Michigan Technology Law Review

Article 5

2021

NHTSA Up in the Clouds: The Formal Recall Process & Over-the-Air Software Updates

Emma Himes
University of Michigan Law School

NHTSA UP IN THE CLOUDS: THE FORMAL RECALL PROCESS & OVER-THE-AIR SOFTWARE UPDATES

Emma Himes *

ABSTRACT

Software updates are pushed to vehicles "over-the-air" (OTA) with increasing frequency as they reduce costs of visiting dealerships and auto shops to receive maintenance. These updates, pushed from the cloud, have been used to remedy safety defects in vehicles and improve software controlling all aspects of vehicles from steering to rearview mirrors. Remedies of vehicle safety defects are overseen by the National Highway Traffic Safety Administration (NHTSA); however, because many OTA software updates do not remedy issues officially deemed safety defects, they are pushed straight from the manufacturer to drivers with little government oversight or transparency. NHTSA's recall process was designed in 1966 to remedy safety defects in vehicles, resulting in a process which is now outdated for modern vehicles running on software. NHTSA has acknowledged the increased use of OTA software updates and prescribed OTA remedies for safety defects, but the current framework leaves NHTSA unable to oversee the rapid output of OTA software updates pushed by auto manufacturers. Without updating the current recall process for software related updates to vehicles, and specifically over-the-air software updates, NHTSA's ability to oversee vehicle safety may decrease and the recall process may grow obsolete as the issues facing vehicles today have changed since Congress defined what constitutes a safety defect.

* J.D. Candidate, Class of 2022, University of Michigan Law School. I would like to thank Professor Emily Frascaroli for introducing me to this topic in the course Legal Issues Surrounding Autonomous Vehicles. I would also like to thank the *MTLR* team for their thoughtful edits.

TABLE OF CONTENTS

INTRODUCTION

Today, the majority of new cars on the road are controlled by software instead of mechanical parts as a result of vehicles becoming "smarter." As the number of lines of code within a single vehicle continues to increase, there has also been an increase in software related recalls of vehicles.[1] Over-the-air ("OTA") software updates have become a common avenue to remedy software related safety defects within the formal recall process overseen by the National Highway Traffic Safety Administration ("NHTSA") due to the lower cost and greater ease of OTA updates. However, OTA software updates do not fit well within the established recall framework, increasing the need for a new recall process which delivers remedies for modern, connected, automated, and autonomous vehicles.

Part I of this note describes NHTSA's current recall process and how it is unable to address software or cybersecurity related safety issues. Part II describes how NHTSA has addressed OTA software updates. Part III describes the increase in OTA software updates and the speed at which manufacturers are releasing software updates. Part IV proposes that NHTSA create a standardized and transparent approach for OTA software updates by modifying the recall process to specifically address remedies for software related safety issues and to create a database documenting all over-the-air

1. Albert Lilly, *The Current State of Automotive Software Related Recalls*, SIBROS (Apr. 22, 2020), https://www.sibros.tech/post/the-current-state-of-automotive-software-related-recalls (citing a "sharp rise in the volume of software related recalls" in the United States according to the National Highway Traffic Safety Association's recall database, with recalls tripling between 2009 and 2019).

updates pushed to vehicles. This note concludes by reiterating that the recall process must adapt to increase transparency from manufacturers and enable NHTSA's recall process to fit vehicles of the present and future.

I. NHTSA RECALL POLICY

NHTSA, which is part of the Department of Transportation ("DOT"), is the agency responsible for "delivering vehicle safety standards," "notifying automobile manufacturers that have safety associated issues, or do not satisfy the Federal safety standards," and "supervising the manufacturer's remedial action to guarantee that the recall drive process has been completed successfully."[2] A recall is issued when NHTSA determines that a vehicle creates an unreasonable safety risk, fails to meet minimum safety standards, or the manufacturer discovers a safety defect.[3] If a defect is discovered, the manufacturer must notify NHTSA, vehicle or equipment owners, dealers, and distributors by first-class mail and remedy the problem within a reasonable time.[4]

The current recall process, codified in the National Traffic and Motor Vehicle Safety Act, 49 U.S.C. §§ 30118-30120 (hereinafter the "Safety Act"), was passed in 1966 to create and administer new safety standards for motor vehicles and road traffic safety.[5] The Safety Act, signed by President Lyndon Johnson, answered a national cry in response to Ralph Nader's book *Unsafe At Any Speed*, which accused Chevrolet of cutting costs at the risk of driver safety by building the engine into the back of the Chevy Corvair.[6] While the Safety Act created a recall process which protected consumers from vehicles like the Corvair, the recall process must now adapt to increase transparency and oversight of OTA software updates for modern vehicles.

In 2000, the Transportation Recall Enhancement, Accountability, and Documentation ("TREAD") Act was passed to enhance the existing recall policy.[7] It requires "vehicle and equipment manufacturers to report periodically to NHTSA on a wide variety of information that could indicate

2. Subir Halder, Amrita Ghosal & Mauro Conti, *Secure OTA Software Updates in Connected Vehicles: A Survey*, COMPUT. NETWORKS, June 2020, at 1, 6, https://www.sciencedirect.com/science/article/pii/S1389128619314963.

3. *Safety Issues & Recalls*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., https://www.nhtsa.gov/recalls (last visited Nov. 24, 2021).

4. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., MOTOR VEHICLE SAFETY DEFECTS AND RECALLS: WHAT EVERY VEHICLE OWNER SHOULD KNOW 1, 11 (2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/14218-mvsdefectsandrecalls_041619-v2-tag.pdf.

5. National Traffic and Motor Safety Act, 49 U.S.C. §§ 30118–30120 (2012).

6. Christopher Jensen, *50 Years Ago, 'Unsafe at Any Speed' Shook the Auto World*, N.Y. TIMES (Nov. 26, 2015), https://www.nytimes.com/2015/11/27/automobiles/50-years-ago-unsafe-at-any-speed-shook-the-auto-world.html.

7. Transportation Recall Enhancement, Accountability, and Documentation (TREAD) Act, Pub. L. No. 106-414, 114 Stat. 1800 (2000).

the existence of a potential safety defect and to advise NHTSA of foreign safety recalls and other safety campaigns."[8] While this act serves goals of transparency and functionality broadly, this most recent language update to the recall process does not address software defects, cybersecurity issues, or OTA remedies.

A. *An Antiquated Recall Process*

When the drafters of the National Traffic and Motor Safety Act of 1966 designed the recall process, they addressed specific concerns related to physical parts of cars like construction, components, and materials that could contribute to causing a deadly accident.[9] The Federal Motor Vehicle Safety Standards often focus on brakes, tires, lighting, air bags, seat belts, car seats and booster seats, energy absorbing steering columns, and motorcycle helmets.[10] Today, software impacts many of these components in vehicles, requiring an adapted recall process.

Each OTA software update pushed to a vehicle makes some change to the millions of lines of code in a vehicle.[11] Improvements include updates varying from improvements to assisted driving software or the functionality of a vehicle's display screen impacting rearview mirrors and cameras.[12] Updates may also patch a security vulnerability.[13] While all updates are pushed by manufacturers with the intention of improving a vehicle, an update may leave a bug in the vehicle's software that did not exist at the time of sale or prior to an OTA software update. A bug may be minor and have no effect on the operation of the vehicle, but there is also a possibility that an OTA update could create a safety defect that was not previously present in the vehicle. The OTA update could also make the vehicle vulnerable to a new cybersecurity risk. The risk of a safety or security issue being created by an OTA update increases as the quantity of updates being pushed increases, because there is less time spent testing each update for

8. *The Implementation of the TREAD Act: One Year Later: Hearing on H.R. 5164 Before the Subcomm. on Com., Trade & Consumer Prot. of the H. Comm. on Energy & Com.*, 107th Cong. 13 (2002) (statement of Honorable Jeffery W. Runge, M.D., Administrator, National Highway Traffic Safety Administration).

9. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 4, at 2.

10. *See id.*

11. Omkar Panse, *The Changing Landscape for Over-the-Air (OTA) Updates*, KPIT https://www.kpit.com/insights/changing-landscape-for-over-the-air-ota-updates (last visited Nov. 24, 2021).

12. *Statement by American Honda Regarding Four Automobile Recalls*, HONDA NEWS (Aug. 4, 2020), https://hondanews.com/en-US/honda-corporate/releases/release-6f203606fa66618d91f0658cf700277c-statement-by-american-honda-regarding-four-automobile-recalls.

13. John Tuttle, *Protecting Connected Cars' Over-the-Air Software Updates*, WARDSAUTO (July 21, 2020), https://www.wardsauto.com/vehicles/protecting-connected-cars-over-air-software-updates.

security vulnerabilities or impacts on the vehicle's software as a whole. Hundreds of OTA updates are being pushed by automotive companies per year, and some of the updates are pushed only days after identifying a problem.[14] For example, Tesla pushed an OTA update within days of Consumer Reports reporting an overly long stopping distance in 2018, reducing the braking distance by 20 feet.[15] The OTA update was pushed so recently after discovery of the problem that some doubted the thoroughness of testing the new software.[16]

Massachusetts Senator Ed Markey stated in 2020 that NHTSA is "neglecting to oversee and keep the public informed about over-the-air (OTA) software updates designed to fix safety defects in cars without a physical recall."[17] In response to criticism, NHTSA updated their Cybersecurity Practices for the Safety of Modern Vehicles, creating a legal basis for OTA software updates to on-board vehicle software.[18] Section 9.8 relating to OTA software updates states:

> Manufacturers that design-in and offer OTA software update capability on their vehicles should:
>
> > [T.22] Maintain the integrity of OTA updates, update servers, the transmission mechanism and the updating process in general.
> >
> > [T.23] Take into account, when designing security measures, the risks associated with compromised servers, insider threats, men-in-the-middle attacks, and protocol vulnerabilities.[19]

While this official acknowledgement of OTA updates by NHTSA is a step in the right direction, the recommendation does little where many, if not all, manufacturers already make efforts to maintain the integrity of OTA updates and account for cybersecurity risks.[20] Nor do the practices explain

---

14. *See* Kristof Horvath, *How Over-The-Air Updates Are Turning the Auto Industry Upside Down*, INTLAND SOFTWARE (Oct. 20, 2020), https://content.intland.com/blog/how-over-the-air-updates-are-turning-the-auto-industry-upside-down.

15. *Id*.

16. *Id*.

17. *Senators Markey & Blumenthal Demand NHTSA Proactively Address the Cyber Risks of Internet-Connected Cars*, ED MARKEY U.S. SENATOR FOR MASS. (June 11, 2020), https://www.markey.senate.gov/news/press-releases/senators-markey-and-blumenthal-demand-nhtsa-proactively-address-the-cyber-risks-of-internet-connected-cars.

18. Ericka Pingol, *NHTSA: Cybersecurity Best Practice of Modern Vehicles*, TREND MICRO (Jan. 25, 2021), https://www.trendmicro.com/us/iot-security/news/6643.

19. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., CYBERSECURITY BEST PRACTICES FOR THE SAFETY OF MODERN VEHICLES 17 (2020), https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/vehicle_cybersecurity_best_practices_01072021.pdf.

20. *See generally* Scooter Doll, *Over-the-Air Updates: How Does Each EV Automaker Compare?*, ELECTREK (Oct. 1, 2021, 1:00 AM), https://electrek.co/2021/10/01/over-the-air-updates-how-does-each-ev-

how NHTSA monitors and responds to OTA software updates for connected cars. NHTSA's response is insufficient in light of robust changes in the automotive space.

Software-related safety defects will become increasingly important as cars become smarter, which will require automotive original equipment manufacturers ("OEMs") to push OTA software updates to fix software glitches and security vulnerabilities. NHTSA's recall process is lacking a toolkit to both identify and remedy software related issues and safety defects in vehicles. In order to improve consumer transparency regarding safety related software updates to vehicles and avoid the delays of the traditional recall process, the regulatory framework for automotive recalls must acknowledge and adapt to allow for greater efficiency and transparency in safety remedies. This note proposes that NHTSA standardize the OTA process by requiring reporting of OTA updates pushed to vehicles and creating a database documenting those updates. This will aid NHTSA in ensuring consumers are protected as the number of vehicles with OTA capabilities on the road increases. A database of updates may also incentivize manufacturers to complete more thorough testing of updates prior to pushing them to drivers.

Further, connecting vehicles to the cloud introduces cybersecurity risks which must be addressed by NHTSA, especially in relation to OTA updates. NHTSA policies and rules must address the concern that "internet-connected vehicles can potentially be hacked and remotely controlled by malicious actors, creating risks not only to the lives of car drivers and passengers, but also to pedestrians and property along the road."[21] NHTSA's recall framework for internet-connected cars must include the infrastructure to responds to OTA cybersecurity risks.

1. Are Software Glitches Safety Defects?

One of the most critical problems with using the 1966 recall policy for OTA updates is that many software related issues are not officially deemed "safety defects" under the Safety Act. For example, in 2019 a Tesla driver fatally crashed into the side of a truck while the Tesla's semiautonomous Autopilot technology was engaged.[22] Following investigations by both NHTSA and Tesla, Tesla vehicles on the road received an OTA software

automaker-compare/#h-over-the-air-capabilities-by-ev-manufacturer (explaining how manufacturers are using OTA updates in order to keep vehicle software up to date, including manufacturers Audi, BMW, Fiat Chrysler, Ford, General Motors, Honda, Hyundai, Jaguar/Land Rover, Mercedes-Benz, Nissan, Porsche, Tesla, Toyota, Volkswagen, and Volvo).

21. *See Senators Markey & Blumenthal Demand NHTSA Proactively Address the Cyber Risks of Internet-Connected Cars*, *supra* note 17.

22. Katie Burke, *Over-the-Air Updates May Alter NHTSA Recall Policy*, AUTO. NEWS (Jan. 23, 2017), https://www.autonews.com/article/20170123/OEM11/301239815/over-the-air-updates-may-alter-nhtsa-recall-policy.

update which forces drivers to keep their hands on the wheel the majority of the time while driving in an attempt to eliminate the cause of the deadly crash.[23] This OTA software update, which "included increased use of radar sensors and a 'strike out' feature that would disable Autopilot if drivers took their hands off the wheel too many times," occurred outside of the traditional recall process as no safety defect was found by NHTSA's Office of Defects Investigation ("ODA").[24] Had NHTSA's ODA identified a defect in the software, NHTSA's spokesman Bryan Thomas stated that Tesla would have been required to follow the recall process prior to pushing an OTA software update.[25] Regardless, the current recall framework does not speak to OTA software updates for safety defects or other safety issues in software which are not officially deemed "safety defects" yet pose a fatal risk.

Since this fatal occurrence, NHTSA has slowly began making progress in the realm of OTA updates. In 2021, NHTSA published multiple recall announcements allowing for defects to be remedied by OTA software updates, which has been deemed as setting a "new precedent for what constitutes an automotive recall."[26] However, NHTSA overstates the effectiveness of the antiquated recall policy in monitoring software related safety risks and documenting OTA updates.

The formal recall process fails to fit modern vehicles and remedies. For example, in 2020, Tesla pushed an OTA update to recalled Model Y vehicles to remedy a trailer brake light failure caused by a software error.[27] This was deemed a safety defect as Federal Motor Vehicle Safety Standard number 108, "Lamps, Reflective Devices, and Associated Equipment," requires illumination of trailer brake lights.[28] Tesla remedied the firmware with an OTA update available on September 23, 2020, and followed the requirements of the formal recall process, including mailing owner notification letters in accordance with 49 C.F.R. § 577.7.[29]

Comparing these two Tesla cases, a fatal Autopilot crash which was not deemed a safety defect and a brake light failure which was deemed a safety defect, reveals that the current recall process is inadequately designed for vehicles running on software and connected to the internet, even where a software design results in a fatality. In September 2021, NHTSA began

---

23. *Id.*
24. *Id.*
25. *Id.*
26. Alex Brisbourne, *Tesla's Over-the-Air Fix: Best Example Yet of the Internet of Things?*, WIRED, https://www.wired.com/insights/2014/02/teslas-air-fix-best-example-yet-internet-things (last visited Nov. 24, 2021).
27. Fred Lambert, *Tesla Issues Model Y Recall Over Trailer Brake Light Failure, But the Fix Is an OTA Software Update*, ELECTREK (Oct. 19, 2020, 4:18 PM), https://electrek.co/2020/10/19/tesla-issues-model-y-recall-trailer-brake-light-failure-ota-software-update.
28. *Id.*
29. *Id.*

investigating an OTA update pushed to Tesla vehicles which contained an improvement to the vehicle's Emergency Light Detection system.[30] Tesla did not file a recall notice with NHTSA, and NHTSA contacted Tesla's Director of Field Quality reiterating that "[a]ny manufacturer issuing an over-the-air update that mitigates a defect that poses an unreasonable risk to motor vehicle safety is required to timely file an accompanying recall notice to NHTSA."[31] If NHTSA determines that there was a safety defect and announces a recall, this may demonstrate that NHTSA is trying to adapt the current recall framework for software issues and OTA updates in addition to demonstrating that they will hold manufacturers pushing OTA updates accountable.

2. Are Cybersecurity Failures Safety Defects?

What NHTSA deems officially a "safety defect" differs from what a consumer or manufacturer may consider unsafe. For example, a hacked vehicle may be found to have no safety defect while objectively posing a safety risk to the public. In 2015, a group of researchers "commandeered a Jeep Cherokee's engine and brakes remotely from a laptop" to spotlight the hacking vulnerabilities of connected cars.[32] This event generated fear, but auto manufacturers responded by differentiating this event from that of a safety defect.[33] In fact, Mitch Bainwol, head of the Alliance of Automobile Manufacturers which represents a dozen auto companies including both General Motors and Toyota said, "[w]e would reject a blanket assertion that a cyber risk is a defect . . . . There is a difference between a routine function of a vehicle where a problem arises and the intervention of a bad actor."[34] Senator Ed Markey disagreed, stating that "[a] cybersecurity vulnerability is a safety defect in the same way an exploding air bag or a malfunctioning ignition switch is a safety defect."[35]

In light of the Jeep hijacking, auto manufacturers with similar security vulnerabilities to Jeep, including Fiat Chrysler, released software updates blocking commands from unauthorized hackers.[36] Fiat Chrysler asserted that the security gap was not a defect, but NHTSA responded in a letter that the gap was "a defect causing an unreasonable safety risk."[37] Regardless,

30. Rob Stumpf, *Feds Order Tesla to Justify OTA Autopilot Updates Instead of Recalling Cars*, DRIVE (Oct. 13, 2021), https://www.thedrive.com/tech/42736/feds-order-tesla-to-justify-ota-updates-instead-of-recalling-cars.

31. *Id.*

32. Mike Spector, *Is a Hacked Vehicle Also Defective?*, WALL ST. J. (Aug. 24, 2015), https://www.wsj.com/articles/is-a-hacked-vehicle-also-defective-1440457334.

33. *Id.*

34. *Id.*

35. *Id.*

36. *Id.*

37. *Id.*

NHTSA never issued a formal classification of the problem as a safety defect,[38] leaving open the question of whether a cybersecurity hack may officially be deemed a "safety defect."

Under the Safety Act, for NHTSA to challenge Fiat Chrysler's assertion, NHTSA "would need to show a vehicle's cybersecurity vulnerability made it far more susceptible to hacking than other cars," explained a former senior NHTSA enforcement lawyer Allan Kam.[39] Not only may it be difficult to prove that the cybersecurity of a vehicle is sufficiently lacking compared to other vehicles, but the process of proving so may also "alert [an] otherwise unaware hacker" to a cybersecurity gap.[40] However, a "quick over-the-air fix could ameliorate that risk."[41] Based upon this reasoning, OTA updates are the best way to quickly fix cybersecurity risks, yet they are not adequately overseen by the NHTSA recall framework.

Instead of taking steps to adapt the recall framework, NHTSA instead pushed responsibility to drivers to protect themselves from cyber threats. On March 17, 2016, NHTSA released a Public Service Announcement stating that "not all hacking incidents may result in a risk to safety" and advised drivers, *not manufacturers*, to take precautions such as keeping software up to date and using caution when connecting third-party devices.[42] This PSA assumes that drivers stay up to date with NHTSA communications, when manufacturers and dealers would likely better convey this information. Additionally, this shifts the burden to drivers when the agency, manufacturers, and dealers are likely to have a more comprehensive understanding of the vehicles, safety issues, and software updates.

Despite this warning to drivers, NHTSA has made efforts to increase the cybersecurity of connected vehicles. In April 2016, NHTSA published a bulletin identifying best practices for ensuring that car manufacturers of emerging technologies comply with the Safety Act and explaining that NHTSA will weigh the following factors when determining whether a cybersecurity vulnerability poses an unreasonable risk to safety:

> (i) The amount of time elapsed since the vulnerability was discovered (*e.g.*, less than one day, three months, or more than six months);

38. *Id.* (explaining that Fiat Chrysler agreed to recall the vehicle while asserting that the cyber risk is not a safety defect, to which NHTSA disagreed in a letter but never required Fiat Chrysler to "classify the problem as a defect").

39. *Id.*

40. *Id.*

41. *Id.*

42. FED. BUREAU OF INVESTIGATION, ALERT NO. I-031716-PSA, PUBLIC SERVICE ANNOUNCEMENT: MOTOR VEHICLES INCREASINGLY VULNERABLE TO REMOTE EXPLOITS (Mar. 17, 2016), https://www.ic3.gov/Media/Y2016/PSA160317.

(ii) the level of expertise needed to exploit the vulnerability (*e.g.*, whether a layman can exploit the vulnerability or whether it takes experts to do so);

(iii) the accessibility of knowledge of the underlying system (*e.g.*, whether how the system works is public knowledge or whether it is sensitive and restricted);

(iv) the necessary window of opportunity to exploit the vulnerability (*e.g.*, an unlimited window or a verry narrow window); and,

(v) the level of equipment needed to exploit the vulnerability (*e.g.*, standard or highly specialized).[43]

The bulletin also explains that "NHTSA may increase the weight it gives to the probability of an attack when there are confirmed incidents of the vulnerability being exploited in a malicious cybersecurity attack" and that a recall may be compelling when a vulnerability is identified in a "vehicle's entry points (e.g., Wi-Fi, infotainment systems, the OBD-II port) that allow remote access to critical safety systems."[44] Similar to software glitches, cybersecurity risks will rarely be deemed as safety defects based upon this criteria. This results in limited government oversight of vehicle software and cybersecurity by creating a recall infrastructure that does not adequately fit modern, connected vehicles.

In recent years, NHTSA has focused much of its research on cybersecurity and directed energy towards the formation of the Automotive Information Sharing & Analysis Center ("Auto-ISAC"), which emphasizes "cybersecurity awareness and collaboration across the automotive industry."[45] NHTSA approaches cybersecurity with goals to expand cybersecurity knowledge, support the automotive industry in setting voluntary standards, fostering new system solutions, and determining the feasibility of developing performance evaluation methods for automotive cybersecurity.[46] While allowing manufacturers to voluntarily set standards is likely sufficient where manufacturers have the knowledge and incentives to

43. Request for Public Comments on NHTSA Enforcement Guidance Bulletin 2016-02: Safety Related Defects and Emerging Automotive Technologies, 81 Fed. Reg. 18935, 18938 (Apr. 1, 2016), https://www.federalregister.gov/documents/2016/04/01/2016-07353/request-for-public-comments-on-nhtsa-enforcement-guidance-bulletin-2016-02-safety-related-defects.

44. *NHTSA Addresses Hacking and Cybersecurity*, CROWELL & MORING LLP (June 1, 2016), https://www.crowell.com/NewsEvents/AlertsNewsletters/all/NHTSA-Addresses-Hacking-and-Cybersecurity.

45. *Vehicle Cybersecurity*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity (last visited Nov. 24, 2021).

46. *Id.*

protect their technology, it also shields manufacturers from liability when cybersecurity goes awry and limits consumer and government oversight of vehicle safety.[47]

B. *A Need for Increased Transparency in Over-the-Air Software Updates*

In many ways, the mechanical failures of the past are being replaced by opaque software issues. In order to gain a better view of the algorithms controlling vehicles, it has been suggested that NHTSA's authority to recall autonomous vehicles ("AVs") "'would [be] enhance[d]' by the statutory provision requiring manufacturers to submit safety evaluation reports" as stated by a Senate Committee Report regarding the American Vision For Safer Transportation Through Advancement of Revolutionary Technologies Act ("AV START Act").[48] However, by the time a report would be submitted to NHTSA, some if not many manufacturers would likely have already pushed an update to remedy any safety issue previously identified in a connected, automated, or autonomous vehicle, especially considering that manufacturers have pushed updates within days of identifying a problem.[49] Additionally, in the case of a cybersecurity gap in software, a public report can alert an otherwise unaware hacker of a vulnerability.[50] For these reasons, it is necessary to create an infrastructure for software updates that is more efficient than the traditional recall process and asks manufacturers to be transparent about their frequent safety improvements to opaque operating systems.

A proactive recall policy would give NHTSA a better view into an automotive company's awareness of their own software. Instead of manufacturers submitting safety evaluation reports as the Senate Committee Report suggested, NHTSA should reform their recall process to specify how software related safety defects, software updates for non-safety purposes, performance updates, and cybersecurity updates will be treated by setting a standard for OTA technology platforms and creating a transparent database of updates. NHTSA could achieve this by creating a database similar to their current recall database.[51] The database would contain information about software and cybersecurity issues that impact consumer safety but do

47. For example, in September 2021 Tesla pushed an OTA update impacting automated driving software after various accidents were reported with emergency vehicles, demonstrating Tesla's self-regulation. However, Tesla did not provide notice to NHTSA or officially deem the issue a safety defect, shielding itself from liability and oversight. Stumpf, *supra* note 30.

48. Mark A. Geistfeld, *The Regulatory Sweet Spot for Autonomous Vehicles*, 53 WAKE FOREST L. REV. 337, 345 (2018) (alteration in the original).

49. Horvath, *supra* note 14.

50. Spector, *supra* note 32.

51. *See Safety Issues & Recalls*, *supra* note 3.

not meet the definition of "safety defects" under the Safety Act and provide a link to the recall database when OTA updates are available for issues deemed "safety defects."

The OTA database could provide a transparent, organized system for manufacturers to log each OTA software update pushed to vehicles on the road, not only allowing NHTSA to better understand the current state of vehicle safety but also to enable consumers to review what updates or software patches their vehicle has undergone. This would also improve transparency as vehicle software grows more complex.

While an OTA database would improve transparency for the government and consumers, automotive manufacturers will likely be hesitant to provide NHTSA with information about any and all safety issues that require updates, fearful that a NHTSA investigation could be opened resulting in a high price tag and millions of recalled vehicles.[52] Although a database of OTA updates may seem invasive to some manufacturers, it could greatly increase trust and transparency and aid efforts to put AVs on the road. This proposed database would likely be more intrusive to companies such as Tesla, that act more like software companies by quickly pushing out updates, than many OEMs which follow a more extended, thorough update process.[53] In order to have the highest engagement from auto manufacturers, an OTA database which shares many of the privacy principles and collaboration goals of Auto-ISAC would be ideal.[54]

II. NHTSA & Over-The-Air Software Updates

NHTSA has prescribed OTA software updates as remedies in their past recall reports and created a legal basis for OTA software updates,[55] but has yet to reform the recall infrastructure in a meaningful way that incorporates OTA updates. An industry-wide standard for components and operating system ("OS") configurations could minimize complexity and maximize efficiency of delivering safety updates to vehicles over-the-air, while also prescribing minimums for evaluating the cybersecurity of connected

52. *See* Keith Barry, *Car Recall Guide: Your Questions Answered*, Consumer Reps. (Sept. 21, 2020), https://www.consumerreports.org/car-recalls-defects/car-recall-guide-questions-answered/ ("Tens of millions of cars get recalled each year . . . . Some recalls include millions of vehicles, while others only include a dozen or so."); Rebecca Elliott & Ben Foldy, *Car-Safety Regulators Urge Tesla to Recall Around 158,000 Vehicles*, Wall St. J. (Jan. 13, 2021, 8:17 PM), https://www.wsj.com/articles/car-safety-regulators-urge-tesla-to-recall-around-158-000-vehicles-11610582727 (explaining a recall request could cost "$300 million to $500 million to address"); Brad Anderson, *Ford Reveals Airbag-Related Recall of 3 Million Vehicles Will Cost It $610 Million*, Carscoops (Jan. 22, 2021), https://www.carscoops.com/2021/01/ford-reveals-airbag-related-recall-of-3-million-vehicles-will-cost-it-610-million.

53. *See infra* Part III.

54. *See Best Practices*, Auto-ISAC, https://automotiveisac.com/best-practices (last accessed Nov. 24, 2021).

55. Pingol, *supra* note 18.

vehicles.[56] Due to increasing complexity of the software systems within vehicles, regulators must consider what consumer protections are necessary as the maintenance and operation of vehicles are no longer fully in the hands of riders. The DOT, which includes the Federal Motor Carrier Safety Administration and NHTSA, must determine how to best oversee OTA software updates with consumer safety in mind.[57]

Over-the-air software updates allow for remote software patches and feature updates, which present lower costs, increased accessibility for remedies, and more accurate predictions of safety issues.[58] Additionally, they may "facilitate higher recall completion rates," as what once required a trip to the auto shop can now be remedied with either an OTA update pushed to vehicles over wireless networks or a downloaded solution from a manufacturer's or NHTSA's website into the vehicle's USB port.[59] For example, "Ford says OTA updates will allow fixes for some recalls and updates of critical safety systems, repairs that currently require customers to bring their vehicles to a dealership's service department."[60] For these reasons, OTA updates are expected to save global OEMs over $35 billion by 2022.[61] Additionally, it is forecasted that nearly 203 million OTA enabled vehicles will ship by 2022, making OTA updates a critical aspect of automotive safety.[62]

III. A PUSH FOR OVER-THE-AIR SOFTWARE UPDATES

In February 2021, Microsoft announced a project with Bosch and Volkswagen to create a platform to deliver over-the-air software updates to vehicles through Microsoft's Azure cloud-based computing system.[63] Microsoft and Bosch hope to make the "installation process of automotive over-the-air updates a quick and seamless process, no different than

56. Halder et al., *supra* note 2, at 5.

57. *See generally* ZEV WINKELMAN ET AL., RAND CORP., WHEN AUTONOMOUS VEHICLES ARE HACKED, WHO IS LIABLE? 67–68 (2019), https://www.rand.org/pubs/research_reports/RR2654.html.

58. Keith Barry, *Automakers Embrace Over-the-Air Updates, But Can We Trust Digital Car Repair?*, CONSUMER REPS. (Apr. 20, 2018), https://www.consumerreports.org/automotive-technology/automakers-embrace-over-the-air-updates-can-we-trust-digital-car-repair.

59. BILL CANIS, CONG. RSCH. SERV., R46398, MOTOR VEHICLE SAFETY: ISSUES FOR CONGRESS 16 (2021).

60. Doug Newcomb, *The Upsides and Downside of Over-the-Air Software Updates for Automobile Dealers*, WARDS AUTO (Nov. 6, 2020), https://www.wardsauto.com/dealers/upsides-and-downside-over-air-software-updates-automobile-dealers.

61. Halder et al., *supra* note 2, at 3.

62. *Id.* at 2.

63. Craig Cole, *Microsoft and Bosch Join Forces to Create New Automotive Software Platform*, ROAD SHOW BY CNET (Feb. 18, 2021, 9:04 AM), https://www.cnet.com/roadshow/news/microsoft-and-bosch-join-forces-to-create-new-automotive-software-platform.

updating to the latest iOS version on your iPhone."[64] The duo also plans to use "GitHub's enterprise platform and even open-source components of their new software platform for sharing across the motor industry."[65] This is a step towards standardization which could lower development costs, increase transparency, and improve safety by sharing knowledge and expertise.

Volkswagen is utilizing Microsoft's cloud to push data and other mobility services to its vehicles and apps on a platform called the Volkswagen Automotive Cloud ("VW.AC"), which is currently being tested and is expected to be available to consumers in 2022.[66] Volkswagen hopes to integrate VW.AC with its new Azure cloud-based machine learning platform as well, allowing for OTA updates to push new software and autonomous modeling to be shared in the cloud.[67]

Although OTA software updates present the ease of an OTA iOS update on an iPhone, vehicle updates must be treated with more formality due to the possibility of safety and security risks to software controlling engine transmissions, door locking, car horns, braking systems, speed, navigation, and audio or information systems.[68] Greater use of OTA updates will subject vehicles to cybersecurity risks, and for that reason, cybersecurity is one of the most pressing issues on the minds of those developing OTA technologies and platforms today.[69]

OEMs have already began demonstrating their commitment to quality maintenance by OTA software updates thorough meticulous update cycles that maximize the rigor of safety procedures over a time span of weeks or months. In 2020, OEMs took 48 days on average to fix and begin remedying safety recalls, but there are still many cases where the timeline exceeds 3-5 months.[70] But other auto manufacturers working with a business model closer to that of a software company than an OEM, such as Tesla, have pushed updates within days of identifying an issue. For example, Tesla pushed 388 OTA software updates to vehicles over a period of just six years.[71] As explained earlier in this note, in 2018 after Consumer Reports

64. *Id.*

65. *Id.*

66. Chris Davies, *VW & Microsoft Are Building an Autonomous Car Platform with Azure at Its Heart*, SLASHGEAR (Feb. 11, 2021, 8:25 AM), https://www.slashgear.com/vw-and-microsoft-are-building-an-autonomous-car-platform-with-azure-at-its-heart-11658892.

67. *Id.*

68. *See* Amit Agarwal, *Understanding Automotive OTA (Over-the-Air Update)*, PATHPARTNER (June 26, 2020), https://www.pathpartnertech.com/understanding-automotive-ota-over-the-air-update.

69. *See* Chris Clark, *Protecting Automotive OTA Software Updates from Security Threats*, SYNOPSYS (July 8, 2021), https://blogs.synopsys.com/from-silicon-to-software/2021/07/08/ota-software-updates-automotive-cybersecurity.

70. Lilly, *supra* note 1.

71. Horvath, *supra* note 14.

reported an "overly long stopping distance for the Model 3" Tesla vehicle, Tesla pushed an OTA software update only a few days later that "shaved about 20 ft off the Model 3's braking distance."[72] The speed of the update earned Tesla praise from Consumer Reports, but also raised concerns from some that the update was too rapid to "develop, test, verify, and document such an impactful update on one of the car's key safety systems."[73]

While OTA software updates have presented manufacturers a new opportunity to improve vehicles once out on the road and in a consumer's possession, the frequency and quality of updates deserves more attention, especially as OTA infrastructure rapidly expands in a fragmented fashion. An OTA software update database maintained by NHTSA could offer a solution to these problems.

IV. A New Recall Process for Over-the-Air Updates

It is only a matter of time before all auto manufacturers are pushing OTA software updates to consumers on the road, some of which will offer new features and others will remedy safety and cybersecurity issues. OTA software updates will save billions and may even be used to entirely avoid recalls for what would have been deemed a software related safety defect in the past.

From 2015 to 2020, NHTSA issued 189 recalls caused by software bugs, resulting in more than 13 million vehicles being physically recalled.[74] If a different framework existed for remedying software related issues in vehicles, it is possible that millions of dollars could have been saved from the recall process by using OTA updates to remedy the issue, along with expediting the delivery of the remedy.

While it will be important to ensure that safety related software updates receive thorough development, testing, verification, and documentation, it will also be important that serious software bugs, whether related to cybersecurity, automated driver assistance systems, or fully autonomous driving systems can be updated or recalled immediately upon discovery of a safety issue. In these situations, NHTSA's recall process requiring a manufacturer to notify NHTSA, vehicle or equipment owners, dealers, and distributors by first-class mail within a reasonable time is out of date and could potentially lead to fatalities. An OTA Software Update database could remedy this gap, by notifying consumers, regulators, representatives, and

72. *Id.*

73. *Id.*

74. Halder et al., *supra* note 2, at 2 ("Honda recalled 350,000 vehicles due to a glitch in the parking brake software. GM recalled 4.3 million cars due to a software issue that blocked the airbags from deploying during an accident. All these recalls could have been avoided if there were OTA software updates.").

other manufacturers while also enabling manufacturers to respond as fast as possible to the issue.

A. *Examples of Software Related Recalls*

As aforementioned, many software issues with vehicles do not constitute safety defects,[75] however some issues have been officially deemed defects by NHTSA.

One safety related software recall in 2021 included almost 1.3 million vehicles which were found to have a software defect that provided emergency responders with the incorrect location of the vehicle following a crash, according to a NHTSA investigation.[76] The defect was to be remedied by either an authorized Mercedes-Benz dealer or an OTA software update of the communication module for the automatic emergency call system.[77] Mercedes-Benz mailed recall notification letters to owners by April 6, 2021, in accordance with 49 C.F.R. § 577.7,[78] notifying all "Mercedes Me" subscribers that the software update will be performed over-the-air and notifying other customers that they may opt out of the OTA software update and instead visit an authorized dealer to have the update performed.[79]

In the NHTSA Safety Recall Report regarding the Mercedes-Benz defect, NHTSA stated that "conditions such as network coverage and consistency of the data connection" may interfere with the success of completing the OTA software update.[80] This raises a potential issue of owners of recalled vehicles being uncertain about whether the safety defect has been resolved in their particular vehicle. Subscribers of the "Mercedes Me" service "may check the status of the update through the associated website and/or through the Mercedes Me App" under "Software Updates."[81] However, owners of recalled vehicles who do not subscribe to "Mercedes Me" will be unable to know if the software update was successfully completed without visiting an authorized Mercedes-Benz dealer. An OTA Software Update database controlled by NHTSA could offer consumers information about how to check if their vehicle is up to date, decreasing the number of vehicles operating with outdated software due to connectivity issues.

---

75. *See supra* Part I(A)(1).

76. Kim Lyons, *Mercedes Recalling More Than 1 Million Vehicles Over Emergency-Call Location Error*, VERGE (Feb. 13, 2021, 6:18 PM), https://www.theverge.com/2021/2/13/22282135/mercedes-recall-1-million-vehicles-emergency-call-location-error.

77. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., PART 573 SAFETY RECALL REPORT 21V-058 39 (2021), https://static.nhtsa.gov/odi/rcl/2021/RCLRPT-21V058-3925.PDF.

78. National Traffic and Motor Safety Act, 49 U.S.C. §§ 30118–30120 (2012).

79. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 77.

80. *Id.*

81. *Id.*

In other cases, an OTA software update will not be the correct remedy for a software or hardware issue in a vehicle. On January 13, 2021, NHTSA requested Tesla recall the 2012–2018 Model S and 2016–2018 Model X in a formal letter stating that the vehicles pose a safety issue due to touchscreen display failure.[82] The agency's Office of Defects Investigation (ODI) determined the displays to be "defective because their computer processors have a finite number of program-and-erase cycles" which will lead to screen failure in five to six years, which is not "sufficient for safety-critical features."[83] The screen failure affects rearview and backup camera images and defogging and defrosting systems and "may decrease the driver's visibility in inclement weather."[84] Tesla confirmed that "all units will inevitably fail given the memory device's finite storage capacity," however, Tesla said that the "driver can perform a shoulder check and use the mirrors" and also "manually clear the windshield."[85] In an attempt to fix the problem, Tesla pushed several OTA software updates; however, "NHTSA said it tentatively believes the fixes are insufficient" because if the touch screen displays fail, over-the-air software updates to some functionalities may still be lost.[86] "Accordingly, ODI request[ed] that Tesla initiate a recall to notify all owners, purchasers, and dealers of the subject vehicles of this safety defect and provide a remedy, in accordance with the requirements of the National Traffic and Motor Safety Act, 49 U.S.C. §§ 30118-30120."[87]

Tesla owners have received formal recall notices from NHTSA on other occasions as well, including when an OTA remedy was issued after discovering that a charge plug was causing fires.[88] However, Tesla pushes many updates outside of the official recall process, many of which are often largely unannounced, like changing "suspension settings to give the car more clearance at high speeds" to avoid certain collisions.[89] Creating a mandatory OTA software update database where Tesla would log all of their system updates would increase transparency and regulatory oversight as AVs become more common and advanced.

82. David Shepardson, *Tesla to Recall 134,951 Vehicles Under Pressure from NHTSA*, AUTO. NEWS (Feb. 2, 2021, 7:11 AM), https://www.autonews.com/regulation-safety/tesla-recall-134951-vehicles-under-pressure-nhtsa.

83. Tom Krisher, *Tesla Balks at Touch Screen Recall, US Agency Takes Action*, DETROIT NEWS (Jan. 13, 2021, 10:15 PM), https://www.detroitnews.com/story/business/autos/2021/01/13/tesla-balks-touch-screen-recall-us-agency-takes-action/115291870.

84. Shepardson, *supra* note 82.

85. *Id.*

86. Krisher, *supra* note 83.

87. Letter from Director of the Office of Defects Investigation, Nat'l Highway Traffic Safety Admin., to Al Prescott, Vice President, Tesla Legal Dep't, (Jan. 13, 2021), https://static.nhtsa.gov/odi/inv/2020/INRM-EA20003-11321.pdf.

88. Brisbourne, *supra* note 26.

89. *Id.*

Finally, in addition to more traditional safety issues like connecting drivers to emergency responders or visibility of rearview cameras, cybersecurity software issues are already proving to be a major issue for manufacturers, regulators, and consumers of vehicles able to receive OTA software updates. The "first major recall due to a cyber security vulnerability" with vehicle software occurred in 2015.[90] Fiat Chrysler recalled 1.4 million cars to remedy a defect which allowed for remote hacking of their vehicles.[91] In this case, NHTSA was able to use its mandatory recall power to address the problem, but cybersecurity risks will not always fit into the definition of a safety defect and NHTSA will need a new mechanism to oversee OTA software updates specifically affecting cybersecurity. Further, because the recall framework is mainly designed to remedy physical safety defects, cyber issues may slip below NHTSA's radar. Based upon the importance of cybersecurity and growing support from legislators to address cyber issues in vehicles, NHTSA creating an OTA software update database would help to address concerns.

B. *Rulemaking to Address Over-the-Air Software Updates*

NHTSA should formally approve OTA software updates as a remedy for safety defects through the rulemaking process instead of simply identifying OTA software updates as a remedy in recall reports or broadly in recommendations. A NHTSA rulemaking process regarding OTA software updates should be commenced in response to multiple studies demonstrating a vast increase in software related recalls and growing fragmentation of OTA update platforms and technologies for vehicles. There are sufficient incentives to create a structured OTA framework to oversee updates, as the efficiency, cost, and safety benefits of secure OTA software updates are vast and will only continue to increase as more connected, automated, and autonomous vehicles are on the road.

Compatibility is increasingly important as "there are now more than 30 different solutions for OTA updates and remote data gathering among the top 50 Tier 1 suppliers and 30 major OEMs."[92] Private software companies are developing platforms which can organize OTA software updates and improve cybersecurity responses,[93] but without an industry standard,

90. *See* Martin C. Libicki, *How I Learned to Stop Worrying and Love the Internet of Things*, RAND BLOG (Aug. 4, 2015), https://www.rand.org/blog/2015/08/how-i-learned-to-stop-worrying-and-love-the-internet.html.

91. *Id.*

92. Mike Gardner, *Why Automotive OTA Update Standards Are Essential*, EMBEDDED (Dec. 18, 2020), https://www.embedded.com/why-automotive-ota-update-standards-are-essential (Tier 1 suppliers are companies that supply vehicle parts directly to OEMs.).

93. *See, e.g.*, WIND RIVER, IMPLEMENTING OVER-THE-AIR SOFTWARE UPDATES FOR AUTOMOTIVE APPLICATIONS 4 (2017), https://events.windriver.com/wrcd01/wrcm/2017/11/Over-the-Air-Updates-for-Automotive-White-Paper.pdf; *OTAmatic Software and Data Management*, AIRBIQUITY,

fragmentation in platform compatibility will continue. Inconsistency between OS technology and platforms is unsustainable as it increases "development costs, time to market, and the risk of errors" in software updates, and for that reason, guidelines alone are insufficient.[94] NHTSA should issue rules deeming OTA software updates as acceptable remedies and standardizing technologies so that all stakeholders can "benefit from common development and test tools."[95]

Some manufacturers may be opposed to sharing their regular updates as it could injure their competitive place in the market. In the rulemaking process, comments should be requested regarding how sharing information about operating systems for OTA software updates could potentially harm competition. Comments should also be requested regarding how greater transparency in updates could improve safety, trust, and innovation and also lower development costs for all manufacturers. The rulemaking process should set a standard for components and OS configurations deemed most suitable based upon comments submitted by experts. Additionally, the standard selected should allow for global OEM compatibility.

NHTSA is currently researching the cybersecurity of physical and OTA updates to firmware.[96] Increasing reliance on OTA updates in the future will pose a hacking risk to a vehicle's data by installing malware or hacking the vehicle's components by disabling a vehicle's ability to keep software up to date.[97] Some envision that private owners in the future will have the responsibility to accept "over-the-air updates that maintain cybersecurity of various components" which will also be shared by "manufacturers who can monitor completion of updates."[98] However, NHTSA could use the rulemaking process regarding OTA software updates to require that cybersecurity updates are automatically adopted by vehicles, unlike advanced driver-assistance system updates which should require driver approval and training on new features.[99] Regardless of the mechanism selected for cybersecurity updates, successful updates to software remains dependent upon consistency of network connection, data connectivity, and consumer education.

---

https://www.airbiquity.com/product-offerings/software-and-data-management (last visited Nov. 24, 2021) (demonstrating that private software companies are creating software which aims to oversee OTA updates and manage vehicle software over the lifecycle of the vehicle while promising improved cybersecurity response time).

94. Gardner, *supra* note 92.

95. *Id.*

96. *Vehicle Cybersecurity*, *supra* note 45.

97. WINKELMAN ET AL., *supra* note 57, at 19 tbl.3.1.

98. *Id.* at 38.

99. Oren Betzaleli, *As More Cars Update Themselves, the Convenience Could Bring Risks*, AXIOS (July 26, 2019), https://www.axios.com/as-more-cars-update-themselves-the-convenience-could-bring-risks-b80d5595-ff3c-4e16-9406-93d4a86b365d.html.

In order to aid in tracking of whether updates are successfully completed and to increase transparency in the frequency, type, and quality of updates, NHTSA should create a new database. This new database would be similar to NHTSA's current recall database, but specifically to track software updates to vehicles on the road. The OTA Software Update database would ideally log all updates pushed to vehicles, organized by VIN so that consumers are able to locate their own vehicle and confirm that their vehicle is up to date. Instead of periodic safety evaluations from manufacturers, as suggested by the Senate Committee Report above,[100] a database would provide NHTSA with a better view into the frequency and type of updates being pushed to vehicles. A database for OTA updates would also increase transparency for consumers and regulators and help facilitate the sharing of safety related expertise among OTA software providers and OEMs.

NHTSA rulemaking must also acknowledge that while thoroughness in development, testing, verification, and documentation of software updates is essential, some software bugs will need to be fixed immediately and should not delay notification to first-class mail within a reasonable time, in accordance with 49 C.F.R. § 577.7, as any delay in the recall process could potentially lead to fatalities. The rulemaking should request comments on the feasibility of carving out an exception in the recall process, specifically for emergency OTA software updates remedying cybersecurity issues. This will become increasingly important as cybersecurity risks to vehicles and safety issues with AV systems become both more complex and opaquer through machine learning and artificial intelligence.

C. *Counter Arguments to Creating an OTA Database*

Because regulation in the automotive industry can increase production costs, it is possible that manufacturers may view NHTSA oversight of OTA updates as an unwanted cost and risk, especially manufacturers like Tesla operating more like a software company than a traditional OEM. However, the automotive industry is changing, and it is reasonable that auto manufacturer costs may shift as the "deployment of driver assistance technologies may result in avoiding crashes altogether."[101] An OTA Software Update Database could possibly help automotive companies to comply with the NHTSA recommendations, increase transparency with consumers, and eliminate formalities of the Safety Act. However, it is possible that this database could interfere with innovation from manufacturers.

First, manufacturers sharing details of safety updates to vehicles in an OTA database could allow competitors to make similar adjustments at a

100. *See* Geistfeld, *supra* note 48 and accompanying text.
101. *Vehicle Cybersecurity*, *supra* note 45.

lower cost. This may disincentivize manufacturers from investing in innovative safety technology if there is potential for the safety updates to be copied by a competitor. On the other hand, collaboration in safety could lead to better vehicles and safety standards for all, especially as the automotive and mobility industries move towards more automated and autonomous vehicles on the road and the deployment of AI in vehicles. Details of safety updates pushed to vehicles would likely only identify the issue resolved, not the actual software code, to ensure the cybersecurity of connected vehicles and to protect the intellectual property of manufacturers.

Additionally, the organization, accessibility, and security of an OTA Database may be a challenge, especially because hundreds of updates are being pushed to millions of vehicles every year,[102] a number that will only increase in future years. Currently NHTSA maintains a database of recalls, so it is likely that NHTSA would need to redistribute resources or hire new employees to increase OTA oversight.

It is also possible that NHTSA would resist change to their recall framework, as it has remained largely unchanged for over 50 years. NHTSA' recall process is active and robust as is: "At the close of 2019, [NHTSA] had 44 open defect investigations (18 Engineering Analyses and 26 Preliminary Evaluations) along with ten investigations into the adequacy of manufacturer recalls."[103] However, while the recall process under the Safety Act of 1966 remains active, it is ill fit for the modern vehicles running on software and using artificial intelligence. For example, "NHTSA and a manufacturer agreed to a $20 million civil penalty based on the Agency's allegations that the manufacturer repeatedly missed reporting deadlines for various recall reports and related submissions," including failing to mail customer notification letters by first class mail within the 60-days.[104] The high penalty formalities of the Safety Act no longer ensure compliance, for example when Tesla pushed an OTA update to vehicles prior to mailing any notification letters.[105]

While there may be some obstacles to creating an OTA Software Update Database, if modeled similar to Auto-ISAC[106] and grounded in protecting the intellectual property of companies and maintaining cybersecurity, a database has the potential to aid NHTSA in overseeing OTA software updates pushed to vehicles.

---

102. *See How Over-The-Air Updates Are Turning the Auto Industry Upside Down*, INTLAND SOFTWARE (Oct. 20, 2020), https://content.intland.com/blog/how-over-the-air-updates-are-turning-the-auto-industry-upside-down.

103. Christopher H. Grigorian & Nicholas Englund, *NHTSA & Motor Vehicle Safety*, FOLEY & LARDNER LLP (Feb. 12, 2020), https://www.foley.com/en/insights/publications/2020/02/top-legal-issues-facing-automotive-industry-2020.

104. *Id.*

105. Lambert, *supra* note 27.

106. *Best Practices*, *supra* note 54.

CONCLUSION

The automotive industry is rapidly evolving, and now is the time for NHTSA to adapt its recall process for OTA software updates and cybersecurity issues. "The global automotive cybersecurity market is expected to grow at an unprecedented rate, from $1.34 billion in 2018 to $5.77 billion by 2025."[107] OTA updates are expected to save global OEMs over $35 billion by 2022.[108] The future of automotive recalls will occur over-the-air, replacing the tire and air bag recalls of the past. While the physical vehicle will remain important, the software within vehicles will rise to greater importance with cybersecurity vulnerabilities as a growing threat. NHTSA is already operating a recall framework that is outdated, and without evolution, it will become obsolete.

As vehicles become smarter and more connected, their software becomes more complex and requires regular updates. OTA software updates are an efficient, cost-effective way to keep modern vehicle software up to date. However, due to the often opaque nature of software and operating systems, there is a lack of transparency for consumers and regulators regarding the process of updating software in vehicles. Additionally, as OEMs and private software distributors work separately to create their own OTA platforms, the technologies are growing increasingly fragmented, resulting in incompatibilities. For these reasons, and to prioritize the most efficient responses to safety issues in a world of increasingly complex vehicles, NHTSA should commence a rulemaking proceeding regarding OTA software updates in order to officially approve the process as a remedy for recalls, set standards for OTA operating systems and components to improve compatibility among global OEMs, and to create an organized, accessible database of OTA software updates which will result in increased transparency for consumers, regulators, and manufacturers.

107. Mark Aiello & Vanessa Miller, *The Impact of Emerging Technologies on Global Automotive Supply Chains*, FOLEY & LARDNER LLP (Feb. 12, 2020) https://www.foley.com/en/insights/publications/2020/02/top-legal-issues-facing-automotive-industry-2020.

108. Halder et al., *supra* note 2, at 3.