www.Privacy4Cars.com

Comments to National Highway Traffic Safety Administration

"Cybersecurity Best Practices for the Safety of Modern Vehicles"

February 17th, 2021

Privacy, Cybersecurity, and the Safety of Modern Vehicles

These comments are submitted for the record to the U.S. Department of Transportation in response to the National Highway Traffic Safety Administration's notice of intent to update its best practices document entitled Cybersecurity Best Practices for the Safety of Modern Vehicles, published in the January 7, 2021 edition of the Federal Register.

I am the Founder and CEO of Privacy4Cars, a Georgia-based technology company building privacy tools for vehicles. I have worked in the automotive space for a decade, and six years ago I started building the first app designed to quickly and easily delete Personally Identifiable Information (PII) from vehicles - and offered it for free to consumers.

I am submitting these comments to raise concerns about the lack of specific attention to consumer privacy and personal data security in Cybersecurity Best Practices for the Safety of Modern Vehicles. Modern vehicles collect a large and continuously growing amount of personal information about drivers and passengers alike, which not only poses risks to consumers safety, but also puts their identities and civil liberties at risk when cybersecurity is insufficient or compromised. The manufacturers themselves made this point with their ~$30 million advertising campaign launched this fall in an effort to kill the "right to repair" Proposition 1 in Massachusetts. In those ads, OEMs sounded the alarm that leaking personal information may result in crimes such as stalking and home invasions - yet actions in this area remain scant: more than 4 out of 5 vehicles for sale last year were resold while still containing the personal information of the previous owners and occupants!

Data hygiene and addressing privacy issues is far from a common practice or a priority: three years ago I responsibly disclosed to the Auto-ISAC a security flaw that affected tens of millions of vehicles across over 20 brands and several manufacturing years. The "CarsBlues" vulnerability made it easy to expose and potentially exploit the contacts, call logs, and text messages of previous occupants (without their phones being connected or their knowledge or consent). But while some manufacturers made changes to their new vehicles in production based on my cybersecurity research, I am not aware of any action taken to fix the infotainment systems of the affected vehicles already on the road, nor I am aware of any effort made to even notify the dealers or consumers that their vehicles were and remain vulnerable - still today.

Unfortunately today NHTSA does not have the authority to require manufacturers to act (e.g. to recall defective units) for any cybersecurity issue that is not strictly affecting safety while driving. This is an incredibly narrow view of the capabilities of vehicles and a terrible anachronism: the most common cybersecurity incidents with vehicles in the last 11 years have been data/privacy breaches, which accounted for 36% of all incidents in 2020.

Furthermore, the stated "Purpose of This Document" being drafted is "to ensure systems will be safe under expected real-world conditions". If data collected by vehicles can be (as demonstrated by the statistics above) exposed, extracted, and exploited, and this results in people not being safe, shouldn't this new administration at NHTSA adopt a more human-centric approach that puts security and privacy of the drivers and other vehicle occupants as its goal, and the safety of the systems simply as a mean to achieve that goal?

We hope NHTSA will finally consider cars the "third screen" (after computers and phones) and consequently require the industry to incorporate more broad cybersecurity and data protection best practices in line with those of general computing devices across the entire lifetime of the vehicles, and have the power to enforce those general computing best practices.

Please see below for additional details and pertinent literature.

Sincerely,

Andrea Amico

Founder and CEO, Privacy4Cars

andrea@privacy4cars.com

[The remainder of this page is intentionally blank.]

Privacy is a Cybersecurity Best Practice

Introduction

Vehicles today capture an increasing amount of personal information including data about your contacts, call logs, or text messages copied from mobile devices, unique identifiers, as well as precise location data from GPS sensors, and even the security code for your garage doors. Sensitive personal information is captured about each of us whether we own, lease, rent, or share vehicles. Some of it is automatically shared with commercial parties while the rest is left behind whenever a vehicle switches hands.

The seamless integration of technology from our homes to our vehicles can create convenient and often helpful experiences for consumers. Yet, efforts to protect consumer privacy have not kept pace with businesses' appetite for more and more data. This negligence creates significant risk for consumers even after they part ways with a vehicle because their personal data remains intact -- and that makes them vulnerable.

Driver and Passenger Safety Includes Privacy

The fastest growing category of crime is those that exploit personal information (identify theft, scams, fraud, stalking, etc.) and often target specific groups such as women, the elderly, and disadvantaged communities. As we've seen with increasing frequency, risks to digital privacy can easily turn into threats against one's physical safety. Inadequate privacy protections at the systems, code, and UX levels of a vehicle put consumers in harm's way and open them up to new and increasing safety risks.

To manage their fiduciary duty to protect Personal Information of consumers and reduce their legal and reputational risk, many large auto finance companies - including OEM captives - are already mandating the deletion of personal information in certain jurisdictions or for certain vehicles, such as repossessed cars. This process can be easy, inexpensive, and auditable. Yet, today only a small fraction of the more than 40 million vehicles sold in the United States and the nearly one billion vehicle handoffs that occur every year, include an attempt to protect the personal information of previous users.

Cybersecurity Vulnerabilities Expose Personal Information

Since 2015, security researchers at DEF CON, the world's largest hacker conference, have publicly demonstrated vehicles' evolving cybersecurity vulnerabilities. We've seen vulnerabilities that enable physical control of vehicle systems as well as those that expose, leak, and exploit personal consumer information. While the former category claims most of the media and political attention, very little has been done to protect personal information against cybersecurity vulnerabilities. Unfortunately the reality is quite different: vehicle cybersecurity firm Upstream reported in their "2021 Global Automotive Cybersecurity Report" that Data/Privacy breaches topped their list at 30% of all vehicle cybersecurity incidents in the 2010-2020 decade, representing 30% of all attacks. In fact, the issue is worsening: this past year Data/Privacy breaches represented 36% of all cyber attacks performed by criminals, even surpassing the hacking of key fobs. Criminals start to value and steal the Personal Information collected by automotive companies more than the vehicles themselves!

Unfortunately we have direct experience of the insufficient focus put on protecting consumer's Personal Information. CarsBlues, a zero-day vulnerability I discovered in 2018 still impacts tens of millions of vehicles on the road today. Even after the vulnerability was disclosed responsibly to the auto industry, there has still been no official notification from the automakers to dealers, consumers, or fleet owners to inform them of the vulnerability or that their personal information may be exposed and exploited by other people with access to the vehicle, including future owners or renters.

Those most at risk include consumers who synced their phones in vehicles that are no longer under their direct supervision, including but not limited to vehicles they've rented, shared through a fleet or subscription service, loaned, sold, returned at the end of a lease, repossessed, or deemed a total loss. Additionally, people who have synced their phones and given others temporary access to their personal vehicle, such as at dealership service centers, repair shops, peer-to-peer exchanges, and valets may also be at risk because of the CarsBlues vulnerability.

In closing, the Cybersecurity Framework from the U.S. Department of Commerce's National Institute of Standards and Technology (NIST's), already recognizes the importance of privacy considerations for cybersecurity best practices. As stated in NIST's Cybersecurity Framework:

"To address privacy implications, organizations may consider how their cybersecurity program might incorporate privacy principles such as: data minimization in the collection, disclosure, and retention of personal information material related to the cybersecurity incident; use limitations outside of cybersecurity activities on any information collected specifically for cybersecurity activities; transparency for certain cybersecurity activities; individual consent and redress for adverse impacts arising from use of personal information in cybersecurity activities; data quality, integrity, and security; and accountability and auditing."