https://Privacy4Cars.com

Public Comment to the Energy and Commerce Committee hearing on "Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security"

Submitted to the Subcommittee on Consumer Protection and Commerce of the Committee on Energy and Commerce

June 14th, 2022

Good morning, Chair Schakowsky, Ranking Member Bilarakis, and Members of the Consumer Protection and Commerce Subcommittee. I commend you for holding this important hearing on "Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security" and I respectfully submit these comments for your consideration.

There are three devices that cause the collection of the massive amount of personal data the American Data Privacy and Protection Act seeks to protect and regulate: computers, smartphones, and vehicles. The first two are often discussed (and I am sure will be mentioned multiple times during this hearing). Vehicles however collect terabytes of sensitive personal information… but too often remain in the shadows of data privacy and security discussions.

I founded Privacy4Cars to give businesses in the automotive industry a simple, reliable, and auditable solution to delete the personal data vehicles routinely collect from drivers and passengers in order to prevent harms to consumers' privacy, security, and safety. This is an issue that affects over 100 million Americans every year and something the Federal Trade Commission warned about multiple times. We have also, from the very beginning of our company, offered free tools to consumers to help them reduce their vehicle data footprint.

I am writing to you to share my firsthand experience with what safeguards are put in place (or not) when it comes to the electronic Nonpublic Personal Information collected by and stored in vehicles and how different companies treat this consumer data which includes sensitive GPS locations, phone records, garage door codes, connected services, and more. This data can, and has, in turn be used to re-

identify consumers, collect intel on them, profile them, contact them, harass them, stalk them, and invade their private homes.

It is important for this commission to realize that modern vehicles are like web browsers…. but in the physical world, and your "browsing history" is being collected, sold, and shared at accelerating and concerning pace. Just like with laptops and smartphones, focusing on the manufacturers of those devices alone is vastly insufficient to protect the privacy and security of consumers, because the data generated by those devices fuels an entire ecosystem. At Privacy4Cars we track hundreds of companies that engage in the brokerage of vehicle data. Unfortunately, we are just at the beginning of the vehicle data revolution: according to consulting company McKinsey the market for vehicle data will be worth between $400 and $750 billions by 2030. Fortunately, we are just at the beginning of the vehicle data revolution: there are no decades-long entrenched interests or large established economies relying on this data. Setting clear rules now can allow for this market to ethically develop in a manner that enables innovation, fosters safety, but balances that with the need to protect the interest of the public at the same time. This is why solutions to address vehicle privacy and security must go well beyond the companies who manufacture vehicles. Protecting consumers requires action from auto insurers, auto finance companies, business and rental fleets, dealerships, repairers, and the many other verticals within the broader auto industry who collect, use, share, and sell this data.

We are already seeing some early encouraging signs that setting reasonable protections for consumers is possible. A growing cohort of auto finance players, including vehicle manufacturers' captive auto finance companies, national banks, large subprime institutions, all the way to regional lenders and credit unions have adopted the practice to remove the electronic personal information left behind by consumers in vehicles that are repossessed or at the end of a lease so they are not breached and disclosed to unauthorized third parties, including dealership personnel and future owners. Similarly, most major fleet management operators (who supply and help manage many corporate and government fleets) have put similar measures in place. Dealerships are starting to take steps as well to protect the Nonpublic Personal Information captured by vehicles on their lot and give their customers the peace of mind they deserve that their data (including their home address and garage codes) does not fall into the hands of somebody else. These companies are supported in this privacy and security protection effort by a vast network of entities that process their vehicles from the time the vehicle stops being under the control of a consumer and until it is resold including auto auctions, vehicle inspection companies, and recovery agents. Those companies have collectively determined and agreed that clearing this data is a reasonable safeguard standard that needs to be in place every time a vehicle is handed off from a consumer to another.

Many of these entities are regulated under the Gramm Leach Bliley Act (GLBA). Given the upcoming December 9th change to GLBA's Safeguards Rule we hope to continue to see businesses pay more attention to the Nonpublic Personal Information vehicles collect, store, and share – and on how to safeguard this data.

Yet, most auto finance companies are still not taking action. Several companies are delaying putting in place much-needed protections due to the lack of clear guidance from Congress, the Federal Trade Commission and the Consumer Financial Protection Bureau on the necessity to protect the electronic personal data consumers captured by vehicles. This is wrong for a number of reasons, including:

- Many vehicle manufacturers' privacy policies attempt to place the burden on consumers to delete any personal data collected by or stored in the vehicle, but our surveys show most consumers are unaware of this data collection, and so are dealership personnel because of the endemic lack of transparency and no investment in educating either business partners and final users of automobiles.
- Conversely, auto finance companies who repossess a vehicle or at the end of a lease, insurance companies after a total loss accident, and dealerships who purchase vehicles to resell them, all have the financial ownership and, directly or through their service providers, the physical access and sufficient time required to clear consumer data from a vehicle before putting it back into the stream of commerce: an activity that usually takes a couple of minutes or less.
- There is a clear parallel and precedent with the many state-by-state requirements to protect personal information left in vehicles that are repossessed, most states have data security, data minimization, and data breach laws, and most states have Model 670 privacy laws and model 673 data security laws for insurance companies. Those hundreds of local statutes by and large require companies to protect personal information of consumers from being accessed by unauthorized third parties and to dispose of personal records that are no longer required for business reasons.[1] It is unclear to us what reasonable business motivation companies in the broader automotive ecosystem may advocate for not disposing of personal consumer records stored in the assets they financed, insured, resold, or rented before transacting on those assets, and for leaving this data available to anybody that will have future physical access to the vehicle.
- NIST published a guideline[2] that provides clear guidance to companies: clearing personal data is the practical sanitization decision and the minimum standard that needs to be in place for any media-storing device, including vehicles. The computer and mobile phone industries self-regulated themselves and created nationwide standards for the ethical reselling and recycling of used laptops, hard drives, smartphones, and other media-storing devices. Those standards require clearing data before reselling any of those devices that may contain Personal Information. Automobiles remain the only mass data capture and storage device for which those standards are not being followed, despite the fact that every year over 40 million used vehicles are resold and over 150 million vehicles are rented.
- Auto industry groups have been actively warning during the Right-To-Repair debate that giving vehicle data access to a third party is a significant risk for consumers.[3] However, the same companies insist that neither they, their auto finance, their franchised dealership, and their service providers and partners have any responsibility in protecting and safeguarding consumers' Personal Information. That's not right.
- We have demonstrated over and over how easy it can be for a person with physical access to a vehicle (which may include the personnel of a dealership or the future buyers and users of the vehicle) to see and extract Personal Information of the former owner and family members, possibly including minors. New owners, for instance, could enter the home of the consumer whose vehicle was resold with just two clicks ("go home" on the navigation system, pressing the garage opener): just as shown in those anti Right-To-Repair ads ran by the auto industry.

[1] https://privacy4cars.com/legal-resources/laws-by-geography/
[2] https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization
[3] See for instance this TV advertisement that ran in advance of the vote on Proposition 1 about the risk of a home invasion: https://youtu.be/_FEeGhS7Ac0

- Last but not least, the recent FTC amendment to the Safeguards Rule[4] which comes into full effect on December 9th 2022, seems to clearly apply to the case of personal information stored in vehicles. The new Rule requires regulated entities, including auto finance companies and dealerships who repossess vehicles, to meet a prescriptive list of requirements, and not doing so would constitute an Unfair or Deceptive Act or Practice. Based on our expertise on how vehicle embedded systems work (for instance, data in vehicles is often unencrypted, the only factor of authentication is the highly shared key, etc.), the only way for companies to comply with the revised Rule is to dispose of the personal information of previous occupants by clearing it prior to the sale of the asset.

We are glad to see that many provisions included in the American Data Privacy and Protection Act clearly highlight how vehicles collect Sensitive Personal Information as defined in the law, and that passing this Act would result in substantial protections being created for vehicle drivers and passengers (including minors) who see their data collected, brokered, and left behind unprotected every day. Based on out audits, last year oved 4 out of 5 vehicles have been resold while still containing the sensitive personal data of the previous owner(s) and their family member(s). This implies that every year the personal information of millions of Americans is being breached and leaked on a day-by-day basis through cars. This massive, silent data breach keeps happening despite the local laws, despite the NIST guidelines, and despite the upcoming changes to the Safeguards Rule because too many auto companies have taken the position that they should not take care of clearing their customers' electronic personal information stored in the infotainment and other systems of the vehicles they control and profit from. This anachronism is astonishing considering that those same companies have clear policies requiring them to remove and destroy data from their computers, servers, storage media, and smartphones used by their employees.

Your Committee has the power and ability to end this opaque and large scale breach of trust and breach of consumer data. My hope is that this Committee will recognize that vehicles are "the third screen", and that vehicles should be subject to exactly the same rules the American Data Privacy and Protection Act would establish for all other consumer personal information.

Thank you for considering these concerns. I'm available for further discussion or additional information as needed.

Sincerely,

Andrea Amico
Founder and CEO
Privacy4Cars
https://privacy4cars.com
andrea@privacy4cars.com

[4] https://www.govinfo.gov/content/pkg/FR-2021-12-09/pdf/2021-25736.pdf