while shopping in Walmart.[123]

Drivers bear the risks of lender inaccuracies, errors, and payment disputes. For instance, prior to the widespread use of VMC technology, if a lender misplaced a driver's monthly payment, the lender could not quickly disable the vehicle's operations or immediately force the driver to make a payment to continue driving the vehicle. Additionally, lenders may also remotely disable drivers' vehicles for reasons unrelated to a default under the contract. For

118. Corkery & Silver-Greenberg, *supra* note 2. The Payment Assurance Technology Association previously established standards for the use of GPS tracking devices and SID devices in consumer transactions. PAYMENT ASSURANCE TECH. ASS'N, STANDARDS FOR MANUFACTURE AND UTILIZATION OF DEVICES FOR STARTER INTERRUPT/GPS TRACKING IN CONSUMER FINANCIAL TRANSACTIONS 2 (2012), http://www.patassociation.com/pdfs/Standards.pdf [https://perma.cc/2UHU-CCR7].

119. Hill, *supra* note 59.

120. NATIONWIDE CAC LLC, LOANPLUS GPS AND STARTER INTERRUPT SYSTEM DISCLOSURE AND AGREEMENT FOR INSTALLATION 2 (2016), https://www.nac-loans.com/sites/default/files/pdf/NATIONWIDE%20CAC/Funding%20Forms/WEB%20CAC%20GPS%20SID%201-16.pdf [https://perma.cc/JN3G-JCTF].

121. *See* Moringiello, *supra* note 14, at 584.

122. *Id.* at 565–71.

123. Michael Corkery & Jessica Silver-Greenberg, *Federal Agency Begins Inquiry into Auto Lenders' Use of GPS Tracking*, N.Y. TIMES (Feb. 19, 2017), https://www.nytimes.com/2017/02/19/business/dealbook/gps-devices-car-loans.html (on file with the *Iowa Law Review*); Corkery & Silver-Greenberg, *supra* note 2.

instance, in *Hanes v. Darar*, the lender repeatedly rejected the driver's monthly payment and subsequently disabled the driver's vehicle using VMC technology because the driver had a verbal disagreement with the lender's wife.[124]

Drivers have reported suffering significant daily interruptions because of remote disablement. Some drivers have reported that they could not drive their children to educational institutions or attend doctors' appointments after lenders remotely disabled their vehicles and failed to provide pre-disablement notifications.[125] In a bankruptcy case involving VMC technology, *In re Horace*, the driver alleged that the VMC device disabled the vehicle on several occasions, including when she was at a medical appointment after surgery.[126] Some lenders may allow drivers to operate their vehicles after remote disablement in the case of emergencies. However, unless existing law requires otherwise, it is the lender who determines what constitutes an emergency and whether to grant the emergency request.

Geofencing features associated with VMC technology may also raise electronic subjugation risks. Geofencing allows lenders and dealers to wield significant control over drivers post-transaction. Such features enable lenders to disable a car once it exits a predetermined area established by the lender. Once a lender receives an alert of the violation, the lender can remotely disable the vehicle to limit the driver's mobility.

Another example of electronic subjugation risks is warning sounds. VMC technology can also enable a lender or dealer to send borrowers multiple audible-payment reminders.[127] The audible payment reminder sounds in the vehicle can increase in volume and frequency immediately before payments are due and potentially after default. These audible tones may work in conjunction with emails and telephone texts and calls regarding payment due dates.

One might contend that VMC warning sounds are less problematic than remote disablement and geofencing. However, it is notable that the CFPB has pursued at least one auto lender for causing SIDs "to play warning tones in vehicles over 71,000 times during periods when the consumer was not in default or was in communication with [the lender] about upcoming payments."[128] These warning sounds were emitted "for four days for many consumers, and they lasted more than four days in hundreds of instances."[129] Individuals who incorrectly received warning sounds were bewildered, troubled,

124. Hanes v. Darar, No. COA11-627, 2012 WL 707110, at *1 (N.C. Ct. App. Mar. 6, 2012).

125. Corkery & Silver-Greenberg, *supra* note 2.

126. *In re* Horace, No. 14-30103, 2015 WL 5145576, at *2–3 (Bankr. N.D. Ohio Aug. 28, 2015).

127. Corkery & Silver-Greenberg, *supra* note 2.

128. Press Release, Consumer Fin. Protection Bur., CFPB Sues USASF Servicing for Illegally Disabling Vehicles and for Improper Double-Billing Practices (Aug. 2, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-sues-usasf-servicing-for-illegally-disabling-vehicles-and-for-improper-double-billing-practices [https://perma.cc/BT6C-J5WG].

129. Complaint ¶ 18, CFPB v. USASF Servicing, LLC, No. 23-cv-03433 (N.D. Ga. Aug. 2, 2023).

and had to spend time communicating with the lender to resolve the dispute.[130] Additionally, the lender wrongfully remotely disabled consumers vehicles "at least 5,200" times when consumer debtors were not in default or had previously made promises to make payments.[131] These consumers could not control whether the lender wrongfully activated the device to issue warning sounds or wrongfully disabled their vehicles. Further, even consumer debtors who made arrangements with the lender to resolve erroneously emitted warning sounds and remote disablement could not control whether the lender "fail[ed] to update [its] accounts and relay appropriate system notifications."[132]

Unlike some borrowers with poor credit who may have to accept VMC technology as part of the lending process, non-subprime borrowers can choose whether to use vehicular subscription services associated with VMC features. Thus, one might argue that there is less of a concern about electronic subjugation given the voluntary nature of subscription services in the non-subprime context. For instance, individuals can choose not to purchase subscriptions for heated seats and can, therefore, avoid remote disablement of those features for nonpayment. However, recall the Ford patent application discussed earlier, which, if approved and implemented in future vehicles, would install VMC-like technology in future Ford vehicles. To the extent that more automobile manufacturers adopt similar design features with built-in remote disablement features for lack of payment, consumers who purchase or lease newer vehicles may have less of a choice and face similar electronic subjugation risks.

VMC technology in newer connected vehicles could permit a sequence of escalating sanctions for drivers who fail to make timely payment.[133] For instance, a driver who has failed to make timely payments could find that the lender or vehicle manufacturer slowly increases the punishment for nonpayment by first initiating a "loss of window control" and then disabling air conditioning functions, all before initiating full vehicle disablement.[134]

Additionally, recall the example of Mercedes's optimal acceleration subscription service mentioned earlier. Increasingly consumers must accept subscription services and the associated remote disablement of features to access the full functionality and capabilities of the factory-ready hardware of their connected vehicles that they may have already paid for in the overall price. For these drivers, electronic subjugation potentially occurs through a series of microtransactions after the point of sale. A driver must make additional payments to maintain access to the full functionality of their vehicles in addition to any vehicle lease or loan payments. Additionally, even drivers who have paid off their vehicle loans and have obtained clear title to their vehicles may need to continue making monthly payments to the vehicle manufacturer to continue using vehicle functions connected to a subscription. These realities arguably demonstrate the growing level of power

130. *Id.* ¶ 19.
131. *Id.* ¶ 16.
132. *Id.* ¶ 20.
133. Markey Letter, *supra* note 30, at 3.
134. *Id.*

and control that automobile manufacturers have over consumers' ability to use and reap the benefits of their vehicles post transaction. It also calls into question the validity of criticisms associated with the seemingly voluntary nature of subscription services enabled by VMC features in the non-subprime vehicle context.

Also, consider that if vehicle safety features operate on a subscription basis, insurance companies, unless restricted by law, could elect not to insure drivers who fail to obtain subscriptions for those options, particularly if those features have been proven to decrease automobile accidents.[135] Rather than potentially declining coverage, it is also possible that insurance companies could use VMC data to increase the premiums of drivers who choose not to pay for vehicle subscription safety features. Indeed, driver data from vehicle subscription services, including roadside assistance, remote unlocking, and navigation, combined with optional smart driver rating features and services, have already served as a treasure trove of information for insurance companies.[136] Insurance businesses may obtain driver consent to use this data to determine rates via boilerplate provisions agreed to by drivers.[137] Insurance companies have already used driver behavioral data sold by vehicle manufacturers to increase consumers insurance rates, and in some cases, deny coverage.[138] Examples of driver behavioral data that insurance companies have obtained access to include: the number of trips taken, "start and end times [for trips taken], the distance driven and an accounting of any speeding, hard breaking or sharp accelerations."[139]

Another potential risk in the subscription vehicle context, particularly for drivers with automatic renewals, is that they may forget that they have subscribed to specific vehicle services. Although state and federal law regulates this practice, the nature of subscription services may allow vehicle manufacturers to charge drivers' credits cards until a driver carefully reviews their billing statements.[140] Lastly, on the issue of voluntariness and electronic

135. Jasper Jolly, *Will 'Connected Cars' Persuade Drivers to Pay for a High-Spec Ride?*, GUARDIAN (July 30, 2022, 11:00 AM), https://www.theguardian.com/business/2022/jul/30/will-connected-cars-persuade-drivers-to-pay-for-a-high-spec-ride [https://perma.cc/E6D8-6HQR].

136. Hill, *supra* note 88 ("Modern cars are internet-enabled, allowing access to services like navigation, roadside assistance and car apps that drivers can connect to their vehicles to locate them or unlock them remotely. In recent years, automakers, including G.M., Honda, Kia and Hyundai, have started offering optional features in their connected-car apps that rate people's driving. Some drivers may not realize that, if they turn on these features, the car companies then give information about how they drive to data brokers like LexisNexis.").

137. *Id.*; *see also* Louis DeNicola, *Which States Restrict the Use of Credit Scores in Determining Insurance Rates?*, EXPERIAN (Jan. 12, 2024), https://www.experian.com/blogs/ask-experian/which-states-prohibit-or-restrict-the-use-of-credit-based-insurance-scores [https://perma.cc/54SC-TR7J] (discussing differences between states).

138. Hill, *supra* note 88.

139. *Id.*

140. Michael P. Daly, Matthew Adler & Meaghan V. Geatens, *FTC Proposes Sweeping, Nationwide Regulations for Automatic Renewals*, AM. BAR ASS'N (Aug. 17, 2023), https://www.americanbar.org/groups/litigation/resources/newsletters/consumer/ftc-nationwide-regulations-automatic-renew

subjugation in the non-subprime context, one study of connected vehicle manufacturer's privacy practices found that ninety-two percent of these companies gave "drivers little to no control over their personal data."[141] Our modern lifestyles often require driving to ensure full participation in society. Thus, unlike with other IoT devices that are not necessities, individuals do not have the same ability to opt out of not driving a vehicle and any related data collection and surveillance.[142]

C. CYBERSECURITY RISKS

Connected vehicles, like other IoT devices, face significant cybersecurity risks. According to one report on this topic "data breaches are on the rise and account for [thirty-seven percent] of [cybersecurity automotive] incidents."[143] In 2023, Toyota reported that, "for more than [ten] years, a misconfigured cloud bucket left more 2.15 million customer records [from connected services] exposed to the open Internet."[144] The leaked data included vehicle location information and "video recordings taken outside [the vehicle]."[145]

Design flaws may also render vehicles susceptible to remote hacking, which may allow a hacker to remotely control a vehicle, including starting and stopping a vehicle's ignition.[146] Consumers have unsuccessfully initiated lawsuits against Fiat–Chrysler and others for selling vehicles with those flaws.[147] Similar vulnerabilities have appeared in connected vehicles manufactured by other car companies.[148] Through Bluetooth and mobile apps, hackers have allegedly controlled Tesla vehicles, unlocked vehicle doors, "honk[ed] the horn and start[ed] the engine."[149] Use of VMC technology could present similar risks.

---

als/?login [https://perma.cc/PK2R-HCQF] (discussing state and federal frameworks regulating automatic renewals); Marshall, *supra* note 3.

141. Caltrider et al., *supra* note 87.

142. *Id.*

143. UPSTREAM SEC. LTD., H1'2023 AUTOMOTIVE CYBER TREND REPORT 3 (2023), https://info.upstream.auto/hubfs/Security_Report/H1-2023_Report/Upstream_H1-2023_Automotive_Cyber_Trend_Report.pdf [https://perma.cc/3RM8-NTZX].

144. Dark Reading Staff, *Toyota Discloses Decade-Long Data Leak Exposing 2.15M Customers' Data*, DARK READING (May 15, 2023), https://www.darkreading.com/cloud-security/toyota-discloses-decade-long-data-leak-exposing-2-15m-customers-data [https://perma.cc/4NSK-ZHEJ]; *see also* Zack Whittaker, *Toyota Confirms Another Years-Long Data Leak, This Time Exposing At Least 260,000 Car Owners*, TECHCRUNCH (May 31, 2023, 8:05 AM), https://techcrunch.com/2023/05/31/toyota-customer-data-leak-years [https://perma.cc/2CYQ-YG8F] (describing another breach).

145. Anthony Spadafora, *Toyota Exposed Car Location Data of 2 Million Drivers for 10 Years — What You Need to Know*, YAHOO (May 12, 2023), https://finance.yahoo.com/news/toyota-exposed-car-location-data-171809438.html [https://perma.cc/BZR4-4PY8].

146. Ionut Arghire, *16 Car Makers and Their Vehicles Hacked Via Telematics, APIs, Infrastructure*, SEC. WK. (Jan. 5, 2023), https://www.securityweek.com/16-car-makers-and-their-vehicles-hacked-telematics-apis-infrastructure [https://perma.cc/24C8-WDBQ].

147. *See, e.g.*, Flynn v. FCA US LLC, 39 F.4th 946, 949, 954 (7th Cir. 2022) (affirming an order dismissing plaintiffs' case against Fiat–Chrysler for data vulnerabilities).

148. Arghire, *supra* note 146.

149. Mirjam Guesgen, *Why Connected Cars Are the Next Frontier in Cybersecurity*, FIN. POST (June 14, 2023), https://financialpost.com/cybersecurity/why-connected-cars-next-frontier-cybersecurity [https://perma.cc/Y8HQ-2QJJ].

Hacking VMC technology and related systems could potentially allow a third party to utilize geofence, SID, and GPS features and obtain information about a vehicle's exact location as well as potentially access other types of vehicle data.[150] Consider that some consumers who used third-party remote-start mobile apps and ignition devices which connect to a vehicle's dashboard have discovered vulnerabilities in the devices that would allow "any hacker [with an internet connection] to fully hijack th[e] remote unlock and ignition device[,] . . . 'locate cars, identify them, unlock them, start the car[s], trigger the alarm . . . [or do] anything a legitimate user could do.'"[151] These vulnerabilities also led to the exposure of consumers' vehicular data and can allow a hacker to access a vehicle's camera.[152] Similarly, data collected through VMC technology by automobile dealers and lenders could possibly be at risk if stored improperly or if associated devices are poorly designed.

Cyberattacks on automobile dealerships which often store consumer data as well as third-party companies providing dealership services may also leave consumers and their data vulnerable.[153] In 2024, a ransomware cyberattack on a leading provider of automobile dealership management services and software disrupted the functions of 15,000 automobile dealerships across the United States for several days.[154] The company provides "vehicle acquisitions,

150. *See* John Mac Ghlionn, *Your Car Is Spying on You—and Making Personal Info Vulnerable to Hackers*, N.Y. POST (July 3, 2023, 6:25 PM), https://nypost.com/2023/07/03/your-car-might-be-making-personal-info-vulnerable-to-hackers [https://perma.cc/Z8GC-E2N7] ("[Cybersecurity a]ttacks . . . will be both from hackers who will be attracted by the increasing amount and value of data that companies in the broad auto ecosystem collect and from regular bad people who will leverage these technologies to stalk, harass, defraud, steal and harm people.").

151. Andy Greenberg, *A Remote-Start App Exposed Thousands of Cars to Hackers*, WIRED (Aug. 10, 2019, 2:50 PM), https://www.wired.com/story/mycar-remote-start-vulnerabilities (on file with the *Iowa Law Review*).

152. *Id.* ("[H]e estimates that there were roughly 60,000 cars left open to theft by those security bugs, with enough exposed data for a hacker to even choose the make and model of the car they wanted to steal."); Justin Banner, *How Phone-As-Key, Remote Start Apps Can Make Your Car Easier to Steal*, MOTORTREND (Apr. 20, 2023), https://www.motortrend.com/news/phone-as-key-remote-start-apps-car-theft-hackers (on file with the *Iowa Law Review*) ("Once [vulnerabilities have been] found, . . . hackers [can] have direct access to a user's data for both them and their vehicle. Just by having that surface level access, vehicles could be tracked and even be susceptible to remote access to unlock doors, start the engine, or even peep the 360-view camera in real time.").

153. Bailey Schulz, *CDK Global Shuts Down Car Dealership Software After Cyberattack*, USA TODAY (June 22, 2024, 5:05 PM), https://www.usatoday.com/story/money/cars/2024/06/19/cdk-cyber-attack-hits-automotive-dealers/74150427007 [https://perma.cc/MXW4-RVWE] ("Dealerships have been an attractive target because of the vast amounts of sensitive customer data they hold."); Sean Hemmersmeier, *Cybersecurity Attack Impacts Sales, Service at Nevada Automotive Group*, L.V. REV.-J. (June 10, 2024, 5:47 PM), https://www.reviewjournal.com/business/cybersecurity-attack-impacts-sales-service-at-nevada-automotive-group-3066257 [https://perma.cc/EQZ7-AQEL] (discussing a cyberattack on an automotive group that disrupted services and operations).

154. Megan Cerullo, *CDK Cyberattack Shuts Down Auto Dealerships Across the U.S. Here's What to Know*, CBS NEWS (June 21, 2024, 5:15 PM), https://www.cbsnews.com/news/cdk-cyber-attack-outage-auto-dealerships-cbs-news-explains [https://perma.cc/Q8TE-CKJL]; Craig Trudell, *CDK Hackers Want Millions in Ransom to End Car Dealership Outage*, BLOOMBERG (June 21, 2024, 5:16 PM), https://www.bloomberg.com/news/articles/2024-06-21/cdk-hackers-want-millions-in-ransom-to-end-car-dealership-outage (on file with the *Iowa Law Review*).

sales, financing, insuring, repairs and maintenance" services to automobile dealerships and these services were negatively impacted during the attack.[155]

Even if not disclosed to third parties or hackers, connected vehicle data could be shared and disclosed within a company in ways that a driver may not expect. Tesla employees have reportedly shared amongst themselves, via the company's internal video messaging system, sensitive videos, and images of drivers captured by Tesla vehicle cameras.[156] Associated computer programs allowed employees to determine the location of the video recordings that could reveal Tesla drivers' addresses, despite claims in Tesla's privacy policy that "camera recordings remain anonymous and are not linked" to drivers or their vehicles.[157] In summary, VMC technology and connected vehicles could potentially generate various cybersecurity and data disclosure risks.

II. STATE AND FEDERAL LEGAL FRAMEWORKS

Various sources of state and federal law regulate transactions involving consumer vehicles. This Section evaluates some (but not all) potentially applicable sources of state and federal law on this topic. Article 9 of the UCC provides important rules governing secured lending transactions, including financing transactions involving consumers' vehicles. However, Article 9's lack of clarity on the issue of whether a remote disablement via VMC technology qualifies as a repossession under Article 9 leaves significant room for the practice of remote disablement to continue without the imposition of breach of the peace limitations.

Several states have adopted laws that directly address the use of VMC technology in transactions involving consumer vehicles. While some laws provide more protections for consumers than others, these laws generally authorize the use of VMC technology. Several laws rely significantly on a notice-and-choice model. Some laws only provide consumer protections for certain types of VMC technology and exclude others. Consumers in states that have not directly addressed the VMC technology issue may have even less protections than consumers in states that have adopted laws to address the issue.

Additionally, this Section analyzes five of the recent slate of state privacy statutes, such as the CCPA. These statutes can impose limits on the use of data collected in both subprime and non-subprime transactions. However, the CCPA, like several other state statutes, relies significantly on an individual rights-based approach to privacy and, to some extent, also relies heavily on

155. Schulz, *supra* note 153.

156. Jon Brodkin, *Tesla Workers Shared Images from Car Cameras, Including "Scenes of Intimacy,"* ARS TECHNICA (Apr. 6, 2023, 12:34 PM), https://arstechnica.com/tech-policy/2023/04/tesla-workers-shared-images-from-car-cameras-including-scenes-of-intimacy [https://perma.cc/3E3Q-UVQ8]; Steve Stecklow, Waylon Cunningham & Hyunjoo Jin, *Tesla Workers Shared Sensitive Images Recorded by Customer Cars*, REUTERS (Apr. 6, 2023, 4:47 PM), https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06 [https://perma.cc/8L9Y-T48Y].

157. Stecklow et al., *supra* note 156.

the notice-and-choice model. Notice implies that companies provide consumers with a document, such as a privacy policy or perhaps terms and conditions containing privacy-related provisions, which describes companies' data collection, use, disclosure, and transfer practices. Choice implies that consumers have the ability to accept or expressly consent to these practices or walk away from the transaction.

A rights-based approach in which consumers get privacy rights can be an important part of a privacy law regime, although it also has several shortcomings. First, this approach places a significant burden on drivers and other consumers to exercise these rights to protect their privacy interests. Given the frequency with which consumers must consent to privacy practices, it is particularly difficult for individuals to understand the privacy implications and risks associated with consent. As Professor Daniel Solove observes, privacy "rights can't practically be exercised at scale with the number of organizations tha[t] process people's data."[158]

With respect to federal frameworks, consumers may face significant difficulties in attempting to prove discrimination under applicable federal law.[159] The FTC's CARS Rule represents an important step towards curtailing abuse in vehicle transactions.[160] Although the CARS Rule contains restrictions on misrepresentations by car dealers in connection with repossessions, the rule does not adequately address the use of VMC technology, or the concerns highlighted in this Article. The CARS Rule is also the subject of an ongoing legal challenge that may negatively impact its validity.[161]

A. THE UNIFORM COMMERCIAL CODE

Turning now to an important source of state law, a state's version of Article 9 of the UCC can also apply to consumer financing transactions. However, as state law, Article 9 may be preempted by certain federal laws. Article 9's provisions must also defer to both state and federal consumer protection laws.[162] Article 9 generally governs transactions that "create[] a security interest in personal property."[163] A security interest can be described as a lien on personal property. There are several types of personal property that can be subject to Article 9, including goods, general intangibles, and

158. Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975, 975 (2023).

159. Nicole K. McConlogue, *Discrimination on Wheels: How Big Data Uses License Plate Surveillance to Put the Brakes on Disadvantaged Drivers*, 18 STAN. J.C.R. & C.L. 279, 318–19 (2022); 15 U.S.C. § 1691 (2018) (prohibiting discrimination in lending, but with carve-outs).

160. Combating Auto Retail Scams Trade Regulation Rule, 89 Fed. Reg. 590, 591 (July 30, 2024) (to be codified at 16 C.F.R. 463).

161. *See generally* Petitioners' Opening Brief, Nat'l Auto. Dealers Ass'n v. FTC, No. 24-60013 (5th Cir. Mar. 15, 2024), 2024 WL 1238109; *see also* Fed. Trade Comm'n, Order Postponing Effective Date of Final Rule Pending Judicial Review, *supra* note 23, at 1 (staying the effective date of the CARS Rule due to the ongoing legal challenge alleging that the CARS Rule is "arbitrary, capricious, an abuse of discretion, without observance of procedure required by law, or otherwise not in accordance with law").

162. U.C.C. §§ 9-109(c)(1), 9-201(c) (AM. L. INST. & UNIF. L. COMM'N 2023).

163. *Id.* § 9-109(a)(1).

chattel paper.[164] Consumer vehicles likely qualify as "consumer goods" under Article 9.[165]

If an individual has obtained a loan to finance a vehicle purchase, and the creditor takes a security interest in the vehicle to secure the purchase price, the transaction is likely to be subject to Article 9. A failure to make timely payments is likely to qualify as an event of default under the loan agreement. Once in default, Article 9 provides the secured party, the lender or creditor "in whose favor a security interest is created,"[166] with various rights, including the right to take possession of the vehicle,[167] subject to some limitations.[168]

Article 9 uses the term "take possession,"[169] but case law also uses the term "repossession."[170] The ability to take possession of collateral upon default is subject to the lender's obligation to not breach the peace.[171] In addition to Article 9, states have also adopted specialized rules applicable to repossessions and motor vehicles.[172] The Uniform Consumer Credit Act also imposes a breach of the peace standard on repossessions.[173] A lender who has breached the peace could be subject to various forms of liability.[174]

---

164. *See id.* § 9-102(a)(11), (42), (44) (defining chattel paper, general intangibles, and goods as several categories of personal property).

165. *See id.* § 9-102(a)(23) (defining consumer goods as "goods that are used or bought for use primarily for personal, family, or household purposes"); *id.* § 9-102(a)(42) (defining software as a general intangible); *id.* § 9-102(a)(44) (defining goods to include various items as well as certain computer programs that are "embedded in goods").

166. *Id.* § 9-102(a)(73).

167. *Id.* § 9-609(a).

168. *Id.* § 9-610.

169. *Id.* § 9-609(a)(1).

170. *See, e.g.*, Van Wormer v. Charter Oak Fed. Credit Union, No. 114865, 2000 WL 1281530, at *1 (Conn. Super. Ct. Aug. 25, 2000); Avery v. Chrysler Credit Corp., 391 S.E.2d 410, 412 (Ga. Ct. App. 1990).

171. U.C.C. § 9-609(a)–(b).

172. STEPHEN L. SEPINUCK & KARA J. BRUCE, PROBLEMS AND MATERIALS ON SECURED TRANSACTIONS 187 (6th ed. 2023) ("Rhode Island requires a secured party repossessing a motor vehicle without the debtor's knowledge to notify the local police department within one hour after the repossession. . . . Louisiana has a non-uniform version of Article 9 that generally does not permit the secured party to repossess collateral unless the debtor has abandoned the collateral or consented to the repossession after or in contemplation of default."); CAL. CIV. CODE § 2983.2(b) (West 2012 & Supp. 2024) (subject to some exceptions "any provision in any conditional sale contract for the sale of a motor vehicle to the contrary notwithstanding, at least [fifteen] days' written notice of intent to dispose of a repossessed or surrendered motor vehicle shall be given to all persons liable on the contract").

173. UNIF. CONSUMER CREDIT CODE § 5.112 (1974); *see also* 12 SARA JANE HUGHES & FRED H. MILLER, HAWKLAND UNIF. COMM. CODE SERIES § 6:39, Westlaw (database updated Oct. 2023) ("The Uniform Consumer Credit Code (U3C), either the 1968, 1974 or a modified version, is the law in ten states.").

174. JAMES J. WHITE & ROBERT S. SUMMERS, UNIF. COMM. CODE § 26-7, at 1335–36 (6th ed. 2010) ("Section 9–609 authorizes repossession or the 'rendering' of equipment unusable without going to court only if the act of repossession or disabling of equipment can be done 'without breach of the peace.'" If such a breach occurs, the creditor may expose itself to: "(1) tort liability, including punitive damages; . . . (3) liability under 9–625; and (4) in a consumer case, it also may deprive the creditor of its right to a deficiency judgment." (footnotes omitted)).

Article 9 does not expressly restrict the use of electronic self-help or remote disablement in the consumer context, unlike other sources of law.[175] In 2022, the American Law Institute and the Uniform Law Commission approved important amendments to the UCC to address various technological developments. Despite these amendments, Article 9, as of the date of writing, does not expressly address remote disablement in the consumer goods context. It is still unclear whether a remote disablement qualifies as a repossession under Article 9. The failure to address remote disablement in the recent amendments reflects a missed opportunity to have the UCC more adequately ameliorate consumer concerns associated with VMC technology.

To the extent that a creditor must obtain "physical possession" of the collateral for a repossession to occur, merely disabling a borrower's vehicle using VMC technology is unlikely to qualify as a secured party taking possession of the collateral for Article 9 purposes.[176] To this end, Professor Juliet Moringiello observes that "the debtor remains in possession of the physical asset" even "[a]fter a remote disablement."[177] However, some case law suggests that physical possession may not always be required.[178] Still, there is a strong argument that the breach of the peace standard under Article 9 does not apply to remote disablement of consumer goods using VMC technology and that the current disablement provisions in Article 9 applies only to collateral that qualifies as "equipment" under Article 9 rather than consumer goods, such as consumer vehicles.[179]

In determining whether a breach of the peace has occurred, some courts primarily evaluate "(1) whether there was entry by the creditor upon the debtor's premises; and (2) whether the debtor or someone acting on his behalf consented (or objected) to the entry and repossession."[180] It is not entirely clear whether a lender's mere use of VMC technology to remotely

175. Such electronic self-help restrictions appear in, among other areas, model rules for software contracts. *See, e.g.*, PRINCIPLES OF THE L. OF SOFTWARE CONTS. § 4.03(b) (AM. L. INST. 2024) (prohibiting automated disablement in the absence of material breach).

176. *See, e.g.*, Dawson v. J & B Detail, L.L.C. (*In re* Dawson), No. 05-22369, 2006 WL 2372821, at *13 (Bankr. N.D. Ohio Aug. 15, 2006) ("Here, the defendants did not obtain possession of the Mustang when the on-time system disabled its ignition. By allowing the on-time system to disable her vehicle, the defendants did interfere with Dawson's use of the Mustang, but they did not deprive her of possession of it.").

177. Moringiello, *supra* note 14, at 584.

178. *See, e.g.*, Van Wormer v. Charter Oak Fed. Credit Union, 2000 WL 1281530, at *3 (Conn. Super. Ct. Aug. 25, 2000) ("Through no fault of their own, [the vehicle] was involved in an accident, presumably immobile and the defendant creditor did not have to physically retake the vehicle to protect its security interest and the value of such interest."); Avery v. Chrysler Credit Corp., 391 S.E.2d 410, 412 (Ga. Ct. App. 1990) ("In our view, it was unnecessary for plaintiff to exercise actual physical control of the automobile in order to repossess it. Rather, plaintiff could, and did, repossess the automobile by taking constructive possession of it."); Thomas B. Hudson & Daniel J. Laudicina, *The Emerging Law of Starter Interrupt Devices*, 61 BUS. LAW. 843, 845 (2006) (noting that "[i]f the use of starter interrupt devices is treated as a constructive repossession, the use must not result in a breach of peace" and that "a cautious approach would be to treat the use of the devices to render a vehicle inoperable as a repossession").

179. *See* U.C.C. § 9-609(a)(2) (AM. L. INST. & UNIF. L. COMM'N 2023).

180. WHITE & SUMMERS, *supra* note 174, § 26-7, at 1336.

disable a vehicle after a default will constitute a repossession that breaches the peace under Article 9 to the extent that the breach of the peace standard even applies. A lender's violation of repossession requirements can limit their recovery against a defaulting consumer and state statutes can authorize a defaulting consumer to sue for damages.[181]

Although Article 9 grants the creditor the ability to take possession of a vehicle upon default, section 9-610 also provides that after default the creditor must dispose of the collateral in a commercially reasonable manner.[182] Courts have considered several factors in determining whether a disposition has been conducted in a commercially reasonable manner, including whether the creditor "advertise[d] or employ[ed] other proper measures for finding the best market," "conduct[ed] the sale at the same time and place as that specified in the advertisements," and sold the collateral "at a propitious time."[183] Section 9-627 also provides some guidance on what constitutes a commercially reasonable disposition, such as if the disposition is "in conformity with reasonable commercial practices among dealers in the type of property that was the subject of the disposition."[184] A creditor's failure to conduct a commercially reasonable disposition may negatively impact the viability of any deficiency claims brought by the creditor against the debtor.[185] The

181. Legal Action Chicago Comment Letter, *supra* note 4, at 5 (citing 810 ILL. COMP. STAT. ANN. 5/9-625, 9-626(3) (West 2004)) (discussing "the "significant implications" of construing "kill switches" as constructive repossession are "especially" noteworthy in "jurisdictions like Illinois, where a creditor's violation of the repossession statutes may bar recovery and even give rise to a counterclaim for statutory damages").

182. U.C.C. § 9-610(a); CAROLYN L. CARTER, JONATHAN SHELDON, JOHN W. VAN ALST, TARA TWOMEY & JEREMIAH BATTLE, JR., REPOSSESSIONS: CONSUMER CREDIT AND SALES LEGAL PRACTICE SERIES § 10.2.1, at 293 (9th ed. 2017) ("The fundamental rule concerning the sale of repossessed property is that every aspect of the sale must be commercially reasonable.").

183. WHITE & SUMMERS, *supra* note 174, § 26-10, at 1346–47; Regal Fin. Co. v. Tex Star Motors, Inc., 355 S.W.3d 595, 601–02 (Tex. 2010) ("Although commercial reasonableness is not precisely defined in Article 9, courts have considered a number of nonexclusive factors when addressing the term, such as: (1) whether the secured party endeavored to obtain the best price possible; (2) whether the collateral was sold in bulk or piecemeal; (3) whether it was sold via private or public sale; (4) whether it was available for inspection before the sale; (5) whether it was sold at a propitious time; (6) whether the expenses incurred during the sale were reasonable and necessary; (7) whether the sale was advertised; (8) whether multiple bids were received; (9) what state the collateral was in; and (10) where the sale was conducted."); *see also* R & J of Tenn., Inc. v. Blankenship-Melton Real Est., Inc., 166 S.W.3d 195, 206 (Tenn. Ct. App. 2004), *abrogated on other grounds by* Auto Credit of Nashville v. Wimmer, 231 S.W.3d 896 (Tenn. 2007) ("Although the statute has not attempted to define the parameters of the term 'commercially reasonable', case law has specified six factors by which the statute requirements may be measured: (1) the type of collateral involved; and (2) the condition of the collateral; and (3) the number of bids solicited; and (4) the time and place of sale; and (5) the purchase price received or the terms of the sale; and (6) any special circumstances involved.").

184. U.C.C. § 9-627(b).

185. *See, e.g.*, *Regal Fin. Co.*, 355 S.W.3d at 599 ("A secured creditor must prove it disposed of the collateral in a commercially reasonable manner before it may recover any deficiency."); David Gray Carlson, *Commercially Reasonable Sales in the 21st Century*, 50 OHIO N.U. L. REV. 47, 47–48 (2023) ("[I]f, in his answer to [a secured party's] complaint, [the defendant] or his surety . . . alleges commercial unreason, then presumptively the secured claim is deemed satisfied by the foreclosure sale, and [the secured party] may not collect the deficit.").

comments to section 9-610 note that a creditor that "holds collateral for a long period of time without disposing of it," with "no good reason for not making a prompt disposition, . . . may be determined not to have acted in a 'commercially reasonable' manner."[186] Section 1-304 of the UCC imposes a good faith obligation on parties in connection with the "performance and enforcement" of their contracts and duties under the UCC.[187]

A creditor's use of a kill switch to disable a vehicle for an extended period of time without subsequently retrieving or disposing of the vehicle arguably renders the vehicle useless to the consumer and brings the vehicle within the creditor's control. The creditor's use of the kill switch and failure to then subsequently dispose of the collateral after a lengthy time period could potentially violate the "commercially reasonable" disposition standard.[188] In one lawsuit, the consumer alleged that the creditor instituted a policy of keeping "kill switches activated for months—and even years—without making any good faith effort to physically retrieve and resell the repossessed vehicles."[189] In that case, the creditor allegedly activated a kill switch device in the consumer's vehicle for more than two years and failed to deactivate it, or sell the vehicle, which led the vehicle to "lose value and deteriorate."[190] The creditor required consumers to pay "additional fee[s] to deactivate the kill switch" once it was activated.[191] In another case, *Nationsbank v. Clegg*, the court found that the creditor's sale of a used vehicle was commercially unreasonable because the creditor waited thirteen months to dispose of the vehicle.[192]

In the context of a strict foreclosure, when a transaction involves a purchase money security interest ("PMSI") in consumer goods (such as when the creditor provides financing to allow the consumer to obtain rights in the consumer goods) or a non-PMSI loan in consumer goods and the consumer has not after default executed a document amending their rights, Article 9 imposes a

186. U.C.C. § 9-610 cmt. 3.

187. *Id.* § 1-304.

188. Overland Bond & Inv. Corp. v. Calhoun, No. 1-22-1804, 2023 WL 8177123, ¶ 8 (Ill. App. Ct. Nov. 27, 2023); *see also* Consol. First Amended Verified Answer, Affirmative Defs., and Class Action Counterclaims ¶ 3, Overland Bond & Inv. Corp. v. Calhoun, No. 2021-M1-108114 (Ill. Cir. Ct. July 15, 2022) [hereinafter Overland Pleading], https://legalactionchicago.org/wp-content/uploads/2022/07/Class-Action-Counterclaims-Overland.pdf [https://perma.cc/22B9-69SY] ("The [UCC], 810 ILCS 5/9-610, requires a secured party to sell or otherwise dispose of collateral in a 'commercially reasonable' manner. Failure to do so constitutes a complete defense to an action based on a failure to pay the debt at issue.").

189. Overland Pleading, *supra* note 188, ¶ 40.

190. *Id.* ¶¶ 5, 51–52.

191. *Id.* ¶ 41.

192. Nationsbank v. Clegg, No. 01-A-01-9510-CH-00469, 1996 Tenn. App. LEXIS 214, at *9 (Tenn. Ct. App. Apr. 10, 1996), *abrogated on other grounds by* Auto Credit of Nashville v. Wimmer, 231 S.W.3d 896 (Tenn. 2007) ("We have found no evidence in the record, or other authority which indicates that the [thirteen] month delay in selling the automobile, a depreciating asset, is 'in keeping with the prevailing trade practices among reputable firms engaged in similar business activities,' in Tennessee. Thus, the delay appears unreasonable to this Court.").

ninety-day time frame for collateral dispositions if certain additional conditions are met, such as payment of sixty percent of the loan.[193]

The types and quantity of data now available in the IoT setting, including data derived from VMC technology, has expanded significantly. Consumer automobile lenders and dealers that provide financing have long retained some degree of control over consumers post-transaction. However, the examples discussed in previous sections of this Article suggest that VMC technology allows lenders and dealers to over-extend this post-transaction control over consumers and their vehicles, and potentially collect significant amounts of data about customers' driving habits and their frequently visited locations. SID and geofence features exemplify this growing post-transaction control. Article 9 provides insufficient guidance on significant issues associated with VMC technology, including whether a remote disablement qualifies as a repossession and the application of the breach of the peace standard.

B. VMC STATE STATUTES

Some states have adopted laws to specifically address VMC technology or amended existing statutes to address remote disablement.[194] California requires buy-here-pay-here ("BHPH") dealers to issue notice and obtain written consent and authorizes electronic tracking technology if it "is used solely to verify and maintain the operational status of the tracking technology, to repossess the vehicle, or to locate the vehicle to service the loan or keep the loan current"

193. U.C.C. § 9-103 (AM. L. INST. & UNIF. L. COMM'N 2023) (defining a purchase money security interest); *id.* § 9-620(e)–(f) ("A secured party that has taken possession of collateral shall dispose of the collateral pursuant to Section 9-610 within the time specified in subsection (f) if: (1) [sixty] percent of the cash price has been paid in the case of a purchase-money security interest in consumer goods; or (2) [sixty] percent of the principal amount of the obligation secured has been paid in the case of a non-purchase-money security interest in consumer goods. . . . To comply with subsection (e), the secured party shall dispose of the collateral: (1) within [ninety] days after taking possession; or (2) within any longer period to which the debtor and all secondary obligors have agreed in an agreement to that effect entered into and signed after default."); SEPINUCK & BRUCE, *supra* note 172, at 210 ("In a consumer transaction, the secured party is prohibited from accepting the collateral in partial satisfaction of the debt; only strict foreclosure is permitted."); *id.* at 210 (noting that per UCC § 9-620 if the consumer has built up sixty percent equity in the consumer goods, "the secured party is prohibited from conducting a strict foreclosure" and must instead "conduct a disposition [of the collateral] pursuant to § 9-610"); *Vehicle Repossession*, FED. TRADE COMM'N (Sept. 2023), https://consumer.ftc.gov/articles/vehicle-repossession [https://perma.cc/97Z4-FPQE] ("After your vehicle is repossessed, your lender can either keep it to cover your debt or sell it. In some states, your lender has to let you know what will happen.").

194. *See, e.g.*, CAL. CIV. CODE § 2983.37 (West Supp. 2024) (amending); COLO. REV. STAT. § 4-9-609(e) (2023) (amending); CONN. GEN. STAT. §§ 42-419(d), 42a-2A-702(e), 42a-9-609 (2023) (amending); NEV. REV. STAT. § 598.9715 (2023) (adopting); N.Y. U.C.C. LAW § 9-102(60-a) (McKinney Supp. 2024) (amending); N.Y. GEN. BUS. LAW § 601(10) (McKinney 2023) (amending); *see also* Legal Action Chicago Comment Letter, *supra* note 4, at 8 (noting that this "is an emerging area of law, and most jurisdictions have not yet responded to the problems [associated with VMC technology] with a legislative solution"); Moringiello, *supra* note 14, at 585, 587 ("Several states have recognized in their statutes that creditors have the ability to disable collateral remotely. . . . A handful of states target subprime automobile lending in their statutes regulating the use of remote disablement.").

or for other limited purposes described in the statute.[195] The California statute appears to directly address the ability of covered companies to use covered devices to enable certain types of pre-default surveillance, but the scope of the statute suggests that it applies primarily to entities that qualify as a BHPH dealer.[196]

New Jersey allows for the use of payment assurance devices in consumer transactions but obligates creditors to give notice and acquire consumer acknowledgement.[197] Before disabling a vehicle, lenders must wait for a statutorily specified number of days after a driver is in default.[198] Lenders must provide drivers with a seventy-two-hour grace period prior to remotely disabling their vehicles and allow drivers to operate their vehicles for at least forty-eight hours.[199] Lenders cannot disable a "vehicle while it is being operated."[200] These restrictions may help set limits on the use of VMC technology post-transaction and, to some extent, curtail the electronic subjugation powers of lenders.

Nevada's VMC technology statute expressly provides that the use of a SID to disable a "motor vehicle constitutes constructive repossession,"[201] which perhaps suggests that the breach of the peace standard would apply to a remote disablement in Nevada. The Nevada statute appears to permit electronic tracking as long as it is "optional and not a required condition of the retail installment contract or lease" and the buyer agrees in writing, or if statutory notice requirements are satisfied.[202]

---

195. CAL. CIV. CODE § 2983.37; *see also* CAL. VEH. CODE § 241 (West 2015) (defining a "buy-here-pay-here" dealer).

196. CAL. CIV. CODE § 2983.37.

197. N.J. STAT. ANN. § 56:8-206 (2023); *see also id.* § 56:8-205 (defining a "payment assurance device" as "a device installed on a motor vehicle with global positioning system capability, starter interrupt capability allowing for the remote enabling or disabling of the motor vehicle, or both, and which is installed pursuant to a motor vehicle consumer's financing agreement or lease agreement"); Moringiello, *supra* note 14, at 588 ("New Jersey's restrictions are also limited to consumer motor vehicle financing, and they require robust notice of the use of such a device, a grace period before activation, a warning prior to activation, and the ability of the borrower to use the vehicle for a period of forty-eight hours post-disablement. New Jersey's statute makes clear that a vehicle cannot be disabled while in motion." (internal footnote omitted)).

198. N.J. STAT. ANN. § 56:8-206(b)(3) ("A creditor may install or have installed a payment assurance device on a motor vehicle only if: . . . the creditor or an agent thereof does not remotely disable the motor vehicle until the consumer is in default on any term under the financing agreement or lease agreement, including but not limited to the periodic payment due on the purchase or lease, for five or more calendar days on a financing agreement or lease agreement whose terms call for at least one weekly payment or for ten or more calendar days on any other financing agreement or lease agreement . . . .").

199. *Id.* § 56:8-206(b)(4), (6).

200. *Id.* § 56:8-206(b)(5).

201. NEV. REV. STAT. § 598.9715(2)(c) (2023); Moringiello, *supra* note 14, at 587–88 (Nevada's "statute specifies that automated shutoff is a 'constructive repossession' for the purposes of Articles 2A and 9 of the UCC and Nevada's law governing contracts for the installment sale of vehicles.").

202. NEV. REV. STAT. § 598.9715(1).

Nevada also imposes limitations on the use, sale, and disclosure of "telemetry data" collected from such devices and the statute contains data retention restrictions.[203] Nevada's data use and sale restrictions apply to "a person who possesses or obtains telemetry data related to a consumer that is collected by electronic tracking technology or starter interruption technology."[204] The term "[e]lectronic tracking technology" appears to be limited solely to technology that collects or records location data and the term "[s]tarter interruption technology" under the statute appears to cover only technology that disables the engine or stater of a vehicle or that causes an audible sound.[205] Nevada's data-related restrictions appear to limit secondary data uses and disclosures to third parties, thereby restraining covered entities' ability to subsequently profit from such data at the expense of consumers' privacy. However, the statute's language suggests that these restrictions apply to "telemetry data" that is "related to a consumer."[206] It is not entirely clear whether all of these restrictions apply equally to anonymized and aggregated telemetry data that may arguably not directly relate to a consumer, even though inferences about a consumer may be gleaned from such data.[207] The statute's data monetization and retention restrictions do not appear to apply to the manufacturers of motor vehicles with "electronic tracking technology or starter interruption technology."[208] Thus, the statute may not apply to vehicles with manufacturer installed VMC features or the Ford patent application example discussed earlier.

---

203. *Id.* § 598.9716(3). The statute defines "telemetry data" as "any information collected by electronic tracking technology or starter interruption technology, regardless of whether such information is transmitted or retained in the device, and includes, without limitation, information pertaining to the location, speed and motion status of a motor vehicle." *Id.* § 598.9716(5)(b). *See generally What Is Telematics?*, VERIZON CONNECT (June 26, 2023), https://www.verizonconnect.com/resources/article/what-is-telematics [https://perma.cc/T5V5-ZS86] (discussing vehicle telematics and noting that "telematics data captured can include location, speed, idling time, harsh acceleration or braking, fuel consumption, vehicle faults, and more").

204. NEV. REV. STAT. § 598.9716(3).

205. *Id.* § 598.9706 (defining "[e]lectronic tracking technology" as "technology that enables the use of a global positioning satellite or similar technology to obtain or record the location of a motor vehicle"); *id.* § 598.9714 (defining "[s]tarter interruption technology" as "technology which can be used to remotely disable the starter of a motor vehicle or to remotely cause an audible sound in a motor vehicle, or both").

206. *Id.* § 598.9716(3) ("A person who possesses or obtains telemetry data related to a consumer that is collected by electronic tracking technology or starter interruption technology may not: (a) Sell any telemetry data. (b) Provide any telemetry data to any person or entity other than: . . . .").

207. *See id.* One might argue that the use and purpose restriction contained in the Nevada statute could impose limits on companies' ability to anonymize and aggregate the data in the first place as such uses may go beyond the permissible uses expressly authorized by the statute. The statute is not entirely clear on this point. *Id.* § 598.9716(3)(c).

208. *Id.* § 598.9716(4)(a) (stating that the section's provisions do not apply to the "manufacturer, or an affiliate under common control or ownership of the manufacturer, of a motor vehicle which is equipped with electronic tracking technology or starter interruption technology or from which telemetry data is obtained").

At least two states have adopted nonuniform amendments to Article 9 to address creditors' use of electronic self-help.[209] Connecticut obligates lenders to acquire the borrower's agreement to make use of electronic self-help and provide notice of intent to use self-help.[210] Limitations on electronic self-help also exist to the extent that the creditor "has reason to know" that injury to the "public health" could occur.[211] Colorado's amended Article 9 provisions appear to apply to electronic disablement in connection with collateral that qualifies as equipment under Article 9 rather than consumer goods.[212] Thus, the existing provisions in Colorado's version of Article 9 are unlikely to apply to the use of VMC technology in consumer vehicle transactions.

Some states have also provided informal guidance on the use of VMC technology.[213] With respect to states that have not directly addressed remote disablement in consumer transactions, at least one scholar has suggested that the use of VMC technology devices in such transactions could be evaluated by "using general principles guiding the exercise of self-help repossession."[214]

In summary, VMC technology state statutes often permit the use of this technology and electronic self-help subject to certain requirements. Some states broadly attempt to address the use of various types of VMC technology while others are focused primarily on SIDs or certain types of entities, and at least one state attempts to directly address data use concerns.[215] For instance, recall that California's statute appears to apply primarily to only certain types of dealers. Additionally, as Professor Juliet Moringiello observes, "the scope of California's [VMC statute] restrictions is narrow; its restrictions apply only

209. *See, e.g.*, COLO. REV. STAT. § 4-9-609(c) (2023) (making such an amendment); CONN. GEN. STAT. § 42a-9-609 (2023) (same). New York also revised its version of Article 9 of the UCC to include a definition of the term "payment assurance device," but the provisions imposing limitations on the use of such devices are not primarily contained in the state's version of the UCC. N.Y. U.C.C. LAW § 9-102(60-a) (McKinney Supp. 2024); N.Y. GEN. BUS. LAW § 601(10).

210. CONN. GEN. STAT. § 42a-9-609(d)(2).

211. *Id.* § 42a-9-609(d)(5).

212. COLO. REV. STAT. § 4-9-609. A secured party, after default, may "without removal, may render equipment unusable and dispose of collateral on a debtor's premises under section 4-9-610." *Id.* § 4-9-609(a)(2). In exercising its rights under this subsection with respect to collateral, "a secured party may not disable or render unusable any computer program or other similar device embedded in the collateral if immediate injury to any person or property is a reasonably foreseeable consequence of such action." *Id.* § 4-9-609(e).

213. Memorandum from John Sande IV to the Nev. Assemb. Comm. on Com. & Lab. (Mar. 22, 2013), https://www.leg.state.nv.us/Session/77th2013/Exhibits/Assembly/CL/ACL493C.pdf [https://perma.cc/2CNK-B9L6] (discussing Kansas, Missouri, Maine, and Iowa); *see also* Atta-Krah, *supra* note 20, at 1204–05 (discussing Iowa, Maryland, and Missouri).

214. Moringiello, *supra* note 20, at 299.

215. Legal Action Chicago Comment Letter, *supra* note 4, at 7–8 (discussing different types of kill switches and noting that "some states have attempted to broadly regulate all kill switch devices (CT, CO, NY), while others have more narrowly focused on starter interrupters (CA, NV)"); *Who We Are*, LEGAL ACTION CHI. (2023), https://legalactionchicago.org/who-we-are [https://perma.cc/H8LK-CKCW]; *Court Cases*, LEGAL ACTION CHI., https://legalactionchicago.org/what-we-do/class-actions [https://perma.cc/Z5RU-S8ZJ] ("Legal Action filed its first class action lawsuit on behalf of clients . . . [whose] cars were remotely disabled by Chicago-based Overland Bond & Investment Corporation by activating 'kill switches' previously installed by its car dealer partner Car Credit Center.").

to the automated shutoff of cars and, further, only to the use of automated means of disablement by [BHPH] dealers."[216]

One analysis of VMC technology state statutes by Legal Action Chicago, an organization that initiates legal cases on behalf of underserved populations, including bringing class actions against at least one VMC technology provider for improper use of kill switches, notes that not all laws in this area provide for a private right of action.[217] Additionally, some of these laws appear to rely significantly on the notice-and-choice (sometimes called "notice and consent") model to protect borrowers in transactions involving VMC technology, although some impose limits on the timing of remote disablement and contain data restrictions, among other things.[218] While providing notice to consumers of the use of VMC technology in their vehicles post-transaction may address exclusion concerns related to the failure to allow consumers to know about the data that lenders and dealers collect about them from VMC technology, it does not address another important aspect of exclusion: "the failure to allow the data subject to . . . participate in [the] handling and use" of that data after collection.[219]

Additionally, legal scholars have long highlighted the many failures of relying excessively on notice-and-choice in the privacy context.[220] With

---

216. Moringiello, *supra* note 14, at 587.

217. Legal Action Chicago Comment Letter, *supra* note 4, at 8 (noting that California, Connecticut, Nevada, and New York "have provided consumers with a private right of action for violations of the kill switch statue" and "established notice requirements providing for disclosure of a kill switch's existence and how it will be used" but that "Colorado has not" done either).

218. Solove, *Murky Consent*, *supra* note 27, at 596–97 ("There are generally two approaches to consent in privacy law, and both fail to work effectively. In the United States, the notice-and-choice approach predominates, in which organizations post a notice about their privacy practices and then people are deemed to have consented to these practices if they fail to opt out. In the European Union ('EU'), the General Data Protection Regulation ('GDPR') uses the express consent approach, in which people must voluntarily and affirmatively consent (opt in)."); Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy: (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 11 ("[T]he substitution of 'notice and choice' for 'notice and consent' transferred the protection of privacy from the legal realm, and from an emphasis on the articulation of rights and responsibilities, to the marketplace, where consumers would now be forced to pay for what the law could otherwise provide."); James W. Hazel & Christopher Slobogin, *Who Knows What, and When?: A Survey of the Privacy Policies Proffered by U.S. Direct to Consumer Genetic Testing Companies*, 28 CORNELL J.L. & PUB. POL'Y 35, 38 (2018) ("Under the current US self-regulatory 'Notice and Choice' (or 'Notice and Consent') framework, a company's privacy documents (usually denominated a Privacy Policy or Terms of Service) provide Notice of a company's data practices, while the consumer's actions (such as clicking 'I agree' or utilizing the service) provide the Choice/Consent.").

219. Solove, *A Taxonomy of Privacy*, *supra* note 28, at 490.

220. *See, e.g.*, Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 341, 341 (Jane K. Winn ed., 2006) (deeming such an approach "unsuccessful in practice" and noting that "individuals endure an onslaught of notices and opportunities for often limited choice"); Kirsten Martin, *Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online*, 34 J. PUB. POL'Y & MKTG. 210, 211 (2015) (noting that there exists "considerable agreement that the notice-and-choice model has failed to meet the privacy expectations of users online"); Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140

potentially fewer alternatives, a subprime borrower may have no choice but to agree to a creditor's use of VMC technology to obtain access to a motor vehicle. Consumers, often by law, must review and execute a significant number of documents in lending transactions, although it is unlikely that most consumers review in detail or sufficiently understand these disclosures. Statutorily imposing requirements for additional VMC technology or electronic self-help disclosures, without more, is unlikely to successfully communicate to borrowers the possible privacy and electronic subjugation implications of entering a transaction that authorizes the creditor to use VMC technology. Lastly, despite possible shortcomings in existing state statutes on VMC technology, individuals in states that have not directly addressed VMC technology may have even fewer protections than consumers in states that have adopted laws to deal with VMC technology.

C. STATE PRIVACY LAW STATUTES

As of the date of writing, eighteen states have adopted comprehensive state privacy laws.[221] This section evaluates key provisions from five of these laws. The CCPA is the first state privacy statute of its kind in the United States. The statute has several notable provisions. For instance, it restricts covered companies' ability to force consumers to waive statutorily granted privacy rights by expressly providing that any such contractual provisions are invalid.[222] The CCPA also grants California residents various rights with respect to their data, including access rights, deletion rights, data sale and sharing rights and "the right to non-discrimination" in exercising CCPA granted rights.[223]

The CCPA contains several exclusions that may impact the statute's applicability to data involved in some types of vehicular transactions. First, the CCPA excludes information covered by the Gramm–Leach–Bliley Act ("GLBA").[224] We will come back to the GLBA below. Second, the statute also creates an exemption for vehicle data "retained or shared between a new motor vehicle dealer" and a vehicle manufacturer "if the vehicle information or ownership information is shared for the purpose of effectuating, or in

---

DÆDALUS 32, 32, 34–35 (2011) (noting that attempted improvements, such as "clearer privacy policies and fairer information practices," cannot "overcome a fundamental flaw in the [notice-and-choice] model").

221. *Which States Have Consumer Data Privacy Laws?*, BLOOMBERG L. (Mar. 18, 2024), https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker (on file with the *Iowa Law Review*).

222. CAL. CIV. CODE § 1798.192 (West 2022) ("Any provision of a contract or agreement of any kind, including a representative action waiver, that purports to waive or limit in any way [a consumer's] rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable."); Press Release, Rob Bonta, Att'y Gen. of Cal., California Consumer Privacy Act (CCPA) (Mar. 13, 2024) [hereinafter AG on CCPA], https://oag.ca.gov/privacy/ccpa [https://perma.cc/WA6Y-NTXB] ("Businesses cannot make you waive these rights, and any contract provision that says you waive these rights is unenforceable.").

223. AG on CCPA, *supra* note 222; *see also* CAL. CIV. CODE §§ 1798.100, .105, .110, .130.

224. CAL. CIV. CODE § 1798.145(e) ("This title shall not apply to personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act.").

anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall."[225] Notwithstanding these exemptions, the CCPA's provisions are likely to apply to a large number of transactions involving consumers and their vehicles. For example, in 2023, the California Privacy Protection Agency ("CPPA") announced plans to review the privacy practices of entities collecting vehicle data, including the activities of connected automobile manufacturers and associated technologies.[226] The Connecticut and Texas attorneys general have recently announced similar plans.[227]

Inspired by the CCPA, several states have also adopted broad privacy statutes. Like the CCPA, the Colorado Privacy Act ("CPA"), the Virginia Consumer Data Protection Act ("VCDPA"), the Utah Consumer Privacy Act ("UCPA"), and the Connecticut Data Privacy Act ("CDPA") grant various rights to the citizens of those states.[228] Examples include the right to access and delete data under certain circumstances.[229]

Under the CCPA and its related amendments, subject to some exceptions, consumers can opt out of the sale and sharing of their data. Its definition of the term "sale" includes releasing, renting, selling, transferring, disclosing, or making available consumers' personal information "to a third party for monetary or other valuable consideration."[230] Likewise, it defines "sharing" as the disclosure of personal information to a third party for "cross-context behavioral advertising, whether or not for monetary or other valuable consideration."[231] There are several exceptions to the definition of sharing,

225. *Id.* § 1798.145(g)(1).

226. Press Release, Cal. Priv. Prot. Agency, CPPA to Review Privacy Practices of Connected Vehicles and Related Technologies (July 31, 2023), https://cppa.ca.gov/announcements/2023/20230731.html [https://perma.cc/8F9V-8SUT].

227. Allison Grande, *Texas AG Taxes Aim at Carmakers Selling Drivers' Data*, LAW360 (June 6, 2024), https://www.law360.com/consumerprotection/articles/1845243 (on file with the *Iowa Law Review*).

228. COLO. REV. STAT. §§ 6-1-1301–1313 (2023); CONN. GEN. STAT. §§ 42-515–525 (2023 & Supp. 2024); UTAH CODE ANN. §§ 13-61-101–404 (2022 & Supp. 2024); VA. CODE ANN. §§ 59.1-575–584 (Supp. 2024).

229. COLO. REV. STAT. § 6-1-1306(1)(b), (d); ALAN L. FRIEL, JULIA B. JACOBSON & KYLE FATH, SQUIRE PATTON BOGGS, PREPARING FOR 2023: STATE PRIVACY LAW COMPLIANCE 4 (2022), https://www.squirepattonboggs.com/-/media/files/insights/publications/2022/05/preparing-for-2023-state-privacy-law-compliance/preparingfor2023stateprivacylawcompliance.pdf [https://perma.cc/DB5L-6PY3].

230. CAL. CIV. CODE § 1798.140(ad)(1) ("'Sell,' 'selling,' 'sale,' or 'sold,' means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration.").

231. *Id.* § 1798.140(ah)(1) ("'Share,' 'shared,' or 'sharing' means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged."); *id.* § 1798.140(k) (defining "[c]ross-context behavioral advertising" as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's

such as instances in which a consumer directs a company to intentionally share data.[232]

Other states have also given consumers a right to opt out of the sale of their data or the use of their data for targeted advertising. The CPA, CDPA, and the VCDPA allow consumers to opt out of the sale of their data, targeted advertising and profiling "in furtherance of decisions that produce legal or similarly significant effects concerning a consumer."[233] Under the UCPA, residents have the right to opt out of the processing of their data for the purposes of targeted advertising and data sales.[234] Unlike the CCPA, which defines the term "sale" to also include "valuable consideration," the term "sale" under the UCPA is narrowly defined as "the exchange of personal data for monetary consideration by a controller to a third party."[235] The definition

activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts").

232. *Id.* § 1798.140(ah)(2).

233. COLO. REV. STAT. § 6-1-1306(1)(a) (2023) ("Right to opt out. (I) A consumer has the right to opt out of the processing of personal data concerning the consumer for purposes of: (A) Targeted advertising; (B) The sale of personal data; or (C) Profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer."); CONN. GEN. STAT. § 42-518(a) (2023) ("A consumer shall have the right to: (1) Confirm whether or not a controller is processing the consumer's personal data and access such personal data, unless such confirmation or access would require the controller to reveal a trade secret; (2) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data; (3) delete personal data provided by, or obtained about, the consumer; (4) obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means, provided such controller shall not be required to reveal any trade secret; and (5) opt out of the processing of the personal data for purposes of (A) targeted advertising, (B) the sale of personal data, except as provided in subsection (b) of 42-520, or (C) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer."). The CDPA's definition of sale is somewhat similar to the CCPA. *Connecticut Data Privacy Act—What Businesses Need to Know*, AKIN GUMP (May 26, 2022), https://www.akingump.com/en/news-insights/connecticut-data-privacy-act-what-businesses-need-to-know.html [https://perma.cc/E3C8-38V3]. The same can be said of the VCDPA and CCPA. *Compare* VA. CODE ANN. § 59.1-577(A)(5) (granting residents the right to opt-out data sales and data processing for "targeted advertising" and "profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer"), *with* CAL. CIV. CODE § 1798.120(a) ("A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. This right may be referred to as the right to opt-out of sale or sharing.").

234. UTAH CODE ANN. § 13-61-201(4) (2022) ("A consumer has the right to opt out of the processing of the consumer's personal data for purposes of: (a) targeted advertising; or (b) the sale of personal data.").

235. *Compare id.* § 13-61-101(31)(a) (2022 & Supp. 2024), *with* CAL. CIV. CODE § 1798.140(ad)(1) (defining "sale"); *see also* Natasha G. Kohne, Michelle A. Reed, Jo-Ellyn Sakowitz Klein, Rachel Claire Kurzweil & Tina M. Jeffcoat, *Utah Consumer Privacy Act: What Businesses Need to Know*, AKIN GUMP (Apr. 8, 2022), https://www.akingump.com/en/insights/alerts/utah-consumer-privacy-act-what-businesses-need-to-know [https://perma.cc/UYG5-5VCD] ("[T]he UCPA bears more resemblance to Virginia's law than Colorado's, adopting, for example, the VCDPA's narrower definition of 'sale' and providing enforcement exclusively through the state attorney general.").

of "sale" excludes data disclosures to third parties "if the purpose is consistent with a consumer's reasonable expectation."[236]

Statutory restrictions on the sale or sharing of data may be helpful in addressing certain secondary uses discussed in Part I. For instance, a driver could elect to exercise their right to stop an automobile manufacturer or dealer from selling data collected via VMC technology or connected vehicles. The usefulness of this right depends primarily on a driver's decision to exercise the right to stop the sale or sharing. Thus, those individuals who fail to opt out will have their data sold or shared. Individuals who elect to opt out of the sale of their data may lose access to vital connected vehicle features. For instance, Tesla's privacy policy notes that opting out of data collection and deactivating connectivity may lead vehicles to suffer from decreased "functionality, serious damage, or inoperability."[237] Drivers who choose to exercise a right to delete could, in theory, have their vehicle data deleted. However, a 2023 Mozilla Foundation report on the privacy practices of connected vehicle manufacturers found that "[only] two of the [twenty-five studied] car brands . . . sa[id] that all drivers have the right to have their personal data deleted."[238]

Admittedly, through the 2020 amendments to the CCPA, the statute has taken incremental steps away from the standard notice-and-choice and rights-based regimes in some respects. For instance, consider the amendments' imposition of data minimization and retention limitations with which companies must comply.[239] More recently, the CPPA issued an enforcement advisory on

236. UTAH CODE ANN. § 13-61-101(31)(b)(iii); *see also* Kohne et al., *supra* note 235 ("Unlike in California, Colorado or Virginia, the UCPA's definition of a sale contains a unique exemption that allows a controller to disclose personal data to a third party if the purpose is consistent with the consumer's 'reasonable expectations.'").

237. Caltrider et al., *supra* note 87.

238. *Id.*

239. CAL. CIV. CODE § 1798.100(a)(3) ("[A] business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose."); *id.* § 1798.100(c) ("A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes."). A few commentators have noted the difference between the California Privacy Rights Act ("CPRA") and the European General Data Protection Regulation ("GDPR"). One in particular contends that "[i]t is clear that the CPRA's data minimization requirements are not as restrictive as the GDPR's requirements under Article 5. For example, the GDPR requires that a business does not collect or retain irrelevant personal information. In comparison, CPRA more broadly requires that additional categories of personal information or sensitive personal information are not collected for an incompatible purpose. Additionally, the CPRA does not define how long is a 'reasonably necessary' period of storage." Andrew Scott, *T-Mobile's Breach Highlights the Importance of Data Minimization and CPRA*, CAL. LAWS. ASS'N (2024), https://calawyers.org/privacy-law/t-mobiles-breach-highlights-the-importance-of-data-minimization-and-cpra [https://perma.cc/JX5P-VQ5D]; *see also* Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the

the CCPA's data minimization requirements in 2024.[240] The FTC has also recommended that firms implement data minimization practices as well.[241] Statutory restrictions on dark patterns in obtaining consent are also notable in that they address another aspect of privacy by design, a concept mandated by the European General Data Protection Regulation.[242] Other state statutes

---

Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 5(1)(b)–(f), 2016 O.J. (L 119) 35, 36 [hereinafter GDPR]. However, some disagree with this conclusion. *See, e.g.*, Christian Auty & Goli Mahdavi, BCLP, *The CPRA Digest: Data Minimization*, JDSUPRA (Jan. 7, 2021), https://www.jdsupra.com/legalnews/the-cpra-digest-data-minimization-7893221 [https://perma.cc/8PKJ-5LLV] ("Data minimization – a core principle under GDPR but not mandated under the CCPA – is now effectively required under the CPRA. Specifically, the CPRA bars businesses from collecting more personal information than 'reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed . . . .'"); Natasha Kohne, Michelle Reed & Rachel Kurzweil, *Calif. Privacy Law Resembles, Transcends EU Data Regulation*, LAW360 (Nov. 13, 2020, 4:30 PM), https://www.law360.com/articles/1327949/calif-privacy-law-resembles-transcends-eu-data-regulation (on file with the *Iowa Law Review*) ("The CPRA's enhanced privacy protections were clearly meant to position California as an adequate jurisdiction to which companies in EU Member States can transfer data pursuant to GDPR Article 45. . . . the CPRA incorporates data retention limitations."). As this last article suggests, the CPRA arguably arose, in part, due to a lack of strong consumer-friendly provisions in the CCPA. *See* CAL. CIV. CODE § 1798.185. Indeed, there is scholarship comparing the CCPA to the GDPR. *See, e.g.*, Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1756 (2021) (discussing the GDPR's purpose, retention, and data minimization requirements but suggesting that the CCPA lacks these components); Gabriela Zanfir-Fortuna, *10 Reasons Why the GDPR Is the Opposite of a 'Notice and Consent' Type of Law*, FUTURE PRIV. F. (Sept. 13, 2019), https://fpf.org/blog/10-reasons-why-the-gdpr-is-the-opposite-of-a-notice-and-consent-type-of-law [https://perma.cc/6WEY-XDB4] (noting that under the GDPR "[a]ll organizations that engage in any sort of sensitive, complex or large scale data uses must conduct a Data Protection Impact Assessment (DPIA) before proceeding" and contending that this requirement pushes the GDPR beyond the traditional notice-and-choice model). *Compare* GDPR, *supra*, art. 35, at 53–54, *with* CAL. CIV. CODE § 1798.185(a)(15) (suggesting that the CCPA might one day incorporate a similar audit provision).

240. *See generally* CAL. PRIV. PROT. AGENCY ENF'T DIV., ENFORCEMENT ADVISORY NO. 2024-01, APPLYING DATA MINIMIZATION TO CONSUMER REQUESTS (2024), https://cppa.ca.gov/pdf/enfadvisory202401.pdf (on file with the *Iowa Law Review*).

241. *FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks*, FED. TRADE COMM'N (Jan. 27, 2015), https://www.ftc.gov/news-events/news/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices-address-consumer-privacy-security [https://perma.cc/PMX7-MGVP]; CONSUMER REPS. & ELEC. PRIV. INFO. CTR., HOW THE FTC CAN MANDATE DATA MINIMIZATION THROUGH A SECTION 5 UNFAIRNESS RULEMAKING 8–16 (2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf [https://perma.cc/Y3HP-XAHR]; *see also* Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 356, 365–66 (2022) (arguing for laws strengthening privacy protections).

242. *E.g.*, GDPR, *supra* note 239, art. 25, at 48; CAL. CIV. CODE § 1798.140(h) ("[A]greement obtained through use of dark patterns does not constitute consent."); *see also* ANN CAVOUKIAN, THE 7 FOUNDATIONAL PRINCIPLES 5 (2020), https://privacy.ucsc.edu/resources/privacy-by-design—foundational-principles.pdf [https://perma.cc/JN6N-H22K] (listing data minimization and respect for user privacy, including "the quality of the consent" as aspects of privacy by design). Much scholarship exists evaluating the value of such restrictions. Lisa M. Austin & David Lie, *Safe Sharing Sites*, 94. N.Y.U. L. REV. 581, 589–90 (2019) (contending that the FTC's notice-and-choice regime fails to fully incorporate Fair Information Practice ("FIP") principles and noting that the GDPR goes beyond the notice-and-choice regime); Kevin E. Davis & Florencia Marotta-Wurgler, *Contracting for Personal Data*, 94. N.Y.U. L. REV. 662, 667 (2019) (contrasting the GDPR framework with

have also incorporated data minimization principles. The CPA imposes on controllers[243] a clear duty of minimization, a duty of care, and a duty to avoid secondary uses.[244] Both the VCDPA and the CDPA also impose data minimization obligations.[245]

The Mozilla Foundation study notes that a large number of studied car bands had "signed on to a list of Consumer Protection Principles from [a] US automotive industry group," which "includes great privacy-preserving principles such as 'data minimization' 'transparency,' and 'choice.'"[246] Despite the imposition of data minimization principles in state law and promises to adhere to similar industry principles, the report found that none of the studied twenty-five brands adhered to these principles.[247]

---

the FTC's approach to privacy and security, and describing the GDPR as providing a regulatory framework that imposes "financial consequences for failure to comply" in contrast to the FTC's "Notice and Choice" approach, "which relies mostly on self-regulation"). *But see* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 955–56 (2017) (discussing the inadequacy of FIPs); Charlotte A. Tschider, *Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age*, 96 DENV. L. REV. 87, 132 (2018) (noting that "GDPR has not evolved traditional notions of notice and consent"); Anders van Marter, *Privacy by Design Opportunity or Roadblock*, NIXON PEABODY (Mar. 3, 2021), https://www.nixonpeabody.com/insights/articles/2021/03/03/privacy-by-design-opportunity-or-roadblock [https://perma.cc/99QF-TKS3] ("While neither the CCPA nor the CPRA, which does not go into effect until January 1, 2023, explicitly require privacy by design, like in the GDPR, they do indicate that perhaps the U.S. is heading in that direction, and businesses should take note.").

243. COLO. REV. STAT. § 6-1-1303(7) (2023) (defining controller as "a person that, alone or jointly with others, determines the purposes for and means of processing personal data."). Notably, the CPA

> applies to any organization that controls or processes personal data regarding 100,000 Colorado consumers or "derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes the personal data of [25,000] consumers or more." Individuals "acting in a commercial or employment context" are excluded from the definition of "consumers."

ANDREAS KALTSOUNIS, SHEA LEITCH & STANTON BURKE, BAKERHOSTETLER, COLORADO'S PRIVACY ACT: A CURVE BALL ON CONSENT AND TARGETED ADS 2 (2021), https://www.jdsupra.com/post/fileServer.aspx?fName=051badb7-3c1f-4345-84eb-6e736bbof7cb.pdf [https://perma.cc/B7UC-EZ8R]. However, unlike "the CCPA and the CDPA, the [CPA] does not exempt nonprofit entities." *Id. See generally* Brooke Penrose, Burns & Levinson LLP, *State of US State Comprehensive Privacy Laws*, JDSUPRA (July 7, 2021), https://www.jdsupra.com/legalnews/state-of-us-state-comprehensive-privacy-6035278 [https://perma.cc/8LUJ-XR2X] (comparing the privacy regimes of California, Colorado, and Virginia).

244. The duty of minimizations means that a "controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed." COLO. REV. STAT. § 6-1-1308(3) (2023). The duty "to avoid secondary use" means that a "controller shall not process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes for which the personal data are processed, unless the controller first obtains the consumer's consent." *Id.* § 6-1-1308(4). The duty of care means that a "controller shall take reasonable measures to secure personal data during both storage and use from unauthorized acquisition. The data security practices must be appropriate to the volume, scope, and nature of the personal data processed and the nature of the business." *Id.* § 6-1-1308(5).

245. *Compare* VA. CODE ANN. § 59.1-578(A) (Supp. 2024), *with* CONN. GEN. STAT. § 42-520(a) (2023 & Supp. 2024).

246. Caltrider et al., *supra* note 87.

247. *Id.*

State privacy laws also require that companies inform consumers of their practices, a core feature of the notice-and-choice model.[248] In the Mozilla Foundation report, privacy researchers spent more than six-hundred hours attempting to review and understand the privacy practices of connected vehicle manufacturers, and yet they found that none of the manufacturers' privacy policies provided "a full picture of how [drivers'] data is used and shared."[249] Indeed, "[i]f three privacy researchers can barely get to the bottom of what's going on with cars, how does the average time-pressed person stand a chance?"[250]

On the issue of choice, vehicle manufacturers may assume that drivers have read their privacy policies and consent to the same simply by entering a vehicle. The same may even apply to a nonowner passenger.[251] Some vehicle manufacturers may also place the onus on drivers and vehicle owners to obtain the consent of passengers to their data practices.[252]

With respect to cybersecurity, the CCPA requires businesses to adopt "reasonable security procedures and practices."[253] The CPPA has published draft regulations on covered entities' cybersecurity audits and obligations.[254] Other pre-existing sources of state law also impose a reasonable cybersecurity standard, with states providing additional guidance on compliance with this standard via narrative reports and subsequent regulation.[255]

The 2020 amendments to the CCPA also include additional protections for "sensitive personal information," a type of personal information that may include precise geolocation data, genetic data, health data, and biometric information used to establish a person's identity, among other things.[256] Recall that connected vehicles associated with VMC features can collect health data and precise geolocation data.[257] Connected vehicles may also collect other types of data that may qualify as sensitive personal information under state law. If the data that a company collects qualifies as sensitive personal information and is "collected or processed [for] the purpose of inferring characteristics," consumers have the right to direct the firm to limit its use of the data to that which is necessary to perform requested services and to those

248. *See, e.g.*, CAL. CIV. CODE § 1798.100 (West 2022); COLO. REV. STAT. 6-1-1308.

249. Caltrider et al., *supra* note 87.

250. *Id.*

251. *Id.*

252. *Id.*

253. CAL. CIV. CODE § 1798.100(e).

254. *Id.* § 1798.185(a)(15); CAL. PRIV. PROT. AGENCY, DRAFT CYBERSECURITY AUDIT REGULATIONS FOR CALIFORNIA PRIVACY PROTECTION AGENCY SEPTEMBER 8, 2023 BOARD MEETING 4 (2023), https://cppa.ca.gov/meetings/materials/20230908item8.pdf [https://perma.cc/4KQF-48D6].

255. William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1153–58 (2019).

256. CAL. CIV. CODE § 1798.140(ae) (defining "sensitive personal information").

257. Fowler, *supra* note 56.

other purposes authorized in any related regulations and the statute.[258] As with other privacy rights, these additional protections for sensitive data may also limit companies' ability to monetize these types of data to the extent that drivers exercise their CCPA rights. However, under this approach, drivers continue to bear a significant burden with respect to protecting sensitive personal information.[259] Social science research indicates that there are

258. CAL. CIV. CODE § 1798.121(d) (describing sensitive personal information that is excluded from the definition); *id.* § 1798.121(a) ("A consumer shall have the right, at any time, to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services."); Eddie Holman, Tracy Shapiro & Khoury Trombetta, Wilson Sonsini Goodrich & Rosati, *New California Privacy Rights Act to Effectively Replace the California Consumer Privacy Act*, JDSUPRA (Nov. 13, 2020), https://www.jdsupra.com/legalnews/new-california-privacy-rights-act-to-45378 [https://perma.cc/CNE6-WHQF] ("Consumers can request that businesses limit their use and disclosure of the consumer's sensitive PI for any purpose other than providing requested goods or services or for other specific business purposes enumerated in the CPRA. Businesses that use or disclose sensitive PI for any other purpose must provide a clear and conspicuous 'Limit the Use of My Sensitive Personal Information' website link. It is worth noting, however, that this opt-out right does not apply if the business collects or processes sensitive personal information 'without the purpose of inferring characteristics about a consumer.'"); Katelyn Ringrose, *New Categories, New Rights: The CPRA's Opt-Out Provision for Sensitive Data*, IAAP (Feb. 8, 2021), https://iapp.org/news/a/new-categories-new-rights-the-cpras-opt-out-provision-for-sensitive-data [https://perma.cc/H9BY-NBVW] (noting that although the "CPRA establishes a range of new protections, including and perhaps most importantly, the right for consumers to limit the use and disclosure of their sensitive personal information," the CPRA "may not go far enough to protect consumers" because this right to limit use is "structured as an opt-out"); David Stauss & Mike Summers, *How Do the CPRA, CPA & VCDPA Treat Sensitive Personal Information?*, HUSCH BLACKWELL (Feb. 16, 2022), https://www.bytebacklaw.com/2022/02/how-do-the-cpra-cpa-and-vcdpa-treat-sensitive-personal-information [https://perma.cc/AH5R-KWW7] ("Where a business collects or processes sensitive personal information for the purpose of inferring characteristics about a consumer, it will either need to self-restrict its use of that information to certain purposes set forth in the CPRA or, if it goes beyond those purposes, it will need to provide consumers with a notice and the right to limit the business's use of the information to the statutory purposes. The CPPA is charged with issuing regulations to ensure that this exception only 'applies to information that is collected or processed incidentally, or without the purpose of inferring characteristics about a consumer' and to ensure that 'businesses do not use the exemption for the purpose of evading consumers' rights to limit the use and disclosure of their sensitive personal information.'"). At least one practitioner suggests that the CCPA "has the most expansive definition for sensitive data" in comparison to the four other state comprehension privacy statutes and notes that unlike the CCPA, the CPA, the CDPA, the UCPA, and the VCDPA exclude "information about an individual's sex life" from the definition of sensitive personal information. Amy Olivero, *Privacy and Digital Health Data: The Femtech Challenge*, IAPP (Oct. 25, 2022), https://iapp.org/news/a/privacy-and-digital-health-data-the-femtech-challenge [https://perma.cc/2NAN-2LNA]. Others similarly observe that "consumers will have a limited right to object to a business's continued use of sensitive personal information," although they acknowledge that the statute does not require that a "business obtain opt-in consent from a consumer before collecting or utilizing their sensitive personal information." David A. Zetoony, *Does the CPRA Require That Companies Get Opt-In Consent from Consumers Before Collecting Their Sensitive Personal Information?*, GREENBERGTRAURIG (Nov. 10, 2020), https://www.gtlaw-dataprivacydish.com/2020/11/does-the-cpra-require-that-companies-get-opt-in-consent-from-consumers-before-collecting-their-sensitive-personal-information [https://perma.cc/L86E-W9W8].

259. *HANDLING SENSITIVE PERSONAL INFORMATION UNDER THE CPRA AND THE VCDPA*, CLARITY PRIV. (2024), https://www.clarip.com/data-privacy/handling-sensitive-personal-information-un

cognitive problems with consent in the privacy context and structural problems can occur even when individuals are "well-informed and rational."[260]

In summary, these state privacy statutes appear to rely significantly on consumers effectively exercising statutorily granted privacy rights. These rights have some value in that they could limit various types of secondary data uses and monetization, such as the sale of vehicular data, if drivers consistently and effectively exercise these rights.[261] This approach places a significant amount of responsibility on drivers to effectively enforce their privacy rights. Companies have grown particularly effective at encouraging consumers to provide consent to their data practices. In some cases, companies can obtain consent by conditioning access to their services and products on the provision of such consent.[262] Evidence regarding the effectiveness of the CCPA's early reliance on consumers' exercise of their CCPA rights indicates that "it's almost impossible to tell how many Californians are taking advantage of their new rights, or precisely how the biggest players are complying."[263]

The incorporation of data minimization principles is a laudable step in moving beyond an overreliance on notice-and-choice and a rights-based approach. However, the effectiveness of data minimization and other limitations on data collection and uses may also depend on the frequency and extent of enforcement of these obligations and whether subsequent guidance emerges to shed light on compliance with these standards in different contexts. Early research in this area in the vehicular context suggests a lack conformity with data minimization principles.[264]

Of the five state statutes evaluated in this Article, only the CCPA grants a limited private right of action.[265] The lack of a private right of action in some

---

der-the-cpra-and-the-vcdpa [https://perma.cc/3YFR-RTMF] (comparing the CCPA to the GDPR and noting that, pursuant to the GDPR, "the processing of special categories is prohibited by default and the burden is on controllers to show that processing is permitted by virtue of one of the enumerated exceptions, including express consent. In contrast, under the CPRA, the burden falls on the consumers to limit processing to certain activities").

260. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1881 (2013).

261. *See* David A. Zetoony, *How Do State Statutes Differ in Terms of Their "Targeted Advertising" Exemptions?*, NAT'L L. REV. (May 31, 2022), https://www.natlawreview.com/article/how-do-state-statutes-differ-terms-their-targeted-advertising-exemptions [https://perma.cc/SJ73-YVAJ] (comparing different laws on this point, each with their own implications).

262. Solove, *supra* note 260, at 1898–99.

263. Susannah Luthi, *'Functionally Useless': California Privacy Law's Big Reveal Falls Short*, POLITICO (Aug. 6, 2021, 4:07 PM), https://www.politico.com/states/california/story/2021/08/05/functionally-useless-california-privacy-laws-big-reveal-falls-short-1389429 [https://perma.cc/TQM2-MTYB]; *see also CCPA Disclosure Metrics: FAANGM (aka Big Tech) Edition*, DATAGRAIL (July 15, 2021), https://www.datagrail.io/blog/privacy-trends/ccpa-metrics-faangm [https://perma.cc/SU48-RURH] (analyzing early reports following passage of the CCPA).

264. Caltrider et al., supra note 87.

265. Taylor Kay Lively, *Connecticut Enacts Comprehensive Consumer Data Privacy Law*, IAPP (May 11, 2022), https://iapp.org/news/a/connecticut-enacts-comprehensive-consumer-data-privacy-law [https://perma.cc/A9GE-FZ2V] ("Like Virginia, Colorado and Utah, the [Connecticut] law lacks a private right of action, and, following Virginia's approach, enforcement falls solely to the

statutes and provisions limiting enforcement exclusively or primarily to state attorney generals or an agency may impact the frequency and extent of enforcement under these statutes. Limits on the time and resources of entities tasked with enforcement can also negatively impact the effectiveness of these statutes in protecting consumers' interests. Additionally, as Professor Lauren Henry Scholz has argued, private rights of action in the privacy context "create accountability through discovery, and have expressive value in creating privacy-protective norms."[266] Indeed, privacy could be viewed, in part, as a dignitary right and the capacity to bring a cause of action when there is a violation of this right recognizes the dignity of the individual plaintiff.[267]

Admittedly, even when state statutes contain a private right of action, additional legal requirements may negatively impact the viability of consumer lawsuits. For instance, in *Dornay v. Volkswagen Group of America, Inc.*, the plaintiffs alleged that various automakers collected information, such as text messages, from their cellphones that were connected to their vehicles without their consent, in violation of Washington's Privacy Act ("WPA").[268] The Ninth Circuit affirmed the dismissal of the plaintiffs' claim and reasoned that the plaintiffs had failed to show that the data collection caused injuries to their persons, businesses, or reputations as required by the WPA.[269] Despite this, private rights of action can facilitate accountability and legal compliance.

Lastly, large technology companies have also played a significant role in the adoption of state comprehensive privacy laws, which have significantly weakened statutory safeguards for consumers.[270] The EPIC report discussed earlier, which evaluated various comprehensive privacy laws, found that, of the fourteen laws studied, "all but California's closely follow a model that was initially drafted by industry giants such as Amazon."[271] Thus, it is not

---

attorney general."); *see also* FITZGERALD ET AL., *supra* note 113, at 18 (evaluating fourteen state comprehensive privacy laws and noting that only the CCPA has a private right of action).

266. Lauren Henry Scholz, *Private Rights of Action in Privacy Law*, 63 WM. & MARY L. REV. 1639, 1639 (2022).

267. *Id.* at 1645 ("Privacy is a personal, dignitary right, so there should be some avenue for an individual to personally contest privacy violations. The ability to bring a claim is itself a recognition of the dignity of the plaintiff.").

268. Dornay v. Volkswagen Grp. of Am., Inc., No. 22-35451, 2023 WL 7318487, at *1 (9th Cir. Nov. 7, 2023), *aff'g* Jones v. Ford Motor Co., 85 F.4th 570 (9th Cir. 2023).

269. *Id.*

270. FITZGERALD ET AL., *supra* note 113, at 4.

271. *Id.* In recent years, Amazon "has killed or undermined privacy protections in more than three dozen bills across [twenty-five] states." Jeffrey Dastin, Chris Kirkham & Aditya Kalra, *Amazon Wages Secret War on Americans' Privacy, Documents Show*, REUTERS (Nov. 19, 2021, 11:00 AM), https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying [https://perma.cc/KAC4-4EXC]. In Virginia, for instance, Amazon "boosted political donations tenfold over four years before persuading lawmakers this year to pass an industry-friendly privacy bill that Amazon itself drafted." *Id.* In Washington, according to state legislators, "Microsoft played a significant role in drafting the original bill. Corporate interests, including those of Amazon and Comcast, a cable provider, also have successfully inserted carve-outs for much of their existing data collection practices which make the current proposals almost meaningless." Mark Scott, *How Lobbyists Rewrote Washington State's Privacy Law*, POLITICO EUR. (Apr. 26, 2019, 7:00 AM), https:/

surprising that more recently adopted state comprehensive privacy statutes provide less protection for consumers. The EPIC study went on to find that many state comprehensive privacy laws do not sufficiently guard against disparate discriminatory impacts online.[272] As such, some privacy laws may not effectively and consistently address the discriminatory concerns discussed in Part I.

D. FEDERAL REGIMES

Financing transactions, including subprime vehicle lending arrangements, between consumers and creditors can be subject to various sources of federal law. With respect to potentially applicable federal law, the Fair Credit Reporting Act imposes significant limitations on covered entities and aims to increase transparency in the credit reporting process, which plays an important role in lending transactions.[273]

The Equal Credit Opportunity Act ("ECOA") prohibits discrimination in credit transactions based on certain protected characteristics.[274] The ECOA may be helpful in addressing discrimination concerns discussed in Part I of this Article. However, several scholars have noted that ECOA claims are particularly difficult to prove and win.[275] Professor Nicole McConlogue contends that the ECOA "does not go so far as to expressly cover other proxies for protected or vulnerable classes."[276] Correlative attributes identified through analytics using data derived from VMC technology and connected vehicles could serve as a proxy for protected characteristics. In 2020, the FTC pursued its first ECOA action since the adoption of the Dodd–Frank Wall Street

/www.politico.eu/article/how-lobbyists-rewrote-washington-state-privacy-law-microsoft-amazon-regulation [https://perma.cc/3EQ5-7PZZ].

272. FITZGERALD ET AL., *supra* note 113, at 19.

273. For a description of the purpose of ECOA, see 15 U.S.C. § 1691 note. *See also id.* § 1681(a) (Fair Credit Reporting Act ("FCRA") findings and purpose); *id.* § 1681a(d)(1) (defining "consumer report" as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living"). For permissible uses of consumer reports, see *id.* § 1681b(a). As Professors Solove and Schwartz note, the FCRA "applies to 'any consumer reporting agency' that furnishes a 'consumer report.'" DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 154 (2015) (quoting 15 U.S.C. § 1681b); *see also* Press Release, Fed. Trade Comm'n, FTC Approves Changes to Five FCRA Rules (Sept. 8, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-approves-changes-five-fcra-rules [https://perma.cc/HZ2E-8ZKC] (discussing motor vehicle dealers and the FCRA).

274. 15 U.S.C. § 1691(a).

275. *See, e.g.*, McConlogue, *supra* note 159, at 318–19 (noting claims are difficult to bring, in part, because "lenders are unlikely to broadcast that they are discriminating" on the basis of, say, race or gender); Winnie Taylor, *Proving Racial Discrimination and Monitoring Fair Lending Compliance: The Missing Data Problem in Nonmortgage Credit*, 31 REV. BANKING & FIN. L. 199, 201 (2011) (discussing the ECOA and how the lack of race data sources makes it difficult to bring claims).

276. McConlogue, *supra* note 159, at 319 (but noting that "while the ECOA specifically prohibits lenders from relying on applicants' sources of income it derives from public assistance programs, that is the only proxy it affirmatively singles out for prohibition based on its disparate impact").

Reform and Consumer Protection Act ("DFA") against an automobile dealership for discriminatory dealer markups, among other things.[277]

The GLBA can also govern data in consumer financing transactions.[278] GLBA regulations may also apply to motor vehicle dealers, including the FTC's Privacy Rule.[279] The Privacy Rule governs covered entities' disclosure of "nonpublic personal information," but does not include information that a covered entity has "a reasonable basis to believe is lawfully made 'publicly available.'"[280] The FTC has indicated that it may revise its Privacy Rule to clarify the scope of its application.[281]

---

277. Press Release, Fed. Trade Comm'n, Auto Dealership Bronx Honda, General Manager to Pay $1.5 Million to Settle FTC Charges They Discriminated Against African-American, Hispanic Car Buyers (May 27, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/05/auto-dealership-bronx-honda-general-manager-pay-15-million-settle-ftc-charges-they-discriminated [https://perma.cc/8WKG-TL9A]; *see also* Statement of Commissioner Slaughter, *supra* note 107, at 3 ("This enforcement action against Bronx Honda is the Commission's first ECOA action since the passage of the Dodd-Frank Act.").

278. 15 U.S.C. § 6801; CFPB Privacy of Consumer Financial Information (Regulation P) Rule, 12 C.F.R. pt. 1016 (2024); FTC Privacy of Consumer Financial Information Rule, 16 C.F.R. pt. 313 (2024); FTC Standards for Safeguarding Customer Information Rule, 16 C.F.R. pt. 314 (2024); FED. TRADE COMM'N, HOW TO COMPLY WITH THE PRIVACY OF CONSUMER FINANCIAL INFORMATION RULE OF THE GRAMM-LEACH-BLILEY ACT 1, 5 (2002) [hereinafter FTC GUIDANCE ON GLB ACT], https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf [https://perma.cc/A2NY-PZP2] ("The Gramm-Leach-Bliley Act required the Federal Trade Commission (FTC) . . . . to implement regulations to carry out the Act's financial privacy provisions (GLB Act). . . . The FTC is responsible for enforcing its Privacy of Consumer Financial Information Rule (Privacy Rule).").

279. 16 C.F.R. pt. 313; *see* FED. TRADE COMM'N, THE FTC'S PRIVACY RULE AND AUTO DEALERS: FREQUENTLY ASKED QUESTIONS 1 (2005), https://www.ftc.gov/system/files/documents/plain-language/bus64-ftcs-privacy-rule-and-auto-dealers-faqs.pdf [https://perma.cc/4M9M-QYEF] (discussing the GLBA and noting that "[t]he [FTC's] Privacy Rule applies to car dealers who: extend credit to someone (for example, through a retail installment contract) in connection with the purchase of a car for personal, family, or household use; arrange for someone to finance or lease a car for personal, family, or household use; or provide financial advice or counseling to individuals. If you engage in these activities, any personal information that you collect to provide these services is covered by the Privacy Rule."); *see also* Privacy of Consumer Financial Information Rule Under the Gramm-Leach-Bliley Act, 84 Fed. Reg. 13150, 13151, 13151 n.7 (proposed Apr. 4, 2019) (to be codified at 16 C.F.R. pt. 313) (noting that "under section 1029 of the Dodd-Frank Act, the Commission retained rulemaking authority for certain motor vehicle dealers" and that the "FTC retained rulemaking jurisdiction as to motor vehicle dealers that are predominantly engaged in the sale and servicing or the leasing and servicing of motor vehicles, excluding those dealers that directly extend credit to consumers and do not routinely assign the extensions of credit to an unaffiliated third party").

280. FTC GUIDANCE ON GLB ACT, *supra* note 278, at 5.

281. Press Release, Fed. Trade Comm'n, FTC Seeks Comment on Proposed Amendments to Safeguards and Privacy Rules (Mar. 5, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/03/ftc-seeks-comment-proposed-amendments-safeguards-privacy-rules [https://perma.cc/5FNK-EL6Y] ("The Dodd-Frank Act transferred the majority of the Commission's rulemaking authority for the Privacy Rule to the Consumer Financial Protection Bureau, leaving the FTC with rulemaking authority only over certain motor vehicle dealers."); 12 U.S.C. § 5519; Michael A. Mancusi, Raqiyyah Pippins, Anthony Raglani & George Eichelberger, *FTC Publishes Final CARS Rule Targeting Unfair and Deceptive Auto Sales Practices*, ARNOLD & PORTER (Dec. 20, 2023), https://www.arnoldporter.com/en/perspectives/advisories/2023/12/ftc-publishes-fina

It is possible that the GLBA framework could apply to covered entities' use of data collected by VMC technology in consumer financing transactions. Professors Daniel Solove and Paul Schwartz have observed that, under the GLBA, covered financial institutions may disclose covered personal information about consumers with nonaffiliated entities "only if they first provide individuals with the ability to opt out of the disclosure."[282] The GLBA framework also imposes certain reuse and redisclosure data restrictions, but relies on a notice-and-choice approach, which has important shortcomings as discussed earlier.[283]

With respect to cybersecurity, the FTC updated the GLBA's Safeguards Rule in 2021 to impose more detailed data security requirements on covered entities, such as motor vehicle dealers and financial institutions, including decreasing access to consumer data and encryption obligations.[284] More recently, in 2023, the FTC amended its Safeguards Rule to "require non-

---

l-cars-rule [https://perma.cc/A3K6-D58U] ("[T]he Dodd-Frank Act reserved regulatory authority over consumer protection matters related to traditional auto dealers to the FTC."). In accordance with the DFA, the CFPB issued its own GLBA regulation. The CFPB's Regulation P recodified the FTC's implementing regulation, among other things, and governs certain nonpublic personal information. 12 C.F.R. pt. 1016; *Privacy of Consumer Financial Information (Regulation P)*, NAT'L CREDIT UNION ADMIN. (Oct. 5, 2022), https://www.ncua.gov/regulation-supervision/manuals-guides/federal-consumer-financial-protection-guide/compliance-management/deposit-regulations/privacy-consumer-financial-information-regulation-p [https://perma.cc/TK2Z-A8LF].

282. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, CONSUMER PRIVACY AND DATA PROTECTION 125–28 (Aspen Publ'g 2021); *see also* 15 U.S.C. § 6802(b) (imposing the opt-out rule and an exception); CONSUMER FIN. PROT. BUREAU, CFPB LAWS AND REGULATIONS: GLBA PRIVACY 5 (2016), https://files.consumerfinance.gov/f/documents/102016_cfpb_GLBAExamManualUpdate.pdf [https://perma.cc/EW58-XT3S] ("Consumers must be given the right to 'opt out' of, or prevent, a financial institution from disclosing nonpublic personal information about them to a nonaffiliated third party unless an exception to that right applies. The exceptions are detailed in Sections 13, 14, and 15 of the regulation.").

283. 12 C.F.R. pt. 1016; FTC GUIDANCE ON GLB ACT, *supra* note 278, at 4; *supra* Section II.B; Letter from Caitriona Fitzgerald, Deputy Dir., Elec. Priv. Info. Ctr., to Patrick McHenry & Maxine Waters, Chair & Ranking Member, House Comm. on Fin. Servs. 1 (Feb. 27, 2023), https://epic.org/documents/epic-statement-re-data-privacy-act-of-2023 [https://perma.cc/C9QH-LG62] ("GLBA requires financial institutions to provide their customers with privacy notices. This notice-and-choice regime, in which consumers are expected to read extensive privacy policies, makes it impossible for consumers to meaningfully protect their privacy."); Jay P. Kesan, Carol M. Hayes & Masooda N. Bashir, *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*, 91 IND. L.J. 267, 278 (2016) ("The GLBA, for instance, represents the current failing paradigm of 'notice and choice' in that it permits financial institutions to share their customers' nonpublic personal information with the institutions' affiliates but the customers must first be told and have the ability to opt out of such sharing. The GLBA also requires financial entities to provide customers with annual privacy notices." (footnote omitted)).

284. Press Release, Fed. Trade Comm'n, FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches (Oct. 27, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data [https://perma.cc/UY73-9R2F]; Allison Grande, *FTC Updates Financial Data Security Rule Over GOP Rebuke*, LAW360 (Oct. 27, 2021, 10:30 PM), https://www.law360.com/technology/articles/1435266 (on file with the *Iowa Law Review*).

banking financial institutions within the FTC's jurisdiction to report data breaches affecting [five hundred] or more people."[285]

We turn now to the FTC's 2023 CARS Rule, which represents an important step towards further curtailing unfair and deceptive trade practices in automobile transactions. The CARS Rule was adopted in accordance with the DFA's grant of rulemaking power over vehicle dealers to the FTC.[286] It imposes on covered entities several prohibitions, such as charging drivers for add-ons[287] "that [do not] provide a [direct] benefit" to drivers.[288] If the CARS Rule survives the ongoing legal challenge to its validity,[289] this restriction could potentially apply to VMC technology add-ons.

The rule also prohibits dealers from making material misrepresentations, whether "expressly or by implication," in connection with a vehicular transaction about several different types of information including the "costs or terms of purchasing, financing, or leasing a Vehicle," "[a]ny costs, limitation, benefit, or any other aspect of an Add-on Product or Service," "[a]ny information on or about a consumer's application for financing," "[w]hether, or under what

285. Lesley Fair, *FTC Announces New Safeguards Rule Provision: Is Your Company Up on What's Required?*, FED. TRADE COMM'N (Oct. 27, 2023), https://www.ftc.gov/business-guidance/blog/2023/10/ftc-announces-new-safeguards-rule-provision-your-company-whats-required [https://perma.cc/44SZ-SP2R]; *FTC Amends Safeguards Rule to Require Non-Banking Financial Institutions to Report Data Security Breaches*, FED. TRADE COMM'N (Oct. 27, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-amends-safeguards-rule-require-non-banking-financial-institutions-report-data-security-breaches [https://perma.cc/5KYG-48AC] ("The FTC's Safeguards Rule requires non-banking financial institutions, such as mortgage brokers, motor vehicle dealers, and payday lenders, to develop, implement, and maintain a comprehensive security program to keep their customers' information safe.").

286. Combating Auto Retail Scams Trade Regulation Rule, 89 Fed. Reg. 590, 590 (proposed Jan. 4, 2024) (to be codified at 16 C.F.R. pt. 463); *FTC CARS Rule: Combating Auto Retail Scams – A Dealers Guide*, FED. TRADE COMM'N (Jan. 24, 2024) [hereinafter *Dealers Guide*], https://www.ftc.gov/business-guidance/resources/ftc-cars-rule-combating-auto-retail-scams-dealers-guide [https://perma.cc/L933-4YLV] ("What is the FTC's legal authority for enacting the CARS Rule? The Dodd-Frank Act gives the FTC authority to make rules about unfair or deceptive dealer practices."). Notably, since the FTC can "issue consumer protection regulations governing auto dealers using an expedited process," the industry is "a likely target for action." Daniel S. Savrin et al., *FTC's Final 'CARS Rule' on Dealer Sales Practices: Implications for Banks, Auto Finance, and 'Captives,'* MORGAN LEWIS (Jan. 18, 2024), https://www.morganlewis.com/pubs/2023/12/ftcs-final-cars-rule-on-dealer-sales-practices-implications-for-banks-auto-finance-and-captives [https://perma.cc/DS54-CS26]. With respect to dealer markups, legal practitioners in this area have suggested that the FTC CARS Rule does not provide adequate guidance on dealer markups. *Id.* ("While a substantial part of the preamble to the CARS Rule proposal explained the role of markup in automotive finance, nothing in the rule would require additional disclosures or limits on dealer markups.").

287. Combating Auto Retail Scams Trade Regulation Rule, 89 Fed. Reg. at 693 (to be codified at 16 C.F.R. § 463.2(a)) (defining add-ons as "any product(s) or service(s) not provided to the consumer or installed on the Vehicle by the Vehicle manufacturer and for which the Dealer, directly or indirectly, charges a consumer in connection with a Vehicle sale, lease, or financing transaction").

288. *Dealers Guide*, *supra* note 286; *see* Combating Auto Retail Scams Trade Regulation Rule, 89 Fed. Reg. at 694 (to be codified at 16 C.F.R. § 463.3).

289. *See generally* Petitioners' Opening Brief, *supra* note 161 (challenging the rule); *see also* Savrin et al., *supra* note 286 (discussing the legal challenge to the rule).

circumstances a Vehicle may be moved across State lines or out of the country," among other things.[290]

To the extent that the material misrepresentations prohibition applies (such as the limitation on misrepresentations regarding the terms of financing or buying an automobile), it could also help ensure that covered dealers avoid making inaccurate statements and promises to drivers regarding subscription services associated with vehicle financing and purchases, and the collection and use of vehicular data obtained via VMC technology and features or connected vehicles that are disclosed as part of the terms of the transaction. Violations of the CARS Rule could lead to "civil penalties of as much as $50,120 per violation," among other things.[291]

The material misrepresentation prohibition also limits dealers' ability to make misrepresentations about "whether, or under what circumstances, a vehicle may be repossessed."[292] This restriction may help in addressing instances in which vehicle dealers make material misrepresentations about their ability to repossess vehicles or use VMC technology to aid in such repossessions. It may cover geofencing features and remote disablement of a vehicle if doing so constitutes repossession. This limitation may require companies to more accurately describe and follow their self-described repossession practices.

Although consumer advocates raised concerns during the rulemaking process about the use of VMC technology with remote disablement capabilities, the FTC chose not to specifically address this issue in detail in its finalized rules.[293] During the rulemaking process, several consumer advocates made recommendations on this issue, including "limit[ing] its use to one time, not to exceed [thirty] days, once a consumer is in default."[294] In response, the FTC noted that it was "already illegal under Section 5 of the FTC Act to engage in deception, including regarding vehicle disablement technology, and to unfairly cause substantial injury to consumers, such as by disabling a vehicle while it is being operated on the highway."[295] It appears that the FTC opted not to include additional rules that specifically address VMC technology in detail as it believed that existing prohibitions under the FTCA, combined with provisions from the CARS Rule limiting misrepresentations in the repossession process, would adequately address the issue.[296] The FTC's failure

290. Combating Auto Retail Scams Trade Regulation Rule, 89 Fed. Reg. at 694 (to be codified at 16 C.F.R. § 463.3(a), (b), (g), (n)).

291. *Dealers Guide*, *supra* note 286.

292. Combating Auto Retail Scams Trade Regulation Rule, 89 Fed. Reg. at 624 (to be codified at 16 C.F.R. § 463.3(o)).

293. *Id.* ("A number of commenters, including consumer advocacy organizations and a group of State attorneys general, expressed concern about electronic disablement of vehicles, including through the use of starter interrupt devices, which are sometimes utilized for vehicle repossession.").

294. *Id.*

295. *Id.*

296. *Id.* (discussing the repossession limitation and stating "[t]his provision will further provide protection for consumers from unfair or deceptive conduct surrounding the repossession of vehicles" and that "[m]oving forward, the Commission will continue to monitor the motor vehicle marketplace for developments in this area to determine whether additional restrictions are warranted").

to more directly address the VMC technology issue represents a missed opportunity to provide clear federal guidance to automobile dealers on the use of such technology.

III. PATH FORWARD

Given the limitations of existing legal frameworks discussed in Part II in remedying the concerns associated with VMC technology and VMC features associated with connected vehicles, discourse about potential solutions to reduce these gaps is necessary. This Part offers four potential solutions to consider with the goal of alleviating the privacy, cybersecurity, and electronic subjugation concerns and inadequacies discussed in Part I. First, the UCC could undergo further revisions to more adequately address the use of VMC technology in secured lending consumer transactions. For instance, the UCC's drafters could more broadly define the term repossession, make the breach of the peace standard applicable to the use of VMC technology, and impose data use restrictions.

Second, more states could adopt laws directly addressing VMC technology or amend existing laws to impose additional restrictions on the use of VMC technology. Third, although state privacy laws may give drivers the ability to opt out of profiling, selling, or sharing of their data and other sources of state law may prohibit discrimination, these laws could incorporate more stringent nondiscrimination provisions. Undoubtedly, enforcement of existing requirements, such as data minimization requirements, is necessary.

Fourth, Congress could adopt comprehensive privacy legislation that addresses modern data practices, including the proliferation of vehicular data and impose specific duties and obligations on covered entities. Congress could also address the role and potential limits of consent in the privacy context. Congress, states, and regulatory bodies with existing authority over the automobile industry can provide clear guidance on the use of subscription-based models with VMC features in consumer connected vehicle transactions.

A. ARTICLE 9 AMENDMENTS

Although there are several possible alternative solutions to the VMC technology concerns discussed earlier, Article 9 plays an important role in secured lending transactions involving consumer vehicles. It is also a core source of commercial law that each state has adopted. As such, amendments to Article 9 sanctioned by the American Law Institute and the Uniform Law Commission—the entities responsible for approving uniform amendments the UCC—could offer a more viable route to enact rules in every state regulating the use of VMC technology in consumer lending transactions. Also, recall that some states have already adopted nonuniform amendments to their version of Article 9 to address VMC technology.

The term "consumer goods" in the UCC generally refers to goods "that are used or bought for use primarily for personal, family, or household

purposes."[297] Article 9 defines the term "consumer goods transactions" as transactions in which consumers take on "an obligation primarily for personal, family, or household purposes and a security interest in consumer goods secures the obligation."[298] Rather than prohibiting remote disablement in all consumer goods transactions, Article 9 could prohibit remote disablement solely in consumer transactions involving motor vehicles that qualify as consumer goods. The central role of vehicles in consumers' lives and the risks associated with remote disablement justifies limits on the use of this remedy when consumer vehicles are at issue. Other sources of commercial law restrict the use of this self-help remedy.[299]

Although somewhat paternalistic, this solution could address some of the electronic subjugation risks associated with remote disablement and avoid lifestyle and daily interruptions caused by remote disablement. However, simply banning the use of remote disablement in certain consumer transactions, without more, would not fully address the privacy, surveillance, and cybersecurity risks associated with VMC technology data collection. Consideration would need to be given to imposing limits on the possible collection and monetization of VMC technology data in consumer vehicle transactions.

An alternative, middle-of-the-road solution is to permit the continued use of remote disablement as a remedy for secured parties after default, but, at the same time, having Article 9 expressly indicate that the use of VMC technology to remotely disable a vehicle's features constitutes a constructive repossession. Article 9 could also make clear that the breach of the peace standard applies to VMC technology remote disablements in consumer transactions. Privacy has significant collective, public, and social value.[300] It plays a critical role in our democracy and the privacy choices of one individual can impact the privacy of others and potentially harm societal interests.[301] As such, courts might elect to consider the risks discussed in this Article when determining whether a party has breached the peace while using VMC

297. U.C.C. § 9-102(23) (AM. L. INST. & UNIF. L. COMM'N 2023).

298. *Id.* § 9-102(24).

299. *See, e.g.*, PRINCIPLES OF THE L. OF SOFTWARE CONTS. § 4.03 cmt. b, illus. 4 (AM. L. INST. 2024) (noting that "automated disablement is not available in a consumer agreement"); Robert A. Hillman & Maureen O'Rourke, *Defending Disclosure in Software Licensing*, 78 U. CHI. L. REV. 95, 111 n.84 (2011) (discussing how the Uniform Computer Information Transactions Act ("UCITA") offers "a limited right of electronic self-help"); Florencia Marotta-Wurgler & Robert Taylor, *Set in Stone? Change and Innovation in Consumer Standard-Form Contracts*, 88 N.Y.U. L. REV. 240, 255 n.46 (2013) (noting that the "drafters of ALI's *Principles of the Law of Software Contracts* have recommended that courts void remote-disablement terms"); Juliet M. Moringiello & William L. Reynold, *What's Software Got to Do with It? The ALI Principles of the Law of Software Contracts*, 84 TUL. L. REV. 1541, 1551 (2010) (noting that the final version of UCITA does not allow remote disablement). A few provisions of the UCITA bear noting to support this point. First, section 605(f) does "not authorize use of an automatic restraint to enforce remedies because of breach of contract or for cancellation for breach." UNIF. COMPUT. INFO. TRANSACTIONS ACT § 605(f) (UNIF. L. COMM'N 2002). Second, on "cancellation of a license" without a court order, "[e]lectronic self-help is prohibited" subject to some exceptions. *Id.* § 816(a)–(b).

300. REGAN, *supra* note 26, at 220–31.

301. *Id.*; Solove, *Murky Consent*, supra note 27, at 635.

technology in vehicle lending transactions. This is a topic that is ripe for future scholarship and development by courts.

One critique of this proposal is that in applying the breach of the peace standard courts have primarily focused on physical entry on to the consumer's premises and consent or objection to "entry and repossession."[302] Following that line of argument, privacy and electronic subjugation related concerns are well beyond the scope of this focus. One response to this critique is that the UCC's drafters "knowingly chose this well-worn phrase and did not try to define it."[303] This reflects a decision by the drafters to acknowledge both pre-code cases defining breach of the peace as well as future standards established by courts for determining application of the breach of the peace limitation. Indeed, the comments to section 9-609 state, "this section does not define or explain the conduct that will constitute a breach of the peace, leaving that matter for continuing development by the courts."[304]

To address concerns associated with the possible disclosure of VMC technology data to third parties, Article 9 could also explicitly impose data restrictions in transactions involving consumer vehicles. For instance, secured parties who possess data obtained from the use of VMC technology in secured lending consumer transactions involving vehicles could be prohibited from disclosing VMC technology data to third parties or entities other than the driver and repossession agents of the lender; similarly, they could be prohibited from using such data for purposes other than as necessary to locate a vehicle to conduct a physical repossession or to ensure continued functionality and safety of the VMC device.[305] They could also be prohibited from retaining such data after a legislatively determined period of time.[306] This approach may require additional amendments to Article 9 and other sources of law to ensure that there are no conflicts or interpretative issues with other provisions applicable to traditional physical repossessions.[307] First Amendment concerns, if any, would also need to be considered.

B. IMPROVING STATE VMC SPECIFIC LAWS

Absent amendments to Article 9, more states could also adopt laws that specifically address the use of VMC technology and existing state laws in this area could provide more adequate protection for consumers. To the extent that they do not already, state laws could restrict companies' ability to require consumers to accept the installation of VMC technology in their vehicles as a

302. WHITE & SUMMERS, *supra* note 174, § 26-7, at 1336.

303. *Id.* ("Accordingly, the numerous pre-code cases, and those under the 1962 and 1972 Codes, are still good law.").

304. U.C.C. § 9-609 cmt. 3 (AM. L. INST. & UNIF. L. COMM'N 2023).

305. *See, e.g.*, NEV. REV. STAT. § 598.9716(3)(c) (2023)(containing similar restrictions).

306. *See id.* § 598.9716(3)(d).

307. Such amendments may be appropriate in particular for the Uniform Commercial Code's section on the rights and duties of secured parties with possession or control of collateral. *See* U.C.C. § 9-207.

condition of loan approval. The use of such technology could be made permissible only in compliance with specific requirements.

To the extent that existing VMC technology state laws do not clearly impose data use and retention limits on VMC data in lending transactions, restrictions similar to those discussed in connection with the Article 9 amendments above could be adopted. State laws could also ensure that data restrictions apply to all types of data collected by VMC technology and not only location data.

State laws could expressly restrict companies' ability to collect data via VMC technology to the period after default. They could also limit the number of periodic location data collections or the types of data that lenders can collect using VMC technology post-default.[308] With respect to remote disablement, more state laws could also provide that, if installed in a consumer's vehicle, the VMC technology may only be activated for a single, uninterrupted period not exceeding a legislatively specified number of days after a default or until the consumer cures the default, whichever is earlier.[309]

To avoid the issue faced by the Georgia consumer discussed in the introduction of this Article, the lender, upon the consumers' satisfaction of the loan terms and balance, should have to pay costs associated with removing the VMC technology from the consumer's vehicle. Companies could also bear responsibility for any repair costs associated with damage to vehicles directly caused by the installation of VMC technology as part of the lending transaction.[310] Existing laws that regulate only certain types of VMC technology or certain types of entities could extend to cover other types of VMC technology and more entities that use such technology in consumer vehicle transactions.

C. ENHANCING STATE PRIVACY LAWS

Where applicable and appropriate, states could consider revising existing state comprehensive privacy laws to better address the electronic subjugation and privacy risks discussed in Part I. While existing state privacy laws that grant consumers a right to know, access or delete their data may help address some exclusion concerns, overreliance on a notice-and-choice approach and a rights-based approach to privacy has several shortcomings as discussed in earlier sections. The privacy choices that individual drivers may make, including a choice to exercise or refrain from exercising state granted privacy rights, can have broader implications for other individuals in their lives, including family members, children, and others.[311]

---

308. Legal Action Chicago Comment Letter, *supra* note 4, at 9.

309. *Id.* (proposing that the FTC adopt a rule such that for "each Motor Vehicle in which Disablement Technology is installed, Disablement Technology may only be activated for a single, continuous period not to exceed [thirty] calendar days following a default—or until the default is cured, whichever is earlier").

310. *See e.g.*, NEV. REV. STAT. § 598.9717 (2023) ("A consumer must not be required to pay . . . costs relating to the use of [a VMC] device.").

311. Solove, *supra* note 158, at 978 (noting that "[i]ndividuals make privacy choices that have effects not just for themselves but for many others").

Definitive obligations on companies regarding data collection, use, and monetization is needed. Existing data minimization limitations and cybersecurity obligations in state privacy laws are only the beginning steps in this direction. For existing restrictions and obligations to be meaningful, state regulatory actors and agencies must be willing to actively enforce these obligations particularly in the connected vehicle context.

More state comprehensive privacy laws should provide consumers with a private right of action. Although existing state privacy laws may afford drivers with the ability to opt out of profiling, or the sale or sharing of their data, and while other sources of state law may prohibit discrimination, as EPIC observes more state privacy statutes could also include stringent nondiscrimination provisions that limit covered entities from collecting, monetizing, or using connected vehicle data in ways that cause discrimination, or "otherwise make[] unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability."[312]

D. ADDITIONAL STATE AND FEDERAL GUIDANCE

In addition to the possible privacy issues VMC technology and features raise, the IoT, and various other technological developments also generate broader concerns about consumers' privacy and data security. Unlike other jurisdictions, the United States has historically adopted a sectoral approach to privacy protection in which distinct laws and regulatory bodies govern separate industries. This sectoral approach, often based on the notice-and-choice model and the data control narrative, has led to regulatory gaps. Recent state comprehensive privacy laws have attempted to fill some of these gaps, but even these laws have shortcomings.

Various scholars and government-related entities, such as the FTC, have long called for the adoption of some version of a comprehensive federal privacy statute.[313] The proliferation of connected vehicles and VMC technology

312. FITZGERALD ET AL., *supra* note 113, at 19 (noting that "[m]ost state privacy laws attempt to prevent discrimination online by prohibiting the processing of personal data in ways that violate state and federal anti-discrimination laws" but existing anti-discrimination laws are inadequate). Other legal experts have also argued that existing anti-discrimination laws are insufficient for the digital age as "[s]ome exclude retail or have unresolved questions as to whether they apply to online businesses. Others apply to specific sectors, like housing and employment, but may not cover new types of online services used to match individuals to these opportunities." *Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security: Hearing on H.R. 8152 Before the H. Comm. on Energy & Com.*, 117th Cong. 4 (2022) (statement of David Brody, Managing Attorney, Digital Justice Initiative). To this point, they observe that, under current federal law, it is permissible for online companies to "charge higher prices to women or to refuse to sell products to Christians" and "a service provider could use discriminatory algorithms to look for workers to target for recruitment so long as the provider does not meet the definition of an 'employment agency' under Title VII." *Id.*

313. Press Release, Fed. Trade Comm'n, FTC Recommends Congress Require the Data Broker Industry to Be More Transparent and Give Consumers Greater Control over Their Personal Information (May 27, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more-transparent-give-consumers-greater [https://perma.cc/JA4L-U4L6]. Other than the FTC, government-related entities that support

and features bolsters earlier calls for comprehensive federal privacy legislation. Any comprehensive federal legislation will need to contend effectively with existing state privacy laws and federal sectoral legislation, and the role that states can subsequently play in protecting consumer privacy if any such federal legislation is adopted.

While notice-and-choice as well as a rights-based approach are important aspects of any privacy regime, these approaches, without more, are unlikely to successfully protect consumers' privacy in the modern area. Thus, while federal privacy legislation can require companies to provide consumers with notice of their privacy practices and grant consumers rights to allow them to have control of their data, such as rights of access and deletion, federal legislation will also need to provide express guidance on permissible and impermissible data practices. Discriminatory practices enabled by data that work as proxies for traditionally protected categories is one such area that could be more adequately addressed.

To move beyond a rights-based and notice-and-choice approach, Congress could also evaluate recent calls for the imposition of various fiduciary duties on companies, such as a duty of loyalty, which may help in ensuring that corporations do not put corporate interests before consumer interests

a federal law include the Government Accountability Office. U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-52, INTERNET PRIVACY: ADDITIONAL FEDERAL AUTHORITY COULD ENHANCE CONSUMER PROTECTION AND PROVIDE FLEXIBILITY 31–34, 38 (2019), https://www.gao.gov/assets/d1952.pdf [https://perma.cc/9JLD-RNDT]. One nonprofit has also supported this proposal. *See generally* Future of Priv. F., Comment Letter on Developing the Administration's Approach to Consumer Privacy (Nov. 9, 2018), https://www.ntia.doc.gov/files/ntia/publications/ntia_request_for_comments_future_of_privacy_forum.pdf [https://perma.cc/APC4-EEHM]. In addition, various scholars and commentators have also supported or otherwise explored this possibility. *See, e.g.*, Mark E. Budnitz, *Touching, Tapping, and Talking: The Formation of Contracts in Cyberspace*, 43 NOVA L. REV. 235, 272–79 (2019) (discussing a lack of federal law and recommending the enactment of one); Shaun G. Jamison, *Creating a National Data Privacy Law for the United States*, 10 CYBARIS INTELL. PROP. L. REV. 1, 35 (2019) ("While it is not a foregone conclusion, it seems logical to place enforcement responsibility for a comprehensive federal data privacy law with the FTC due to their long experience bringing enforcement actions in this arena."); Ohm, *supra* note 103, at 1762–64 (2010) (noting that "there is an urgent need for comprehensive privacy reform in this country" and recommending the enactment of a federal law that would "mandate a minimum floor of safe data-handling practices on every data handler in the U.S."); W. Gregory Voss, *Obstacles to Transatlantic Harmonization of Data Privacy Law in Context*, 2019 U. ILL. J.L. TECH. & POL'Y 405, 458–61 (discussing the possibility of a federal law). In multiple instances, Congressional committees have also held hearings to discuss the possibility of a federal law in this area. *See, e.g.*, *Congress Should Enact a National, Comprehensive Consumer Privacy Framework: Hearing Before the S. Comm. on Com., Sci., & Transp.*, 117th Cong. 10 (Sept. 29, 2021) (statement of Maureen K. Ohlhausen, Former Acting Chair, Fed. Trade Comm'n) (arguing for a federal privacy law but against a private right of action); *Examining Legislative Proposals to Protect Consumer Data Privacy: Hearing Before the S. Comm. on Com., Sci., & Transp.*, 116th Cong. 16 (Dec. 4, 2019) (statement of Laura Moy, Assoc. Professor of L., Geo. Univ. L. Ctr.) (arguing in favor of a comprehensive federal privacy law); *Federal Trade Commission: Protecting Consumers and Fostering Competition in the 21st Century: Hearing Before the H. Comm. on Appropriations, Subcomm. on Fin. Servs. & Gen. Gov't*, 116th Cong. 2 (Sept. 25, 2019) (statement of Joseph J. Simons, Chairman, Fed. Trade Comm'n) (same).

when dealing with consumer data and a duty to avoid unreasonable risks.[314] First Amendment concerns associated with any such duties would need to be evaluated.

Congress could also consider restricting certain types of data practices and limiting the power or timing of consent.[315] At least one state appears to have tentatively moved in this direction. For instance, Illinois's Biometric Information Privacy Act ("BIPA") contains a private of right of action and prohibits companies from selling, leasing, or profiting from biometric identifiers once collected, although the statute permits a business to collect and disclose biometric identifiers if it initially "receives a written release executed by the" individual, among other things.[316] Connected vehicles can collect biometric related data. Recall that some automobile manufacturers already collect eye-movement tracking data[317] and use facial recognition technology.[318] Although BIPA is not entirely free from the constraints of the notice and consent model, the Seventh Circuit has noted that BIPA "flatly prohibits for-profit transactions" in biometric identifiers,[319] and various legal experts have observed that, pursuant to BIPA, covered entities cannot sell protected biometric data "regardless of any disclosure or consent."[320] Admittedly, Congress would need to consider First Amendment concerns connected to any such potential data restrictions.

---

314. *See, e.g.*, Balkin, *supra* note 27, at 1206 ("Although professional malpractice and professional breach of duty normally arise out of a contract, courts regularly enforce tort duties that do not have to be spelled out in a contract or explicitly agreed to by the parties; they also award tort damages. That is also true with respect to duties about information." (footnote omitted)); Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, 46 J. CORP. L. 143, 147 (2020) ("[r]econceptualizing [c]onsumer [t]ransactions as [f]iduciary [r]elationships"); Solove, *Murky Consent*, *supra* note 27, at 632–37 (discussing various possible duties, including that of loyalty, in the context of privacy law).

315. *See, e.g.*, Stacy-Ann Elvy, *Age-Appropriate Design Code Mandates*, 45 U. PA. J. INT'L L. 953, 1043–52 (2024) [hereinafter Elvy, *Age-Appropriate Design*] (discussing proposals to restrict the role and timing of consent); Solove, *Murky Consent*, *supra* note 27, at 627–38 (discussing limiting the role of consent).

316. 740 ILL. COMP. STAT. 14/15(b)-(c);14/20 (West 2010); *see also*, Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 817, 811–21 (2022) (discussing BIPA and the value of a private right of action).

317. OTONOMO, A PRIVACY PLAYBOOK FOR CONNECTED CAR DATA 15, 17 (2019), https://fpf.org/wp-content/uploads/2020/01/OtonomoPrivacyPaper.pdf [https://perma.cc/8TZ6-RNYT].

318. *Id.* at 17.

319. Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1247 (7th Cir. 2021); *see also* Vance v. Microsoft Corp., 534 F. Supp. 3d 1301, 1308 (W.D. Wash. 2021) ("[Section] 15(c) [of BIPA] is a flat-out prohibition. . . . In other words, unlike the collection, possession or dissemination of biometric data, no private entity may 'otherwise profit' from biometric data even if they inform and obtain permission from the subject. *Compare, e.g.*, 740 ILCS 14/15(d) (allowing dissemination of biometric data with consent from subject), *with* 740 ILCS 14/15(c) (containing no exceptions)."); Alan S. Wernick, *How Will Proposed Amendments to Illinois's BIPA Affect the Use of Biometric Data*, AM. BAR ASSOC. (June 17, 2024), https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-june/how-will-proposed-amendments-to-illinois-bipa-affect-the-use-of-biometric-data (on file with the *Iowa Law Review*) (discussing amendments to BIPA that impact electronic consent and damages).

320. LOCKE LORD LLP, BIOMETRIC INFORMATION PRIVACY ACT (BIPA): A CHECKLIST FOR DEFENDANTS 1 (2017), https://www.lockelord.com/-/media/files/newsandevents/publications

Additionally, on the issue of consent, in recent years, some courts have attempted to expressly acknowledge and address the realities of consumer online agreements by conducting a more granular and refined application of existing standards for determining consent.[321] These courts have insisted on meticulously analyzing the presentation of online terms and conditions from the consumer's perspective. While a privacy policy may be distinct from a contract, principles courts establish to evaluate companies' terms and conditions may provide helpful guidance in restoring the integrity of consent and choice in the privacy context.[322]

To the extent that existing state privacy laws and federal frameworks do not contain adequate cybersecurity requirements for the vehicular context, Congress could impose, via a comprehensive privacy statute, stringent cybersecurity obligations. Such restrictions should apply to any data collected via the use of VMC technology or features in consumer vehicle transactions. Covered entities could be required to adopt appropriate cybersecurity practices to ensure that connected vehicle data and VMC data are not stored improperly and to limit unnecessary disclosures of data to employees and

/2017/11/bipaperdewshetty.pdf [https://perma.cc/L4M7-KRGT] ("If you are collecting biometrics as defined by BIPA, evaluate your practices for compliance. . . . Also, do you sell, lease, trade, or otherwise profit from a person's biometrics? If so, stop immediately. This is prohibited regardless of any disclosure or consent."); *see also* Anjelica Cappellino, *The Illinois Biometric Information Privacy Act: What Makes a Winning Case?*, EXPERT INST. (May 27, 2021), https://www.expertinstitute.com/resources/insights/the-illinois-biometric-information-privacy-act-what-makes-a-winning-case [https://perma.cc/7NVP-GUQX] ("The BIPA prohibits any private entity from selling the data, even with consent."). *Compare* Lydia de la Torre, Elliot Golding & India K. Scarver, *The Illinois Biometric Information Privacy Act ("BIPA"): When Will Companies Heed the Warning Signs?*, NAT'L L. REV. (Feb. 17, 2020), https://www.natlawreview.com/article/illinois-biometric-information-privacy-act-bipa-when-will-companies-heed-warning [https://perma.cc/D4PU-SJ3Y] (noting that "BIPA imposes five distinct obligations," including a "[p]rohibition against profiting (even with consent)" by way of "selling, leasing, trading, or otherwise profiting from biometric data"), *with* Theodore F. Claypoole & Cameron S. Stoll, *State Forays into the Regulation of Biometric Data*, LAW360 (Nov. 10, 2015, 11:12 AM), https://www.law360.com/articles/724349/state-forays-into-the-regulation-of-biometric-data (on file with the *Iowa Law Review*) (noting that "BIPA prohibits an entity from profiting from biometric data it collects" in contrast to the Texas law that "allows a party to sell, lease or disclose biometric identifiers under a narrow set of circumstances"). It also bears noting that, of the many state laws on the issue, "only BIPA prohibits the sale of biometric information without exception." Joshua Valentino, *Setting the Framework for Biometric Privacy Legislation After the "Big Bang" of Biometrics in the Workplace*, 38 HOFSTRA LAB. & EMP. L.J. 167, 178 (2020). *But see* Vigil v. Take-Two Interactive Software, Inc., 235 F. Supp. 3d 499, 512 n.9 (S.D.N.Y. 2017), *aff'd in part, vacated in part on other grounds sub nom.* Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12 (2d Cir. 2017) ("In relation to the other terms in Section 15(c)—'selling,' 'leasing,' and 'trading'—'otherwise profiting' is a catchall for prohibiting commercially transferring biometric information and biometric identifiers in a manner not contemplated by the original biometric-facilitated transaction, without consent from the individual pursuant to Section 15(d). Promoting a transaction—here, the sale of a video game—by advertising a biometric-related feature does not contravene the statute."); Elvy, *Age-Appropriate Design*, *supra* note 315, at 1045 n.354 (same).

321. *See, e.g.*, Berkson v. Gogo LLC, 97 F. Supp. 3d 359, 402 (E.D.N.Y. 2015) (providing multi-prong inquiry in analyzing electronic contracts that addresses these nuances); *see also* Nancy S. Kim, *Online Contracting*, 72 BUS. LAW. 243, 247–52 (2016–2017) (discussing several cases in which courts have conducted nuanced analyses of reasonable notice and manifestation of assent standard).

322. Stacy-Ann Elvy, Response, *Privacy Law's Consent Conundrum*, 104 B.U. L. REV. 641, 642 (2024).

unrelated third parties. Additionally, such a statute could authorize express binding regulations from regulatory authorities clarifying companies' cybersecurity obligations and the contents of their cybersecurity programs in the vehicular context beyond the reasonable cybersecurity standard discussed in Part II.[323] Previously issued nonbinding and voluntary guidance from existing regulatory actors, such as the National Institute of Standards and Technology and the National Highway Traffic Safety Administration regarding cybersecurity and connected vehicles and objects, could be a useful starting point in this regard.[324]

With respect to the use of subscription based for-profit models supported by VMC features in connected vehicles, Congress and states could consider addressing the electronic subjugation risks associated with these models and connected vehicles given the essential role that vehicles play in consumers' daily lives and existing restrictions on consumers' ability to obtain a refund for purchased or leased vehicles. The shift to subscription-based models enabled by VMC features represents a broader technological transition in society that enhances and cements corporate control over citizens and their devices post-transaction.

This shift has inundated various industries. While subscription-based models and remote disablement may raise less concerns in other contexts and industries, the use of this business model combined with VMC features in the consumer connected vehicle setting, particularly when associated with essential vehicle functions, raises significant risks for consumers. Congress might consider imposing limits on this practice in the consumer vehicle context. Existing regulatory bodies with authority over the automobile industry should also consider electronic subjugation and safety risks associated with

323. *See supra* Part II. For a discussion of concerns associated with the ambiguous reasonable cybersecurity standard see Scott J. Shackelford, Anne Boustead & Christos Makridis, *Defining "Reasonable" Cybersecurity: Lessons from the States*, 25 YALE J.L. & TECH. 86, 88–90 (2023).

324. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., U.S. DEP'T OF TRANSP., CYBERSECURITY BEST PRACTICES FOR THE SAFETY OF MODERN VEHICLES 1 (2022), https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf [https://perma.cc/E8XJ-7GVD] (updating "the agency's non-binding and voluntary guidance to the automotive industry for improving motor vehicle cybersecurity"); U.S. DEP'T OF TRANSP., HOW TO USE THE CYBERSECURITY FRAMEWORK PROFILE FOR CONNECTED VEHICLE ENVIRONMENTS 2 (2021), https://www.its.dot.gov/research_areas/cybersecurity/docs/3_How_to_Use_the_CSF_Profile_for_CVE.pdf [https://perma.cc/9R6Z-8J8N] (introducing the "NIST Cybersecurity Framework" to the connected vehicle context and "how organizations can use it to manage cybersecurity risk"); MICHAEL FAGAN, KATERINA N. MEGAS, KAREN SCARFONE & MATTHEW SMITH, NAT'L INST. OF STANDARDS & TECH., NISTIR 8259A, IOT DEVICE CYBERSECURITY CAPABILITY CORE BASELINE 3 (2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf [https://perma.cc/6T8E-DHF9] (defining IoT "device cybersecurity capability core baseline"); MICHAEL FAGAN, KATERINA N. MEGAS, KAREN SCARFONE & MATTHEW SMITH, NAT'L INST. OF STANDARDS & TECH., NISTIR 8259, FOUNDATIONAL CYBERSECURITY ACTIVITIES FOR IOT DEVICE MANUFACTURERS ii (2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf [https://perma.cc/PF9T-B6B4] (describing "recommended activities related to cybersecurity that manufacturers should consider performing before their IoT devices are sold to customers").

these practices as well. Recall that, in 2022 and 2023, New Jersey and Pennsylvania proposed limiting the use of vehicle subscription-based models.[325]

States, Congress, and regulatory bodies may also need to revisit the connection between a vehicle's warranty and subscription-based services in connected vehicles. A vehicle's warranty may last for only a few years, but if the consumer continues to pay for a subscription to essential vehicle functions that are associated with VMC features, automobile companies should continue to provide repair and maintenance services associated with those subscriptions.[326] Lastly, Congress may need to take a fresh look at the Magnuson–Moss Warranty Act, which governs consumer product warranties.[327]

CONCLUSION

This Article tells an important story, one where VMC technology and subscription services in connected vehicles are part of a growing technological and societal shift in which individuals have less privacy and control of their lives and devices. The privacy, cybersecurity, and electronic subjugation risks discussed in this Article are not just faced by those of us who are less well-off financially. Indeed, subscription-based models supported by VMC features appear to be spreading to the non-subprime automobile context. States, Congress, and regulatory bodies must contend effectively with the privacy, cybersecurity, and electronic subjugation risks associated with VMC technology and subscription-based models in connected vehicles. This Article charts an initial path forward.

325. S.B. 3271, 220th Leg., Reg. Sess. (N.J. 2022); Memorandum from Pa. Sen. Marty Flynn, *supra* note 51.

326. Barry, *supra* note 16.

327. 15 U.S.C. §§ 2301–2312.