2024

Remote Repossession

Rebecca Crootof

REMOTE REPOSSESSION

*Rebecca Crootof**

Ford's February 2023 patent application raises a new possibility: that after a default, an internet-connected vehicle might autonomously drive itself off of the owner's premises—to a public space, to the repossession agency, or even to a junkyard. But while this "remote repossession" would minimize the risks of harm that attend in-person repossessions, it creates at least three new risks. First, a danger of bodily injury and property damage to the owner. Second, an increased likelihood of physical harm to a third-party with no obviously responsible entity. And third, most invisibly but also perhaps most importantly: further erosion of consumers' current structural rights—which might include a right against intrusions, a right to a certain amount of due process and human engagement before a repossession, and a right to be free from foreseeable harms associated with corporate remote interference.

I employ a techlaw methodology to explore what legal changes would better protect us—as potential defaulting owners, as possibly harmed third-parties, and as consumers who must increasingly rely on corporations to take reasonable care when engaging in digital self-help.

Table of Contents

* Associate Professor of Law, University of Richmond School of Law and Affiliate Fellow, Yale Law School Information Society Project. For insightful comments and questions, thanks to BJ Ard, Gilat Bachar, Jim Gibson, John Goldberg, Mark Lemley, Aaron Perzanowski, David Schwartz, Danielle Wingfield, and Josephine Wolff, as well as to participants in the University of Richmond Faculty Workshop, the University of Richmond Junior Faculty Forum, the Institute for Law, Innovation & Technology, the Sixth Junior Faculty Forum for Law and STEM, and the 29th Annual Clifford Symposium on Tort Law and Social Policy. Bethany Jones provided excellent research assistance, and the editors of the *DePaul Law Review* offered many helpful suggestions.

Introduction

Thanks to the proliferation of networked devices, many Internet of Things ("IoT") companies had a newfound power. They can now engage in "remote interference," which entails employing over-the-air updates to alter or deactivate a physical device.[1] This might be done for a host of reasons that benefit both the company and the consumer: for example, remote updates can enable new capabilities or eliminate cybersecurity vulnerabilities.[2] But the ability to unilaterally alter a device is also a new source of coercion and control: thanks to contract law, companies can lawfully hold property hostage[3] or even punish consumers for their conduct.[4]

While others have written on the consumer, contractual, cybersecurity, national security, privacy, and property issues associated with digital self-help,[5] I have been primarily interested in its capacity for facilitating

1. Rebecca Crootof, *The Internet of Torts: Expanding Civil Liability Standards to Address Corporate Remote Interference*, 69 Duke L.J. 583, 585 (2019) [hereinafter Crootof, *IoTorts*].

2. *Id.* at 586–87. For example, after a May 2018 Consumer Reports alleged that the Tesla Model 3 had a stopping distance worse than any other contemporary car, Tesla pushed out a software update that improved the car's braking distance by nineteen feet—quite likely resulting in saved lives. *Id.* at 586 n.7; Patrick Olsen, *Tesla Model 3 Gets CR Recommendation After Breaking Update*, Consumer Reports (May 30, 2018), https://www.consumerreports.org/car-safety/tesla-model-3-gets-cr-recommendation-after-braking-update/ [https://perma.cc/DM4T-DTK8].

3. Crootof, *IoTorts*, *supra* note 1, at 604. For example, smart-speaker company Sonos announced that "it would not provide expected and necessary software updates unless consumers agreed to changes to the privacy and data-collection policy, which expand the company's ability to use the speakers to collect, use, and share personal data." *Id.*

4. *Id.* at 605. For example, after a user left an angry comment on the smart-garage-door-opener company Garadget's community board and a one-star review on Amazon, the product's inventor and distributer denied the unit server connection. *Id.* Because the user had not yet activated his device, he was not locked out of his garage or left with his garage door permanently open—but another might have been. *Id.*

5. *See, e.g.*, Joshua A.T. Fairfield, Owned: Property, Privacy, and the New Digital Serfdom (2017); Margaret Jane Radin, Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law (2013); Aaron Perzanowski & Jason Schultz, The End of Ownership: Personal Property in the Digital Economy (2016); Ryan Calo, *Tiny Salespeople: Mediated Transactions and the Internet of Things*, 2013 IEEE Security & Privacy 70 (2013); Danielle Keats Citron, *Sexual Privacy*, 128 Yale L.J. 1870 (2019); Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 Berkeley Tech. L.J. 1089 (1998); Laura DeNardis & Mark Raymond, *The Internet of Things as a Global Policy Frontier*, 51 U.C. Davis L. Rev. 475 (2017); Stacy-Ann Elvy, *Hybrid Transactions*

physical harm. The embodied nature of IoT devices means that remote interference can sometimes risk foreseeable bodily injury and property damage[6]—consider the risks associated with baby monitors, senior lifelines, home-security systems, fire alarms, and medical implants that suddenly don't work as expected![7]—but it remains unclear whether tort law will evolve to enable harmed individuals to hold companies liable.[8]

In my prior writing on corporate interference and remotely-caused harms, one of my paradigmatic examples was that car companies now use starter-interrupt devices to remotely boot cars, mere days after a payment is missed.[9] Despite "reports of parents unable to take children to the emergency room, individuals marooned in dangerous neighborhoods, and people whose cars were disabled while idling in an intersection," this self-help practice is both lawful and cheap—and so companies are likely to continue employing it, despite the fact that there is "an obvious risk of injury when an otherwise operational car does not work as expected."[10]

Clearly, I was thinking too small.

In February 2023, Ford's "Systems and Methods to Repossess a Vehicle" patent application was published.[11] Unsurprisingly, it noted various remote interferences intended to spur a debtor to make an overdue payment, including the possibility of disabling different car systems, ranging from "second level" components (the air conditioning

---

and the INTERNET of Things: Goods, Services, or Software?, 74 Wash. & Lee L. Rev. 77 (2017); Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 Calif. L. Rev. 805, 812 (2016); João Marinotti & Asaf Lubin, Cyber Vigilantes: The Limits of Technological Self-Help (Oct. 2023) (manuscript on file with author); Christina Mulligan, *Personal Property Servitudes on the Internet of Things*, 50 Ga. L. Rev. 1121, 1158 (2016); Margaret Jane Radin, *Regulation by Contract, Regulation by Machine*, 160 J. Inst. Theo. Econ. 142 (2004); Charlotte A. Tschider, *Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age*, 96 Denver L. Rev. 87, 109 (2018).

6. Crootof, *IoTorts*, *supra* note 1, at 606–08. There is a growing literature on the physical risks associated with hackable IoT devices; I observed that "corporations can do anything hackers can do—but their actions are legitimized by contract." *Id.* at 610.

7. *Id.* at 589, 607–08.

8. "[A]bsent a better understanding of how IoT-enabled harms operate and propagate, judges are likely to apply contracts, products liability, and negligence doctrinal standards narrowly, in ways that functionally minimize corporate liability." *Id.* at 611; *see also id.* at 611–22 (discussing contractual obstacles to suit); *id.* at 622–26 (discussing difficulties in applying products liability law); *id.* at 627–32 (discussing difficulties in establishing duty and breach for a negligence analysis); *id.* at 632–38 (discussing difficulties in establishing causation).

9. *See* Michael Corkery & Jessica Silver-Greenberg, *Miss a Payment? Good Luck Moving That Car*, N.Y. Times (Sept. 24, 2014, 9:33 PM), https://dealbook.nytimes.com/2014/09/24/miss-apayment-good-luck-moving-that-car (describing a lender who "remotely activated a device . . . that prevented [a lessor's] car from starting.").

10. Crootof, *IoTorts*, *supra* note 1, at 585.

11. U.S. Patent Application No. 17/408,004, Publication No. US 2023/0055958 A1 (published Feb. 23, 2023) (Ford Global Technologies, LLC, applicant) [hereinafter Patent Application].

or remote key fob) to "first level" components (the infotainment system or cruise control) to "primary-use" components (the engine, steering wheel, lights, accelerator, and brake).[12] The patent application also proposed "activating the audio component [in the vehicle] . . . to emit an incessant and unpleasant sound,"[13] as well as configuring the vehicle's cameras and sensors to capture images that might allow for the identification of "undesirable actions that the owner of the vehicle may take in response to the lockout condition."[14]

But then—*wow*—the Ford patent application suggests that cars with autonomous or semi-autonomous capabilities could be remotely driven "from a first spot to a second spot that is more convenient for a tow truck to tow the vehicle," such as a location "outside the property line";[15] "from the premises of the owner to a location such as, for example the premises of the repossession agency";[16] or, after remotely considering the "financial viability of executing a repossession procedure," "to a junkyard."[17]

Not only might companies remotely use or deactivate features on our devices or the devices themselves—implicating issues I discussed in my prior article—but they are now anticipating *remotely repossessing* them, an entirely new means of taking matters into their own hands.

While remote repossession would minimize confrontations between the owner and repossessor, it creates new risks.[18] Imagine: After a default

12. *Id.* at 3. But no need to be afraid of the risk of not being able to seek medical help that might be associated with an unexpected lockout! The lockout "may be lifted momentarily in case of an emergency situation so as to allow the vehicle to travel to a medical facility when the emergency is a medical emergency." *Id.* at 1. To "avoid endangering safety and health of the owner and other people associated with the vehicle, when the vehicle has been placed in the lockout condition," the patent proposes that the system "may evaluate images provided by one or more cameras of the vehicle in order to detect an emergency (e.g., a medical emergency situation) such as, for example, a driver of the vehicle suffering a heart attack" and "may immediately communicate with the computer of the medical facility to dispatch medical assistance." *Id.* at 4. *See also id.* at 5 (further detailing what might be done in a lockout situation, including the possibility of the repossession system computer identifying the address of the closest medical facility and "automatically configur[ing] a GPS device in the vehicle to assist the owner travel to the medical facility as quickly as possible.").

This is likely Ford attempting to cover all of their bases for purposes of patent coverage, rather than an actual plan. Aside from the fact that emergencies are unlikely to happen near the locked-down vehicle, it seems unlikely that a remote monitor will be able to quickly identify and respond to "real" ones—emergency room doctors practiced at triage have difficulty visually identifying heart attacks.

13. *Id.* at 4.

14. *Id.*

15. *Id.*

16. *Id.*

17. Patent Application, *supra* note 11, at 4–5.

18. I use the term "owner" (which encompasses "leaser") in this Article in part because that is the language in the Ford patent application and in part because it emphasizes the new power remote corporate interference enables in a way that the alternative—"debtor"—does not.

on an auto loan, a company begins the process of remotely repossessing a vehicle. The car drives away without incident—when no precious personal property happened to be in the car, before the family's pet cat who enjoys sleeping behind the back wheel has arrived, after the child who has snuck into the backseat of the parked car to play pretend has left,[19] without destroying the cherished heirloom rosebush that lines the driveway—and promptly veers into oncoming traffic, crashing into your car.[20] Happily, you are unscathed, but both the repossessed vehicle and your car are totaled. (And, while it goes without saying, you were driving perfectly.)

There are at least three kinds of harms raised by this scenario.[21] First, the increased danger of bodily injury and property damage to the owner and owner's property. I have previously considered the risks and legal issues associated with harmful remote corporate interference, and so I do not here reiterate the barriers to a successful suit for compensation nor my recommendations.[22] But it is worth noting two facts relevant to the remote repossession context. We are all at risk of becoming the debtor in this scenario, especially as car loans grow more expensive.[23] Additionally, although these harms may touch every member of society, they will fall more heavily on certain vulnerable demographics. Low-income folks with low credit ratings will obviously be specially affected,[24] and in America that group tends to be comprised disproportionately of people of color.[25] This overlaps with another demographic that will be particularly affected by remote repossessions: those in the

19. This is not a pure hypothetical—my children actually do this.

20. Nor is this a pure hypothetical—at least as of 2020, the inability of autonomous vehicles to maintain proper lane positions accounted for 73% of all incidents observed on public roadway tests. Erik Bascome, *Automated Driving Systems Are Prone to Errors, Study Finds*, Gov't Tech. (Aug. 12, 2020), https://www.govtech.com/fs/transportation/automated-driving-systems-are-prone-to-errors-study-finds.html [https://perma.cc/W354-2EU6].

21. *Cf.* Mark A. Lemley & Bryan Casey, *Remedies for Robots*, 86 U. Chi. L. Rev. 1311, 1326–42 (2019) (creating a typology of harms associated with robotic actions, including unavoidable harms, deliberate least-cost harms, defect-driven harms, misuse harms, unforeseen harms, and systemic harms).

22. *See* Crootof, *Io Torts*, *supra* note 1.

23. *See, e.g.*, Jenn Jones, *Average Car Payment and Auto Loan Statistics 2023*, Lending Tree, https://www.lendingtree.com/auto/debt-statistics/ [https://perma.cc/FM8X-5QN9] (last updated June 27, 2023) (observing that "[t]he 10.8% hike in the average new car payment is nearly 5 percentage points higher than the new vehicle price increase of 6.1%" and that "[o]verall [American] vehicle debt more than doubled between the fourth quarter of 2012 ($783 billion) and the fourth quarter of 2022 ($1.55 trillion)").

24. *See, e.g.*, Matt Phillips, *Low-income households are falling behind on car bills*, Axios (Mar. 1, 2023), https://www.axios.com/2023/03/01/low-income-households-are-falling-behind-on-car-bills.

25. The causal reasons for this in the auto loan context have been linked to structural racism. *See* Alexander W. Butler, Erik J. Mayer & James P. Weston, *Racial Discrimination in the Auto Loan Market*, 36 Rev. Fin. Stud. 1 (2023) (finding that "Black and Hispanic applicants' loan approval rates are 1.5 percentage points lower" than White applicants', "even controlling for creditworthiness"

eighteen to thirty-nine age bracket, some of whom are reportedly missing rent or credit card payments in order to cover their car debt.[26] So, to generalize, those with fewer resources and less access to justice will be more likely to experience the increase in this first category of harm.[27]

A second type of harm is the increased likelihood of an accident with a third-party, which raises a different accountability issue. When the remotely repossessed vehicle totals your car, who do you sue for your damages? The owner? The remote repossessor? The car manufacturer? The software designer? This is hardly a new question, even before the explosion in autonomous vehicle scholarship—there have long been complicated causal chains involving multiple actors. But, absent legal adjustments, contractual barriers and inadequate awareness about how technology tends to shield remote decisionmakers may render your negligence suit against a remote repossessor more difficult to win than you might anticipate.[28]

While interesting in their own right, the questions of who bears the costs when a remotely repossessed vehicle harms an owner or third-party could be seen as short-term, transitional problems. Should companies engage in remote repossession, an accident occur, and the harmed party sue, a judge will wrestle with various precedents and analogies and policy considerations to determine where responsibility lies and what liability standard should be applied. Tort law will evolve.[29]

But there is a third potential harm here, as well—to all of us, as consumers. Taking a permissive stance and trusting courts to resolve the uncertainties associated with remote repossession risks undermining rights that we may not even recognize we have. Thanks to the current infeasibility of engaging in remote repossession, we arguably have a right against intrusion, a right to a certain amount of due process and human engagement before a repossession, and a right to be free from

---

and that minorities who receive loans pay interest rates 70 basis points higher than comparable white borrowers).

26. *See, e.g.*, Emmet White, *Auto Loans Are Going Unpaid, But Who's Not Paying?*, AUTOWEEK (Mar. 2, 2023), https://www.autoweek.com/news/industry-news/a43141284/auto-loans-unpaid-gen-z/ [https://perma.cc/6SA6-3LSJ].

27. But wait—aren't autonomous vehicles luxury items, unlikely to be purchased by folks with fewer resources? Maybe at the moment, but car companies are exploring making vehicles increasingly autonomous. And even inexpensive cars may have various autonomous features—like cruise control, lane awareness, and parking assistance—that could be activated to enable remote repossessions.

28. *See* Lemley & Casey, *supra* note 21, at 1352–53.

29. That being acknowledged, there are reasons to fear it will evolve in problematic ways. For example, absent a techlaw analysis, traditional torts—like trespass or conversion—will probably not protect the rights to be free from exclusive use of real property or protections for personal property, as both require that the prohibited actions occur without consent. Here, however, the owner has likely preemptively consented to the possibility of remote repossession. *See also* Crootof, *IoTorts*, *supra* note 1, at 610–41 (discussing various barriers to civil liability suits by owners for corporate remote interference that causes physical harm).

foreseeable harms associated with corporate remote interference. But all of these "structural rights"—rights which have thus far been protected by what is physically possible and which we have been able to take for granted—are endangered by remote repossession.[30] Recognizing this threat early enables us to take steps to consider and codify the rights worth preserving.

I employ a techlaw methodology to explore these issues, which provides guidance on how technology can complicate traditional doctrinal analyses and highlights considerations that the usual process of legal evolution might miss.[31] In Part I, I briefly review the benefits and risks that accompany remote repossession. In Part II, I argue that to protect public safety—the primary reason given for current limitations on repossessions—there should be (1) a prohibition on contractual clauses that purport to shift liability from the repossessing entity to the owner; (2) an assumption that the repossessor is the default defendant; and (3) a rebuttable presumption that third-parties harmed during remote repossessions did not contribute to causing the accident. In Part III, I discuss how rendering repossession newly cheap and easy might undermine other, non-codified consumer rights and argue that, to the extent remote repossession is permitted, we need to evaluate whether these rights should be proactively protected. In the conclusion, I review how a techlaw methodology informed this Article's analysis and argue that this situation's factors weigh in favor of taking proactive legal action.

I. A New Kind of Corporate Self-Help

Historically, a company that wanted to repossess a car after an alleged breach of contract would have two options: engage in self-help or involve the state.[32] Because of the opportunity for physical harm and conflict escalation associated with self-help, however, companies could only take matters into their own hands up until doing so risked a "breach of the peace."[33] At that point—which is usually understood

30. Harry Surden, *Structural Rights in Privacy*, 60 SMU L. Rev. 1605, 1610–14 (2007) (introducing the concept of "structural rights").

31. Rebecca Crootof & BJ Ard, *Structuring Techlaw*, 34 Harv. J.L. & Tech. 347, 349–50 (2021) (outlining a methodology for responding to tech-fostered legal uncertainties); Rebecca Crootof & BJ Ard, Distinguishing Techlaw (Jan. 2024) (unpublished manuscript) (describing core techlaw concepts); BJ Ard & Rebecca Crootof, *The Case for "Technology Law"*, The Record (Dec. 16, 2020), https://ngtc.unl.edu/blog/case-for-technology-law [https://perma.cc/2EKU-GD67] (arguing that Technology Law should be recognized as a standalone subject).

32. "Self-help" entails actions taken by private parties to a controversary, either to prevent or resolve a dispute, that do not entail the involvement of a government actor or disinterested third-party. Celia R. Taylor, *Self-Help in Contract Law: An Exploration and Proposal*, 33 Wake Forest L. Rev. 839, 841 (1998).

33. Cohen, *supra* note 5, at 1103.

to occur as soon as the owner contests the property's removal[34] or prevents it the activity by keeping the property in a locked space[35]—the company must involve state actors, as only the state has the authority to exercise force or to go onto another's land without permission.[36]

Remote corporate interference created a third option for a would-be repossessor: remotely disabling certain features or an entire device, which grants companies some of the benefits of repossession—denying the owner use of the item, and thereby incentivizing payment—without engaging in activities that risked breaches of the peace.[37]

Now, the combination of remote interference and device mobility offers a fourth possibility: Having the item move itself to a public road or other location where the company can retrieve it. This remote repossession grants the company all of the benefits associated with remote interference, plus the added ability to recover (and thus resell) the property itself, all without risking a confrontation.[38] This is understandably appealing to car companies: At present, "approximately 20% of auto loans in default never become a repossession."[39] A new, no-muss, no-fuss means of retrieving vehicles would allow companies to retrieve a *lot* more vehicles.[40] And apparently many companies are interested in this activity: Ford has since abandoned its patent application, most likely because the Patent Office thought that the technology was obvious in light of prior patent applications for similar activities.[41]

---

34. Both Connecticut and New York courts have held that conduct resulting in verbal objections alone can constitute prohibited breaches of the peace. Aviles v. Wayside Auto Body, Inc., 49 F. Supp. 3d 216, 226 (D. Conn. 2014); Boles v. Cnty. of Montgomery, No. 6:11–cv–522, 2014 WL 582259, at *9 (N.D.N.Y. Feb. 13, 2014). Under such law, the remote activation of car alarms might alone be found to be a breach of the peace. *See* Patent Application, *supra* note 11, at 4.

35. Most states allow repossessing agents to enter driveways that are open to the public. *See, e.g.*, CAL. BUS. & PROF. CODE § 7508.2(d) (West 2023) (prohibiting entry into "any private building or secured area"). Massachusetts, however, does not allow any entrance onto private property. MASS. GEN. LAWS ch. 255B, § 20B (2001).

36. Cohen, *supra* note 5, at 1103 (noting also that even the state power is limited by due process principles).

37. Crootof, *IoTorts*, *supra* note 1, at 603.

38. Indeed, avoiding confrontation is the motivating reason for Ford's patent. The application observes, as background, that when a lender attempts to repossess a vehicle, "[t]ypically, the owner is uncooperative . . . and may attempt to impeded the repossession operation. In some cases, this can lead to confrontation. It is therefore desirable to provide a solution to address this issue." Patent Application, *supra* note 11, at 1.

39. *Auto Loan Defaults Are Increasing, But We Are Not Heading Into a Repo Crisis*, COX AUTO. fig.1 (Aug. 3, 2022), https://www.coxautoinc.com/market-insights/auto-loan-defaults-are-increasing-but-we-are-not-heading-into-a-repo-crisis/ [https://perma.cc/GR86-U8EP].

40. There were 2.1, 1.6, and 1.5 million auto loan defaults in 2019, 2020, and 2021 respectively (with the dramatic 2020 decrease attributed to the coronavirus-associated loan accommodation and government stimulus). *Id.*

41. *See, e.g.*, U.S. Patent Application No. 11/350,934, Publication No. US 20070136083 A1 (published Jun. 14, 2007) (Simon et al., applicant).

A techlaw perspective—which entails stepping back to see how this new activity is akin to other tech-enabled ones—highlights how remote repossession is yet one more example of a scenario where new technology enables a new activity, raising the questions of whether old law does and should apply and whether new interpretations or rules are needed.[42] To resolve these uncertainties, it is useful to first understand why the current law is what it is.

There are many benefits to facilitating corporate self-help. As David Pozen has observed, "[s]elf-help would not pose such a knotty problem for legal designers if it did not yield valuable benefits."[43] The possibility of self-help may deter "wrongdoing from occurring in the first place, reduce administrative costs, promote autonomy- or sovereignty-related values, and facilitate speedier redress."[44] Further, self-help might facilitate "cooperative relations, mitigate feelings of alienation from the law, or generate deeper internalization of first-order legal norms."[45]

However, because of the likelihood of self-interested interpretations, "[t]here is ample reason to worry that [those who engage in self-help] will misconstrue the law along the way—not just, or even primarily, on account of bad faith," but rather because of internal, even unconscious, motivations to reach a particular conclusion.[46] And "[s]elf-interested enforcement is even more problematic when the relevant law is drafted by the enforcing entity—as is the case when IoT companies act in accordance with their terms of service."[47] Indeed, given that IoT devices enable a new level of ongoing, intimate corporate surveillance,[48] IoT companies have "a newfound ability to identify violations of once under-enforced or unenforceable contractual terms," which in turn "invites companies to incorporate increasingly stringent and invasive terms into their contracts—precisely because those terms can now be enforced."[49] Further, the risks of abusive contractual terms and enforcement are heightened in the repossession context, given the company's

42. Crootof & Ard, *supra* note 31, at 356–76 (discussing how technological developments raise application uncertainties (whether and how extant law applies) and normative uncertainties (whether the application of the law accomplishes its aims)).

43. David E. Pozen, *Self-Help and the Separation of Powers*, 124 YALE L.J. 2, 49 (2014).

44. *Id.*

45. *Id.*

46. *Id.* (noting that self-helpers may be biased by "motivated cognition and reliance on congenial interpretive methods or theories of law.").

47. Crootof, *IoTorts*, *supra* note 1, at 604.

48. *Id.* at 596–98.

49. *Id.* at 599–600; *see also* Marinotti & Lubin, *supra* note 5 (highlighting how companies abuse technological self-help measures and proposing a framework for distinguishing legitimate forms of technological self-help from illegitimate cyber vigilantism).

added incentive to reclaim and resell the contested goods.[50] (There's a reason the paradigmatic case on unconscionability was based on a repossession contract.)[51]

So, while we may want to permit a certain amount of corporate self-help—including remote repossession[52]—for both practical and normative reasons, we also want to ensure that it is appropriately bounded. Protecting public safety, as manifested in the prohibition on breaching the peace, is an objective worth preserving, though new interpretations or standards may be needed in this new context. And, in light of the new risks associated with remote repossession, new codifications of once-structural rights may also be necessary.

II. Protecting Public Safety

The restriction on the use of self-help in car repossessions was originally intended to promote public safety by minimizing the risk of conflict escalation.[53] Evaluating this old justification in this new context requires weighing whether public safety would be better protected if we trade lowering the risk of confrontation between the company and owner for (possibly) increasing the risk of other harms.

To some extent, this analysis turns on facts we don't yet have. We know that direct confrontations in traditional repossession scenarios have led to physical violence and can gather data on associated harms, but we have no information about the safety of remotely repossessing vehicles. Still, to the extent vehicles with varying degrees of autonomous capabilities are approved for road use, they will presumably operate reasonably safely. Accordingly, in balancing the safety concerns associated with the risk of confrontation against those associated with the risks of accidents, one might conclude that there is a strong safety argument for permitting remote repossessions.

However, there are additional concerns to consider, arising from the possibility that the repossessing entity might be able to evade liability

50. David Friedman, *In Defense of Private Orderings: Comments on Julie Cohen's "Copyright and the Jurisprudence of Self-Help"*, 13 Berkeley Tech. L.J. 1151, 1162 (1998) ("In the case of physical goods, there is an obvious reason why creditors may be tempted to abuse their right to repossess—they want the goods . . . in order to sell it again to someone else.").

51. Williams v. Walker-Thomas Furniture Co., 350 F.2d 445, 450 (D.C. Cir. 1965).

52. As I can see arguments on both sides, I don't have a strong stance as to whether remote repossession should be permitted or prohibited. My main aim in this contribution is to argue that we should anticipate certain likely consequences of permitting remote repossession, identify likely pitfalls for legal interpreters, and proactively create new law to minimize the erosion of extant structural rights.

53. *See, e.g.*, Morris v. First Nat'l Bank & Trust Co., 254 N.E.2d 683, 686 (Ohio 1970) (stating that one purpose of self-help car repossessions is to discourage acts by citizens that may result in violence).

for associated harms. Absent legal rules that minimize their ability to do so, repossessing entities will attempt to sidestep liability. And, to the extent they can, repossessing entities may not be properly incentivized to minimize the risk of remote repossession harms. Accordingly, this Part concludes with recommendations for legal adjustments that will protect public safety by increasing the likelihood that the remote repossessor is held liable for the harms they cause. (Again, I have discussed the challenges of holding corporations engaging in remote interference to be held liable for harms to owners and their property elsewhere;[54] here, I focus on harms to third-parties.)

A. Contracting Out of Liability

Remote repossessors may attempt to contractly evade liability by requiring owners to agree to indemnify them for any harms that arise from that activity.[55] While liability-shifting clauses may already be formally unenforceable,[56] companies regularly include contractual terms that they know will not be applied to dissuade consumers from bringing suit in the first place.[57] Tesla's warranty for its vehicles, for example, purports to waive liability for contract, tort, breach of warranty, and misrepresentation claims, even those which some courts have found unwaivable, such as those grounded in gross negligence or based on reasonably foreseeable harms.[58] For reasons discussed below, there are a host of policy reasons why the owner should not be held liable for harms arising from remote repossession.

---

54. *See* Crootof, *IoTorts*, *supra* note 1.

55. As one cynical commenter on an article about remote repossessions noted:

> Typhooner: Assume the car is involved in an accident while on its solo tour. Who is responsible? The manufacturer of the system? The person pressing the 'move' button? The leasing agency?
>
> Jeff: They'll simply write the rules to say the owner is liable since "If they had paid their bill we wouldn't [have] had to repossess the vehicle"

Typhooner & Jeff, Comment to Peter Holderith, *Ford Applies to Patent Self-Repossessing Cars That Can Drive Themselves* Away, The Drive, (Mar. 2, 2023), https://www.thedrive.com/news/future-fords-could-repossess-themselves-and-drive-away-if-you-miss-payments [https://perma.cc/S7U9-GZF2].

56. *See* Crootof, *IoTorts*, *supra* note 1, at 614 nn.156–62 (providing examples of state law that invalidate exculpatory clauses that are overly broad, presented in complex or unclear language, attempt to waive liability for intentional acts or gross negligence, or are otherwise unconscionable or contrary to public policy).

57. *See id.* at 615–16.

58. Tesla, Model S Model X Model 3 Model Y New Vehicle Limited Warranty 11 (2021), https://www.tesla.com/sites/default/files/downloads/tesla-new-vehicle-limited-warranty-en-us.pdf. The latest warranty does note, however, that this limitation may not apply "in jurisdictions that do not allow the exclusion or limitation of indirect, direct, special, incidental or consequential damages." *Id.*

B. Identifying the Appropriate Accountable Entity

We currently have established and relatively clear employment and tort law rules regarding who is liable when a repossessing agent has an accident that harms a third-party. If repossessing agents are independent contractors, they are solely liable unless they've breached a nondelegable duty.[59] If they are employees, their employer may also be vicariously liable under respondeat superior. If the accident is due to a vehicle malfunction, the designers, manufacturers, and sellers might also be liable under products liability law. Regardless, the harmed third-party can successfully bring a suit for compensation, which will make them "whole"—or at least cover their monetary damages—and, theoretically, the threat of such suits will incentivize the various defendants to take better care.

But when an autonomously-driven, remotely-repossessed vehicle is involved in an accident that harms a third-party, who pays? In addition to the usual suspects already populating the autonomous vehicle liability literature (the designers,[60] the manufacturers,[61] and the operators[62]), we now add the absent owner and repossessing entity.

---

59. Indeed, secured creditors often hire independent contractors to conduct repossessions just to evade liability. Christopher P. Bennett, *The Buck Stops Here: Peaceable Repossession Is a Nondelegable Duty*, 63 Mo. L. Rev. 785, 785 (1998). However, some states have found that taking care to avoid breaches of the peace is a nondelegable duty, though none of the cases discuss accidents that occur during repossession. *Id.* at 785, 790, 792–93 (reviewing Florida, Missouri, Minnesota, and Texas case law, finding that avoiding breaches of the peace in car repossession to be a nondelegable duty).

While I was not able to find much case law on accidents that occurred during repossessions, there was an Indiana case in which a creditor had hired a fifteen-year-old independent contractor to repossess a vehicle, who then hit another vehicle and injured its occupants. Birrell v. Ind. Auto Sales & Repair, 698 N.E.2d 6 (Ind. Ct. App. 1998). The court held that that creditors are generally not liable for the negligence of an independent contractor, unless the "act to be performed will probably cause injury to others unless due precaution is taken," and declared this to be nondelegable duty. *Id.* at 8–9.

60. *See, e.g.*, Suhrid A. Wadekar, *Autonomous Vehicles: As Machines Learn to Drive, What Must We Learn?*, 27 B.U. J. Sci. & Tech. L. 345, 383 (2021) (stating that "makers" of autonomous vehicle software or makers of components of the software can be held liable when an accident occurs if failure could have been identified and prevented through testing).

61. *See, e.g.*, Rose Angelique Dizon, *Softening the Blow: Finding an Alternative Liability Regime for Fully Autonomous Vehicles*, 63 Ateneo L.J. 1015, 1034 (2019) (stating that autonomous vehicle manufacturers, sellers, and importers are already accepting "blanket" liability for accidents caused by defective vehicles); Mark A. Geistfeld, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation*, 105 Calif. L. Rev. 1611, 1642 (2017) (asserting that when autonomous vehicle manufacturers accept liability for injuries incurred during accidents, any increased costs manufacturers face will be shifted to consumers through increased prices or "decreased product functionality").

62. *See, e.g.*, Dizon, *supra* note 61, at 1028 (noting that some U.S. states impose strict liability on autonomous vehicle operators); *id.* at 1034 (arguing that operators should not be held liable under either a negligence or strict liability standard).

There's a strong argument against holding the owner liable in this scenario. While their payment default was a *but for* cause of the third-party's harm, it was hardly a proximate one. Aside from the fact that a suit would fail the directness and foreseeability tests, the various intervening actors would likely break the causal chain. And, as a practical matter, the individual who has been defaulting on their loans will probably be judgement proof. In short, locating liability with the owner will effectively result in the harmed third-party bearing the costs.

Meanwhile, a variety of public policy considerations favor holding the remote repossessor liable—possibly even strictly liable. They benefit the most[63] from the activity which creates a non-reciprocal risk;[64] they are in control of the vehicle during the course of the remote repossession, with greatest awareness of the timing, environs, and attendant risks; they are best situated to minimize the risk that their employees will employ remote repossession excessively or abusively;[65] and they are both the cheapest cost-avoider and entity best able to spread the costs of accidents.[66]

There may also be reason to hold the designer or manufacturer liable.[67] Assuming no one in the repossessing company intentionally employed the recovered vehicle to order to harm another, many third-party harms will be due to some error made by vehicle itself—accordingly, many of the arguments for repossessor liability would also support products liability claims.[68]

But regardless of the defendant and what type of suit is brought—a claim in negligence, strict liability, or products liability—the claimant will need to prove causation. Given how technology obscures the role of distant decisionmakers, this may be difficult.

---

63. While consumers arguably benefit from the possibility of remote repossession as well, in the form of lower prices or interest rates, see Corkery & Silver-Greenberg, *supra* note 9, it seems likely that the repossessor asymmetrically benefits from the activity.

64. This might be an argument for holding the company strictly liable. *See* George P. Fletcher, *Fairness and Utility in Tort Theory*, 85 Harv. L. Rev. 537, 541–42, 548 (1972) ("If the defendant creates a risk that exceeds those to which he is reciprocally subject, it seems fair to hold him liable for the results of his aberrant indulgence.").

65. *See* Corkery & Silver-Greenberg, *supra* note 9 (detailing allegations of repossessing agents using—or one might say abusing—their ability to remotely deactivate lessor's cars). Liability is also needed in part to ensure that the company itself does not employ remote repossession abusively. *See supra* notes 46–51 and accompanying text.

66. *See* Guido Calabresi, The Cost of Accidents: A Legal and Economic Analysis 26–28 (1970).

67. Mohamed Alawadhi et al., *Review and Analysis of the Importance of Autonomous Vehicles Liability: A Systematic Literature Review*, 11 Int'l J. Sys. Assurance Eng'g & Mgmt. 1227, 1236 (2020) (conducting a literature review and concluding that scholars tend to agree that, as the level of automation increases, manufacturers should bear more liability).

68. *See supra* notes 64–66 and accompanying text.

C. Misdirecting Responsibility

Technology often fosters the inappropriate delegation of responsibility from more temporally- and geographically-remote decision makers to individuals more immediately involved in an accident, regardless of whether the more immediate actors have the ability to minimize the risk of harm.[69] M.C. Elish and Tim Hwang describe this more immediate human as a "liability sponge," who "absorb[s]" the legal liability and moral judgement in a negative incident.[70] In doing so, the more immediate humans "shield a host of remote decisionmakers who contributed to or may even have been better able to prevent the accident: the humans who designed, programmed, manufactured, purchased, or deployed the system."[71]

The tendency to blame the more immediate human for an accident is particularly evident with vehicles with autonomous capabilities. When an autonomous vehicle ran over a pedestrian in 2018, journalists and others were quick to ascribe blame to the human "driver" and to suggest that Uber bore no responsibility.[72] This narrative has persisted, notwithstanding subsequent reports detailing the various software failures that contributed to that accident.[73]

Given this background, there is reason to be concerned that courts evaluating claims by third-party drivers for harms stemming from accidents with remotely repossessed vehicles will inappropriately attribute much of the responsibility for the harm to the most immediate human—here, the harmed third-party—rather than to the repossessing entity, despite the fact that the latter is in putative control of the vehicle.[74]

---

69. *See, e.g.*, Crootof, *IoTorts*, *supra* note 1, at 636 (noting that this occurs both because earlier decisions are obscured by later actions and courts tend to presume that early adopters assume the risks associated with a new technology). As a result, "the human in a highly complex and automated system may become simply a component—accidentally or intentionally—that bears the brunt of the moral and legal responsibilities when the overall system malfunctions." Madeleine Clare Elish, *Moral Crumple Zones: Cautionary Tales in Human Robot Interaction*, Engaging Sci., Tech. & Soc'y 40, 42 (2019).

70. M.C. Elish & Tim Hwang, *Praise the Machine! Punish the Human! The Contradictory History of Accountability in Automated Aviation* 15 (Compar. Stud. in Intelligent Sys., Working Paper #1 V2, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2720477 [https://perma.cc/LJ9U-J9N6]. Elish also termed these individuals "moral crumple zones"—insofar as, by absorbing this liability, crumple zones protect the system: "While the crumple zone in a car is meant to protect the human driver, the moral crumple zone protects the integrity of the technological system, at the expense of the nearest human operator." Elish, *supra* note 69, at 41.

71. Rebecca Crootof, Margot E. Kaminski & W. Nicholson Price II, *Human in the Loop*, 76 Vand. L. Rev. 429, 483 (2023).

72. Elish, *supra* note 69, at 52–53.

73. *Id.* at 53.

74. *Cf.* Ryan Calo, *Robots in American Law* 36 (U. Wash. Sch. L., Legal Studies Research Paper No. 2016-04, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2737598 [https://perma.

D. Recommended Legal Adjustments

Again, permitting corporate self-help may be generally beneficial, and so it may be in the interests of both companies and consumers to permit remote repossessions.[75] Simultaneously, legal shifts may be necessary to minimize abusive and potentially harmful self-help practices.[76] In the interest of promoting public safety during remote repossessions, law can incentivize the repossessing entity to minimize the harms associated with the activity and require them to provide compensation should harm occur.

Specifically, repossessing entities should be prohibited from attempting to contractually shift liability for third-party harms to the owner (and possibly disciplined for including such clauses). Should an accident occur, repossessing entities should be the default defendant, perhaps subject to a strict liability standard, and there should be a rebuttable presumption that the third-party did not contribute to the accident.

First, repossession companies should be prohibited from attempting to use contract law to shift liability for a third-party's harms to the vehicle owner. Not only should indemnification or other liability-shifting clauses in this context be explicitly found to be prima facie unconscionable or otherwise contrary to public policy,[77] courts should consider imposing penalties on companies which include them and lawyers who draft them. As noted above, given that owners are likely to be judgement-proof, shifting liability to them makes little sense—such contractual terms would just "launder injustice" by legitimizing an unfair allocation of liability to the harmed third-party.[78] Additionally, many of the justifications for a limited unconscionability doctrine will not apply in situations where a remote repossession harms a third-party, as the harmed entity cannot be said to have assumed the risk. Nor will the market address the problem; if anything, not imposing liability may foster a market for lemons.[79] Further, the difficulty in preventing

---

cc/M7KB-G5Z2] (observing that judges tend to attribute liability to the person "in the loop" over a robotic system).

75. *See supra* notes 43–45 and accompanying text.

76. *See supra* notes 46–51 and accompanying text.

77. This would not require an excessive legal stretch; under the U.C.C., clauses limiting liability for bodily harms caused by consumer goods are already prima facie unconscionable, U.C.C. § 2-719(3) (Am. L. Inst. & Unif. L. Comm'n 1951), though this is a rebuttable presumption, see Mullan v. Quickie Aircraft Corp., 797 F.2d 845, 852–53 (10th Cir. 1986).

78. Daniel Markovits, *Good Faith as Contract's Core Value*, *in* Philosophical Foundations of Contract Law 272, 291 (Gregory Klass, George Letsas & Prince Saprai eds., 2014).

79. *See* Crootof, *IoTorts*, *supra* note 1, at 638–39 (discussing the unreasonableness of assuming that consumers will make purchases based on an informed consideration of contractual terms, how one technology can shield another from reputational costs (noting that many who know that the first autonomous vehicle to kill a pedestrian was an Uber car, but few know it was a Volvo), how

companies from including unenforceable contractual terms that may discourage meritorious suits also weighs in favor of courts imposing harsh consequences on those who attempt to benefit from unenforceable waivers.[80]

Second, as noted above, there are multiple potential defendants when a remotely-repossessed vehicle harms a third-party. Of these, the remote repossessor is the most appropriate default defendant—and there are many arguments for holding them strictly liable.[81] Should the accident be of the kind that likely was due to a product defect, either the harmed plaintiff or the remote repossessor could file claims (for compensation or contribution, respectively) against the relevant corporate defendants in the products chain.

Finally, to counter the human tendency to blame the most immediate individual involved in an accident when technology obscures the responsibility of remote decisionmakers, there should be a rebuttable presumption that the third-party was not contributorily negligent or comparatively at fault.

The usual analysis would end here, with the conclusion that this combination of legal tweaks would allow repossessing entities to take advantage of the benefits of remote repossession, while encouraging them to do so in as safe a manner as possible.

But is public safety the only interest worth protecting?

III. Preserving Previously-Latent Structural Rights

Harry Surden has argued that structural constraints—which include physical, technological, and other architectural barriers—make certain

---

an IoT industry might be incentivized to collectively downplay potential harms, how consumers become locked in proprietary ecosystems, and why these varied means of evading reputational costs might foster a market for lemons, as consumers cannot judge which devices are safer and so companies who invest in safety cannot recoup those costs).

80. *See* Mathias v. Accor Econ. Lodging, Inc., 347 F.3d 672 (7th Cir. 2003) (noting that large punitive damages can be appropriate, especially when their imposition would address underenforcement). Scholars have proposed various consequences for this practice. *See, e.g.*, Edward K. Cheng et al., *Unenforceable Waivers*, 76 Vand. L. Rev. 571, 594–606 (2023) (suggesting that courts (1) using a non-severability doctrine to invalidate contracts with unenforceable waivers, (2) legislate civil penalties for businesses that use unenforceable waivers, and (3) allow courts to impose punitive damages when a company uses unenforceable waivers); Bailey Kuklin, *On the Knowing Inclusion of Unenforceable Contract and Lease Terms*, 56 U. Cin. L. Rev. 845, 885–95 (1988) (proposing damages in contract and in tort for the inclusion of unenforceable waivers). *But see* Anthony Sebok, *Just Kidding? The Problem of Unenforceable Waivers of Liability*, JOTWELL (Feb. 8, 2023), https://torts.jotwell.com/just-kidding-the-problem-of-unenforceable-waivers-of-liability/ [https://perma.cc/C3KJ-P6RS] (discussing reasons to be skeptical of employing punitive damages for this purpose and suggesting instead that lawyers who approve the inclusion of such terms could be subject to discipline for violating the rules of professional conduct).

81. *See supra* notes 64–66 and accompanying text.

conduct impossible, expensive, or prohibitively costly.[82] These barriers and costs operate as regulatory forces, effectively protecting a non-legalized "right."[83] The fact that these "structural" rights are not codified in law does not mean they are not equally important to those that are; there just hasn't been a need to protect them legally.[84] But should technological developments lessen or remove these structural constraints, non-codified rights are vulnerable to erosion or elimination.[85]

The possibility of remote repossession threatens to undermine various latent structural rights which currently protect consumers from repossessor overreach. These arguably include a right against intrusion, a right to a certain amount of due process or human engagement before a repossession, and a right to be free from foreseeable harms associated with corporate remote interference. This list is likely underinclusive; my aim here is to highlight at least some of the various rights we currently enjoy that might be undermined by adopting a permissive approach to remote repossession.

Recognizing that structural rights are at risk weighs in favor of taking a more proactive regulatory approach to protect our threatened interests.[86] Rather than viewing these moves as legal interventions to create new rights, they are better understood as employing law to preserve long-existing ones.[87]

A. A Right Against Corporate Intrusion

Over twenty years ago, Julie Cohen was concerned that digital rights management technologies would enable remote restrictions or deletions of content in the name of copyright enforcement. She observed, "[c]ourts . . . have not explained, because they have not needed to, whether the judicially-developed 'breach of the peace' standard is *only* designed to minimize the likelihood of physical violence and harm to persons and property, or is (or should be) more broadly concerned with preventing nonconsensual intrusion."[88] There had been no need

82. Surden, *supra* note 30, at 1610–14; *id.* at 1617–18 (acknowledging that his arguments draw on the scholarship of Lawrence Lessig and Ronald Coase).

83. *Id.*

84. *Id.* at 1608 ("[T]here is a societal assumption that certain behaviors are reliably constrained by alternative regulators—such as structure—without need for explicit, legal rules to moderate the conduct.").

85. *Id.* at 1617–20.

86. *Id.* at 1619.

87. *Id.* at 1625–26; *see* Crootof & Ard, *supra* note 31, at 384–86 (reviewing the benefits of a more precautionary approach to regulating new tech-enabled activities).

88. Cohen, *supra* note 5, at 1102 (emphasis in original).

to delineate between the two interests, because we enjoyed a structural right against corporate intrusion.

But Cohen believed this right was under threat. She invited readers to imagine that "a team of high-tech repo men had just used a transporter device to 'beam' your sofa out of your living room and back to the furniture store," to emphasize the intrusive nature of this form of taking.[89] "It would be difficult," she concluded, "for the creditor to convince you that no intrusion had occurred."[90] Ultimately, Cohen argued that the non-violent nature of digital self-help did not render the act any less invasive and that the issues of protecting public safety and protecting a right against intrusion should be disaggregated and considered separately.[91] Absent regulatory action, Cohen feared that "[i]ndividuals' legal entitlement to privacy will simply recede as the technologies of intrusion advance."[92]

Ultimately, this once-structural right against corporate intrusion was not protected and, as Cohen predicted, it "simply recede[d] as the technologies of intrusion advance[d]."[93] Today, companies regularly remotely interfere with purchased property—sometimes by adding or removing features, sometimes by disabling the device—with their right to do so enshrined in terms of service contracts.[94]

Is there is a difference between disabling a device and removing it, such that remote repossession raises new issues? Certainly, in some cases, a disabled device might be rendered useless and effectively "repossessed." As I have observed previously, "[w]ithout the ability to exchange information with a service provider, an IoT smart-home hub is little more than an unusually expensive paperweight."[95] For other IoT devices, however, disabling certain features still leaves the device largely unchanged. An IoT paperweight would still serve its primary purpose absent its connected capabilities![96] It may be that it is worth

89. *Id.* at 1106.

90. *Id.*; *but see* Friedman, *supra* note 50, at 1163 (arguing that Cohen's hypothetically "beamed-out" sofa is much less intrusive than physical repossession, and arguably not "intrusive" or a privacy violation at all).

91. Cohen, *supra* note 5; *see also id.* at 1106 ("[P]hysical harm is not the only kind of harm threatened by unilateral acts of private enforcement.").

92. *Id.* at 1108.

93. *Id.*

94. Crootof, *IoTorts*, *supra* note 1, at 593–610.

95. *Id.* at 600.

96. I was disappointed to find that no enterprising entrepreneur has yet developed an IoT paperweight. However, there are plenty of other examples of IoT devices that can function just fine without their internet-based services, including IoT hairbrushes, water bottles, and fidget spinners.

distinguishing between takings that render an IoT device useless and less-useful, as they might be understood as differently intrusive acts.[97]

In this context, however, there is little distinction between traditional and remote repossession—each results in a similar type of intrusion. If traditional repossession is permitted, there is no strong argument for protecting against intrusive remote repossession. Other structural rights, however, are stronger candidates for codified protection.

B. A Right to Due Process and Human Engagement

To engage in nonconsensual intrusions, a repossessing entity must often involve a state actor. But involving the state takes time, creating a practical constraint on repossession. Insofar as the lender must pay a repossessing company, both state-enabled intrusions and repossessing vehicles in public areas has a cost. Meanwhile, the appearance of a tow truck and the time it takes to hook the contested vehicle up and drive it away provide at least some form of contemporaneous notification that a vehicle is being repossessed. Collectively, these constraints could be understood as a structural right to a certain amount of due process.

Additionally, when a repossession is effectuated by a human agent, the owner has an opportunity for engagement and negotiation.[98] I don't want to overstate this point—repossession agents are hardly famed for their empathic listening skills—but there is at least an opportunity to engage with a person who can exercise discretion and contextual judgement, to offer evidence of an accounting error or show proof of payment, or at the very least verify that the vehicle isn't being hacked and stolen. But remote repossession eliminates this opportunity—this structural right—to contest the taking with a person.

Ford's patent application anticipates that some amount of process will be provided. It details a "multi-step repossession procedure"[99] as an example of how a lending institution might attempt to resolve a default. After non-payment, the institution might send out a first notice and request acknowledgement;[100] if the owner fails to respond, after "a period of time (a week, for example)," it might send out a second notice, with a warning that lack of acknowledgement will initiate

97. *See* Juliet M. Moringiello, *Automating Repossession*, 22 Nev. L.J. 563, 567 (2022) (arguing that "automated disablement is sufficiently different from self-help repossession and face-to-face disablement that it should be addressed in Article 9 of the UCC with restictions tailored to the practice.").

98. *See id.* at 594 (observing that "[s]ome courts appear to value friction in the repossession process by recognizing a right to object to repossession.").

99. Patent Application, *supra* note 11, at 3.

100. *Id.*

repossession proceedings;[101] after "an additional period of time, (another week, for example), and upon failing to receive an acknowledgement," it may "initiate execution of a multi-step repossession procedure."[102] The patent application then describes an increasingly inconvenient progression of remote interferences, including "disabl[ing] a functionality of one or more components of the vehicle,"[103] "activating an audio component in the vehicle,"[104] enforcing a complete or temporally- or geographically-bounded lockout,[105] initiating repossession by having the agency attempt to contact the owner;[106] and making arrangements to impound the vehicle, either through traditional methods or by employing its self-driving features.[107] Should the owner take steps to block such repossession—say, by locking the vehicle within a garage—the vehicle might send information on its location to the police.[108]

Importantly, Ford's patent never suggests that any of this proposed process is legally required. The questions, then, are: What amount and type of process is due before a company can remotely repossess secured property? What initial contractual language and disclosure is necessary? Post-default, what notices and warnings are required? How much time must elapse before a company can employ remote repossession? Must there be a contemporaneous warning? Must it take any particular form? Is there a right to contest the repossession? Separately, is there a right to engage with a human agent? How would these requirements be operationalized? (These latter questions regarding contestation and human engagement are even more pressing if the decision to engage in remote repossession itself is automated.)[109]

Connecticut has modeled one approach to answering these questions. It prohibits electronic self-help, unless (1) the owner has agreed to a separate contractual term authorizing the company to use electronic self-help in the original agreement, and (2) at least fifteen days before engaging in electronic self-help, the secured party gives notice that it will do so, explains the nature of the breach, and provides a human representative's contact information.[110] State or federal statutes might

101. *Id.*
102. *Id.*
103. *Id.*
104. *Id.* at 4.
105. Patent Application, *supra* note 11.
106. *Id.*
107. *Id.* at 4–5.
108. *Id.* at 5.
109. *See generally* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008); Margot E. Kaminski & Jennifer M. Urban, *The Right to Contest AI*, 121 COLUM. L. REV. 1957 (2021).
110. CONN. GEN. STAT. § 42a-9-609 (2012).

similarly codify due process rights, either for remote repossessions or for remote interferences more generally. Indeed, many of the issues associated with remote repossession implicate rights applicable to all corporate remote interferences.

C. A Right to Protection from Foreseeable Risks of Harm

Recall the introductory hypo, which catalogued potential foreseeable harms to the owner that might occur with remote repossession: conversion, kidnapping, the killing of a pet, the destruction of personal property, or the destruction of the disputed property itself.[111] How might law minimize the likelihood of these harms?

Working within the boundaries of repossession law, one option would be to frame these all as prohibited breaches of the peace.[112] For example, in *MBank El Paso N.A. v. Sanchez*, the Texas Supreme Court found the service creditor liable for having breached the peace after its contractor towed the car to the repossession yard and left it there—with the owner in it.[113] An autonomous vehicle that does the same thing to the owner's child should equally constitute a breach of the peace. Similar precedents could be found for situations where the repossessing entity harmed a pet, other personal property, or the disputed property itself.[114]

Simply using analogy to stretch the concept of a "breach of the peace" to encompass foreseeable harms has the appeal of minimalism—but this approach would forego the opportunity to protect the rights of consumers more broadly.

I instead recommend explicitly protecting our current structural right to be free from companies interfering with our property in ways that

111. *See supra* notes 18–20 and accompanying text.

112. Alternatively, remote repossessors could be analogized to landlords, rather than traditional car repossessors, given that landlords have a greater affirmative duty to protect the safety of their tenants. Crootof, *Io Torts*, *supra* note 1, at 630. However, this duty tends to be activated when (1) there was no contractual breach and (2) the tenant's harm was due to a criminal act enabled by the landlord's choices—neither of which would be relevant here. *Id.* at 630–31; *see also* Carl Campanile, *Proposed Law Hopes to Help Trapped Pets After Evictions*, N.Y. Post (Sept. 26, 2017, 4:24 PM), https://nypost.com/2017/09/26/proposed-law-hopes-to-helptrapped-pets-after-evictions (noting that New York landlords do not have an obligation to check for the presence of pets before changing a delinquent tenant's locks).

113. Bennett, *supra* note 59, at 792 (citing MBank El Paso, N.A. v. Sanchez, 836 S.W.2d 151, 153 (Tex. 1992)).

114. *See id.* at 790 (noting that both Missouri and Minnesota case law hold secured creditors liable for breaching the peace when contractors physically injured the car owner during repossession); *see also id.* at 793 (describing a Florida case where the service creditor was held liable for breaching the peace when a repossessing contractor intentionally damaged the car they were meant to repossess).

create a foreseeable risk of bodily harm or property damage.[115] Doing so would permit companies to continue to engage in remote repossessions, foreground the safety concern that animates the prohibition on breaches of the peace in the first place, and establish precedent for a broader protection of a once-structural right. New legal protections could take various forms, such as an implied warranty of reasonable interference, an interference defect (under products liability law), and an IoT-specific fiduciary duty.[116]

Regardless of how it manifests, it is a once-structural right now at risk of erosion that is worth affirmatively protecting now, before IoT technologies' design and social uses have stabilized.[117] One might assume that we don't need a new duty—negligence already protects us from unreasonable actions. But many consumer rights are grounded on consumer expectations about what corporate action is "reasonable," and so the right to be free from foreseeable harms associated with corporate remote interference extends beyond the remote repossession context—a decision to protect this structural right, now, will determine our future expectations about what precautions are reasonable and, by extension, IoT companies' responsibilities. As I noted previously, while discussing corporate remote interference generally:

> Once social norms are established, they affect how legal questions are evaluated. If it is generally assumed that IoT companies have an obligation to avoid causing foreseeable harm, courts and other legal actors will be more likely to strike exculpatory clauses as unconscionable, find a design defect in cases regarding harms resulting from

115. Crootof, *IoTorts*, *supra* note 1, at 649 (arguing for the recognition of a relational duty "to only employ remote interference when it is reasonably safe to do so").

Additionally or alternatively, the structural right at risk could be conceived even more broadly, as the right to be free from any type of foreseeable harm associated with remote interference, see *id.* at 606–08, or even as the right to be free from remote interference at all. While I argue for the legal protection of a more narrow right, that choice reflects the word limit on a symposium contribution more than my considered decision against arguing for broader consumer protections.

116. *Id.* at 652–58. As relevant in the case study discussed here, the first two approaches would better protect bystanders. With regard to the warranty approach, the U.C.C. extends express and implied warranties to third-parties "who may reasonably be expected to use, consume or be affected by" a product. U.C.C. § 2-318 (Am. L. Inst. & Unif. L. Comm'n 1951); *see also* Jennifer Camero, *Two Too Many: Third Party Beneficiaries of Warranties Under the Uniform Commercial Code*, 86 St. John's L. Rev. 1, 21–23 (2012) (noting that two of the three U.C.C. categories of protected bystanders have no privity requirement and that, while the third is limited to a buyer's family or guests, some courts have applied it to bystanders). Meanwhile, under products liability law, manufacturers owe a duty to anticipate and prevent likely harms to bystanders. *See* MacPherson v. Buick Motor Co., 111 N.E. 1050, 1053 (N.Y. 1916). A fiduciary obligation, in contrast, would only be owed to the consumer in privity with the company.

117. *See* Gaia Bernstein, *When Technologies Are Still New: Windows of Opportunity for Privacy Protection*, 51 Vill. L. Rev. 921, 941–43 (2006).

> remote interference, or articulate a duty for the purpose of a negligence analysis. If not, they will not.[118]

As we purchase more and more internet-connected devices, we are ceding more and more control over our own goods. Car companies are pushing advertisements to owner's internal displays;[119] collecting and sharing personal information;[120] and employing over-the-air updates to eliminate or require consumers to pay subscriptions for what once were built-in features, like remote car starters[121] or adaptive cruise control.[122] But there isn't anything special about car companies; IoT companies are continuously meddling with 'your' products.[123] Establishing a right to free from foreseeable harms associated with corporate remote interference would draw a line in the sand regarding what IoT companies can do. It may not be the perfect place to draw that line—but it would be an already-overdue start.

Conclusion

Recognizing that a technological development has shifted the regulatory equilibrium raises overlapping questions:[124] How does existing law apply? Is the new state of affairs normatively preferable? If not, should law be used to adjust it, to achieve a different balance among the

---

118. Crootof, *IoTorts*, *supra* note 1, at 642.

119. Ford—always on the cutting edge!—has patented a system that uses a vehicle's cameras to detect billboards and post them on a car's infotainment display. *See* Andrew Liszewski, *Get Ready for In-Car Ads*, Gizmodo (May 13, 2021), https://gizmodo.com/get-ready-for-in-car-ads-1846888390 [https://perma.cc/L4EG-APG9].

120. *See* Jon Keegan & Alfred Ng, *Who Is Collecting Data From Your Car?*, The Markup (July 27, 2022), https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car [https://perma.cc/3TJS-X3PP].

121. *See* Tim De Chant, *Toyota Owners Have to Pay $8/mo to Keep Using Their Key Fob for Remote Start*, Ars Technica (Dec. 13, 2021), https://arstechnica.com/cars/2021/12/toyota-owners-have-to-pay-8-mo-to-keep-using-their-key-fob-for-remote-start/.

122. *See* Joseph Cox, *BMW Wants to Charge for Heated Seats. These Grey Market Hackers Will Fix That*, Motherboard (July 19, 2022), https://www.vice.com/en/article/7k8bv9/bmw-wants-to-charge-for-heated-seats-these-grey-market-hackers-will-fix-that [https://perma.cc/U2QN-BDZ7].

123. *E.g.*, Alfred Ng, *The Privacy Loophole in Your Doorbell*, Politico (Mar. 7, 2023), https://www.politico.com/news/2023/03/07/privacy-loophole-ring-doorbell-00084979 [https://perma.cc/27LG-QV3B] (recounting how a local police department obtained a warrant to all footage on an individual's home security cameras—including footage from *inside* his home—for an investigation into his *neighbor's* activities); Ben Ellery & James Beal, *Roald Dahl eBooks 'Force Censored Versions on Readers' Despite Backlash*, The Times (Feb. 25, 2023), https://www.thetimes.co.uk/article/roald-dahl-collection-books-changes-text-puffin-uk-2023-rm2622vl0 [https://perma.cc/3X3V-B3M8] (discussing how companies are remotely altering text in already-purchased e-books to reflect modern norms); Brad Stone, *Amazon Erases Orwell Books from Kindle*, N.Y. Times (July 17, 2009), https://www.nytimes.com/2009/07/18/ technology/companies/18amazon.html (reporting on how Amazon remotely deleted already-purchased e-books).

124. Crootof & Ard, *supra* note 31, at 356–79.

regulatory modalities? And if adjustment is needed, which institution is best suited to make it?[125]

This Article showcases the benefits of a techlaw approach. While different technologies raise different specific regulatory questions, technological change tends to present familiar types of legal uncertainties that are resolved in familiar ways. By drawing on insights about the interaction of technology and law from varied case studies and legal fields, a techlaw approach fosters a more structured, comprehensive, and expedited analysis of these uncertainties and how to resolve them.

Following the methodology BJ Ard and I have developed, one first identifies which type of legal uncertainty is at issue.[126] An "application uncertainty" arises when there is a question as to whether or how existing law applies to a new technology, actor, or activity, while a "normative uncertainty" arises when there is a question of whether existing law accomplishes its intended purpose. Disentangling the questions of how law is likely to evolve and how it should evolve enables a more nuanced analysis. Here, for example, I have considered application and normative questions both separately and in light of the other, which in turn enabled a more nuanced approach to resolving both.

Second, one considers whether a more permissive or precautionary regulatory stance is more appropriate.[127] A permissive approach essentially adopts a presumption against regulation and places the burden of rebutting that presumption on those who would suffer from the use or proliferation of the technology. In contrast, a more precautionary, regulation-friendly stance places the burden of compliance or contesting overly-burdensome regulations on those likely to benefit from the use or proliferation of a technology.

A number of factors favor taking a proactive approach to regulating remote repossessions. The harms of remote repossessions will tend to fall on a diffuse class (the poor, the young, and consumers generally) which have relatively little wealth, political clout, or ability to organize effectively for change. Meanwhile, the benefits of remote repossession will largely accrue to car companies, a concentrated, well-resourced, and politically powerful group.[128] Accordingly, public choice theory and a general awareness of power relations both weigh in favor of a

125. BJ Ard, *Making Sense of Legal Disruption*, 2022 Wis. L. Rev. Forward 42, 49–51 (discussing the import of considering relative institutional authority, competence, and legitimacy when considering which entity is best suited to resolve techlaw uncertainties).

126. Crootof & Ard, *supra* note 31, at 350, 356–79.

127. *Id.* at 350, 379–87.

128. *E.g.*, Alexander Sammon, *Want to Stare Into the Republican Soul in 2023?*, Slate (May 30, 2023), https://slate.com/news-and-politics/2023/05/rich-republicans-party-car-dealers-2024-desantis.html.

precautionary approach, as regulatory overreach is more likely to be effectively challenged than a failure to regulate sufficiently.

A separate argument for a more proactive approach is the fact that remote repossession risks a number of structural rights, which will only be protected if they are identified and codified as legal rights. A more permissive approach tends to delegate evolutionary power to legal interpreters, while a proactive approach vests power in law makers. Given courts' general reluctance to appear to be creating law and stepping outside of their institutional roles, a precautionary approach involving the legislature is more likely to vindicate and protect these previously implicit rights.

The third step of the methodology requires evaluating the relative utility of different legal responses—such as how best to extend the law or whether and what new law should be created. In doing so, the methodology fosters a more thorough analysis, as it highlights techlaw considerations that might not otherwise have been taken into account. For example, with regard to the question of when to stretch extant law to address a new scenario, an awareness of common traps alerts us to how technology can complicate traditional doctrinal analyses. Here, technology's tendency to misdirect responsibility from those most able to avoid an accident to those more proximately involved is highly relevant. A techlaw approach also highlights considerations that the usual process of legal evolution might miss, such as the question of whether a structural right is being undermined, which in this context weighs in favor of also creating new law.

This brief application of a techlaw methodology to the question of how best to regulate remote repossession clarifies why a proactive approach is preferable.[129] Given what is at stake—our futures as potential defaulting owners, as possibly harmed third-parties, and as consumers who must increasingly rely on corporations to take reasonable care when engaging in remote interference—we need every advantage we can get.

129. This is far from a comprehensive techlaw analysis of regulating remote repossessions. I did not, for example, evaluate the relative benefits of regulating the technology, the actor, or the activity, Crootof & Ard, *supra* note 31, at 357–59; whether to regulate directly, via law, or indirectly, by using law to shift markets, norms, or technological architectures, see LAWRENCE LESSIG, CODE: VERSION 2.0 (2006); the most appropriate analogies for extending the law and their respective risks, Crootof & Ard, *supra* note 31, at 387–98; the scope, form, or implementation of new regulations, *id.* at 401–05, nor how tech-neutral or tech-specific they should be, *id.* at 405–13; or which (if any) institution had the requisite authority, competence, and legitimacy to regulate remote repossessions, *id.* at 413; *see also* Ard, *supra* note 125. Still, even this partial application yields helpful insights.