PRIVACY4CARS

www.Privacy4Cars.com

Comments To the Subcommittee on Consumer Protection and Commerce Of the House Committee on Energy and Commerce Hearing on **"Autonomous Vehicles: Promises and Challenges of Evolving Vehicle Technologies"**

February 11th, 2020

Good morning, Chair Schakowsky, Ranking Member McMorris Rodgers, and Members of the Consumer Protection and Commerce Subcommittee. Privacy4Cars is grateful for the opportunity to present this statement to the Subcommittee with respect to your hearing on "Autonomous Vehicles: Promises and Challenges of Evolving Vehicle Technologies." We respectfully ask that this statement is included in the official record of this hearing. Autonomous Vehicles (AVs) hold incredible promise to be a positive and transformative technology for Americans. In order to achieve such promise, a thoughtful deployment of this technology is necessary.

On Nov 15th, 2016, Energy and Commerce Ranking Member Frank Pallone, Jr., in his opening remarks at the first Autonomous Vehicle hearing[1], rightly pointed out that such deployment needs three fundamental pillars: safety, cybersecurity, and privacy-by-design. Three and a half years later, not only Autonomous Vehicle technologies have made significantly less progress than what industry leaders had promised to the government, investors, and the public[2] [3], but Connected Vehicles (in many ways a precursor technology to AVs) that are currently for sale in dealerships and on American roads have not, again despite the many promises of the industry, significantly improved safety[4] while objective metrics of both cybersecurity and privacy issues are getting worse.

[1] Subcommittee on Commerce, Manufacturing, and Trade hearing titled "Disrupter Series: Self-Driving Cars" https://energycommerce.house.gov/newsroom/press-releases/pallone-s-opening-statement-at-autonomous-vehicles-hearing

[2] All the Promises Automakers Have Made About the Future of Cars, July 2017 https://www.theatlantic.com/technology/archive/2017/07/all-the-promises-automakers-have-made-about-the-future-of-cars/532806/

[3] When will autonomous vehicles be finished? Definitely do not hold your breath. Really—stop ithttps://www.wired.com/story/when-will-self-driving-cars-ready/

[4] NHTSA Traffic Safety Facts Annual Report Tables https://cdan.nhtsa.gov/tsftables/tsfar.htm

Automotive cybersecurity incidents doubled in 2019 compared to 2018, and are up 605% since 2016[5], the year in which this Committee started its work on Autonomous Vehicles. Even more concerning is that for the past two years attacks carried out by criminals have surpassed the vulnerabilities identified and responsibly disclosed by researchers. As the number of Connected Vehicles continues to grow in the United States (most manufacturers have promised to have most if not all their new vehicles connected by 2020), so is the attack surface exposed to potential cyber-attacks, and so is the number of experts who are issuing stern warnings.

The privacy picture painted by Connected Vehicles, and in the future Autonomous Vehicles, is possibly even more gloomy, as illustrated for instance in the recent Washington Post expose "What does your car know about you? We hacked a Chevy to find out."[6] "We're at a turning point for driving surveillance: In the 2020 model year, most new cars sold in the United States will come with built-in Internet connections, including 100 percent of Fords, GMs and BMWs and all but one model Toyota and Volkswagen," said journalist Geoffrey Fowler. "We focused on the computer with the most accessible data: the infotainment system," he went on, "There on a map was the precise location where I'd driven to take apart the Chevy. There were my other destinations, like the hardware store I'd stopped at to buy some tape. Among the trove of data points were unique identifiers for my and Doug's phones, and a detailed log of phone calls from the previous week. There was a long list of contacts, right down to people's address, emails and even photos.".

What people don' realize is that data may haunt you long after you believe you are done with a car. "[We] also extracted the data from a Chevrolet infotainment computer that I bought used on eBay for $375. It contained enough data to reconstruct the Upstate New York travels and relationships of a total stranger. We know he or she frequently called someone listed as "Sweetie," whose photo we also have. We could see the exact Gulf station where they bought gas, the restaurant where they ate (called Taste China) and the unique identifiers for their Samsung Galaxy Note phones," said the Post Tech columnist. That infotainment system came from a total loss vehicle that had been in a crash. Neither the manufacturer or the insurance company or the shop that sold the used part took action to protect this person's identity. Sometimes it gets worse, as in the case of Mr. Marulla, who discovered that over three years after his lease was expired could still "track [his former electric Ford Focus] movements, see where it plugs in," he said. "Now I know where the current owner likely lives, and if I watch it tomorrow I can probably figure out where he works. I have not been the owner of this vehicle for four years, Ford knows this, yet they took no action whatsoever to remove me as the owner in this application," reported renowned

[5] Automotive cybersecurity incidents doubled in 2019, up 605% since 2016 https://www.helpnetsecurity.com/2020/01/06/automotive-cybersecurity-incidents/. Full report by cybersecurity firm Upstream available at https://www.upstream.auto/upstream-security-global-automotive-cybersecurity-report-2020/

[6] What does your car know about you? We hacked a Chevy to find out https://www.washingtonpost.com/technology/2019/12/17/what-does-your-car-know-about-you-we-hacked-chevy-find-out/

cybersecurity expert Brian Krebs[7]. Or in the case of Mr. Sinclair, who realized he could still track the Ford vehicle he had rented five months before from Enterprise Rent-A-Car, lock and unlock it, and start and stop its engine[8]. “While Ford said infotainment screens will indicate when a device is paired, it's obvious that multiple Enterprise employees and renters have continued to miss the warning,” reported ArsTechnica, and “Even now, after I discussed the problem with both Enterprise and Ford representatives, Sinclair's access still hasn't been revoked.” Unfortunately, none of this was surprising to us at Privacy4Cars, because we have reached out to multiple automakers and the Auto-ISAC for over a year, showing them how easy it is to gain access to a vehicle a stranger has access to for just a few minutes. This is sometimes resulting in repugnant crimes, such as in the case of the stalker who admitted using the connected Land Rover to spy, track, control, and ultimately invade the home of his ex-girlfriend[9].

These are the reasons why experts, advocates, and the general public are increasingly concerned with the privacy challenges posed by modern vehicles’ ability to collect massive amounts (several Terabytes a year) of detailed personal information from their occupants – often without people’s knowledge, understanding, or transparent consent. The resulting lack of trust can have very severe negative effects on the deployment of Autonomous technologies, and halt or severely delay the benefits AVs can deliver.

At Privacy4Cars we have first-hand experience over these issues. Our founder is a former automotive executive and a vehicle privacy and cybersecurity expert. He authored the first research demonstrating that the vast majority of vehicles being resold, rented, or shared still contain the personal information of the previous and unsuspecting users. He has been working with multiple industry associations such as the US Chamber and the International Automotive Remarketers’ Alliance Alliance (IARA)[10] where he spearheaded the formation of a partnership with the Automotive Information Sharing and Analysis Center (Auto-ISAC), the association established by the auto industry to address cybersecurity issues and a partner of the Department of Homeland Security. When the auto industry insisted that the personal information of the vehicle users (such as contact books, call logs, and even full text messages synced from the smartphones of the car occupants) where kept safe by cars, he demonstrated (and responsibly disclosed to the Auto-ISAC) it was instead easy to extract and potentially exploit the personal information stored in the

[7] When your used car is a little too mobile https://krebsonsecurity.com/2020/02/when-your-used-car-is-a-little-too-mobile/

[8] Five months after returning rental car, man still has remote control https://arstechnica.com/information-technology/2019/10/five-months-after-returning-rental-car-man-still-has-remote-control/

[9] Man pleads guilty to stalking and controlling ex-girlfriend's car with his computer https://www.abc.net.au/news/2019-11-06/ract-employee-pleads-guilty-to-using-app-to-stalk-ex-girlfriend/11678980

[10] IARA is the industry association that reunites many of the leading players in the $100 billion vehicle wholesaling industry in the US and Canada, including automotive OEMs, automotive finance companies as large as captives and national blue-chip banks to smaller regional auto leasing and lending companies, most of the main auto auctions, large fleet management and fleet companies such as rentals, vehicle repossession companies, dealers, and many other service providers. www.iara.biz

infotainment systems of tens of millions of vehicles across 23 different automotive makes[11] - and all is needed is less than a handful of minutes and a common device that can be purchased for $45 at many retail chains. Even the Michigan police, recognizing the threat the data collected by cars poses if it were to fall in the wrong hands, has recently issued a warning on the risk of identity theft arising from personal information stored in the vehicles' computers[12]!

The security and privacy issues with Connected, and soon with Autonomous Vehicles affects not only consumers, but also many large and small businesses related to the automotive sector across America: from the local dealerships in your hometown to large fleets, from credit unions to auto wholesalers, from insurance companies to auto portfolio lenders. A poll of IARA members in the Spring of 2019 showed that 79% of executives are concerned about the Personally Identifiable Information (PII) retained by In-Vehicle Infotainment Systems (IVIS). Many reached out to and are partnering with Privacy4Cars where we developed the first process to simply and efficiently erase PII from modern vehicles[13]. Privacy4Cars' mission is to protect the privacy, security, and safety of consumers, which is why we make our Privacy4Cars app available as a free download for consumers on both iOS and Android devices. We also humbly realize that government, and your Subcommittee specifically, needs to intervene to reduce the current risks and make sure guardrails are put in place so the industry has the clarity needed to develop these new technologies in a safe, secure, and privacy-respecting manner. Based on our experience, we recommend the Subcommittee considers the following:

1. To introduce IoT Cybersecurity standards for all Connected and Autonomous Vehicles
2. To introduce Privacy-by-design standards for all Connected and Autonomous Vehicles
3. To expand the Driver Privacy Act of 2015 from the EDR only to all vehicle computers
4. To introduce a cybersecurity and privacy rating system (similar to the vehicle safety ratings)
5. To give NHTSA (or another federal agency) the ability to enforce cybersecurity and privacy standards, with similar powers they have for safety (including issuing recall notices)

IoT Cybersecurity standards for Connected and Autonomous Vehicles

Vehicles are the largest, most complex, most expensive IoTs Americans own. They are often the first or second-largest purchase a household makes and yet are not required to meet any standard when it comes to cybersecurity – from the day they leave the factory and throughout their lifetime (the average car is 11 years old). Most vehicle systems fail to include some of the most basic data protection techniques that are commonplace with modern computing and mobile devices, such as authentication and encryption. We recommend that all manufacturers who want to sell or test on public roads Connected or Autonomous Vehicles need to first abide to cybersecurity standards,

[11] CarsBlues Vehicle Hack Exploits Vehicle Infotainment Systems Allowing Access to Call Logs, Text Messages and More https://www.privacy4cars.com/can-my-car-be-hacked/default.aspx

[12] Police warn about car Bluetooth hacking https://www.wilx.com/content/news/Police-warn-about-car-blutooth-hacking--567002751.html

[13] Privacy4Cars and Americas Auto Auction align to offer personal information deletion service https://www.autoremarketing.com/technology/privacy4cars-americas-auto-auction-align-offer-personal-information-deletion-service

such as the “Cybersecurity for IoT Program” published by NIST[14] here in the US or the “Secure by Design” program in the UK[15] and its related extensive study. Some States are already passing laws to require IoTs to adopt “reasonable security standards”, but a standard framework at the Federal level can benefit both the industry and consumers, especially considering Connected and Autonomous vehicles carry a much higher risk potential than most IoTs: hacked vehicles may both cause physical harm to individuals and cripple our country’s infrastructure[16].

Privacy-by-design standards for Connected and Autonomous Vehicles

In 2014 the Alliance of Automotive Manufacturers and the Association of Global Automakers committed to self-regulate and adopt the six Consumer Privacy Protection Principles of Transparency, Choice, Respect for Context, Data Minimization, De-Identification, & Retention, and Data Security[17]. While we applaud the industry’s intent, the current application of those principles is either lacking or insufficient, as determined by many national and international independent studies including the recent “Guidelines on processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications”[18]. For instance, several manufacturers monitor users by default and without explicitly communicating they are being tracked[19], and keep doing so unless users ask to be disconnected (something most wouldn’t know to do or how to do). The data collected and covered by current policies includes behavioral data (e.g. where and how you drive), personal nonpublic information (e.g. who you call, what you text), biometrics (e.g. your weight and increasingly facial recognition), and has retention policies that go as long as 20 years or “as long as necessary” or “according to our data retention policies” which are not disclosed[20]. Companies share this data with a growing set of – again undisclosed – third parties, and also hackers are starting to target data collected by vehicles, as proven by the recent leak of vehicle-

[14] NIST Cybersecurity for IoT Program https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

[15] Secure by Design
The Government's Code of Practice for Consumer Internet of Things (IoT) Security for manufacturers, with guidance for consumers on smart devices at home. https://www.gov.uk/government/collections/secure-by-design

[16] Hackers could use connected cars to gridlock whole cities https://rh.gatech.edu/news/623759/hackers-could-use-connected-cars-gridlock-whole-cities

[17] Privacy Principles for Vehicle Technologies and Services https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf

[18] European Data Protection Board https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_en

[19] For example, Toyota Connected Services states “When you lease or buy a vehicle equipped with Connected Services, data collection is active. You may deactivate Connected Services at any time by contacting us […] If you do not deactivate Connected Services, you specifically consent to our electronic collection and use of your personal information and vehicle data and our storage of such data wherever we designate” https://www.toyota.com/privacyvts/

[20] For example, Hyundai Vehicle Owner Privacy Policy https://www.hyundaiusa.com/owner-privacy-policy.aspx

generated datasets from both manufacturers[21] [22] and fleet and rental operators[23]. This data can be used not only for criminal purposes but also to potentially discriminate against certain segments of the population, as we highlighted over a year ago to the European Data Protection Supervisor's Public Consultation on Digital Ethics[24]. "Would it be possible" we asked, "that two different Autonomous vehicles departing at the same time and the same place, would take different routes (e.g. so they drive by specific stores) or that would have different priority in case of traffic depending on the microprofile (including race, religion, sexual orientation, or party affiliation) of their occupants?" The answer is yes, they could – unless laws prevent this form of discrimination.

At Privacy4Cars we believe that data collection from all Connected or Autonomous Vehicles must be turned off by default and should require a clear, contextual, and highly prominent notice before users agree to sign in. We believe the data cannot be used to discriminate against certain parts of the population. We also believe all players in the automotive ecosystem—including all companies that could potentially have access to any data collected or transmitted by vehicles— should commit to the same principles, and whenever businesses encourage the promiscuous sharing of vehicles across many users (such as Autonomous Vehicles in the future, and today with rental, carsharing, and ridesharing), consent needs to be collected upfront from every user.

Privacy4Cars' statistical evidence also suggests that there is an urgent need to educate vehicle users on the dangers of leaving their Personally Identifiable Information in vehicles they no longer use. The members of this Subcommittee would never agree to hand-over their cell phones—with all their personal data—over to strangers. Yet the same members may have failed to realize that they (and their family members) have essentially done exactly that last time they sold a vehicle, returned a rental car, or shared a car through a subscription or just a ride. The sensible approach, with all Connected and Autonomous Vehicles, is to require the data of the previous owner to be deleted and the connected services to be disconnected, as repeatedly recommended by the FTC since 2016[25] - the year in which you held the first hearing on Autonomous Vehicles.

[21] Toyota Security Breach Exposes Personal Info of 3.1 Million Clients https://www.bleepingcomputer.com/news/security/toyota-security-breach-exposes-personal-info-of-31-million-clients/

[22] Honda Exposes 26,000 Records of North American Customers https://www.bleepingcomputer.com/news/security/honda-exposes-26-000-records-of-north-american-customers/

[23] Buchbinder Car Renter Exposes Info of Over 3 Million Customers https://www.bleepingcomputer.com/news/security/buchbinder-car-renter-exposes-info-of-over-3-million-customers/

[24] Public Consultation on Digital Ethics report https://edps.europa.eu/sites/edp/files/publication/18-09-25_edps_publicconsultationdigitalethicssummary_en.pdf

[25] FTC recommendations: August 2016 https://www.consumer.ftc.gov/blog/2016/08/what-your-phone-telling-your-rental-car August 2018 https://www.consumer.ftc.gov/blog/2018/08/selling-your-car-clear-your-personal-data-first August 2018 https://www.ftc.gov/news-events/blogs/business-blog/2018/08/be-discreet-when-you-delete-your-fleet

Expanding the Driver Privacy Act

NHTSA has long issued recommendations and standards regarding the data collected by Event Data Recorders[26], the "black boxes" that are activated in case of a vehicle collision. In 2015 Congress, as part of the FAST Act, passed the "Driver Privacy Act", stating that vehicles owners should be in control of the data generated by these units. Thanks to this law, accessing the data in the EDR requires a warrant, and this legislation was instrumental in protecting individual liberties and privacy rights in a recent Georgia Supreme Court ruling[27]. Unfortunately, In-Vehicle Infotainment Systems – or any other data collecting computer in vehicles – do not fall under this framework. Considering that most vehicles for sale today are Connected, and that the data they collected through their infotainment, telematics and other systems is even more rich than the one saved by EDRs, this dichotomy between EDR data and other vehicle data is simply anachronistic. Autonomous Vehicles, with their greater array of sensors, will only exacerbate this problem if no action is taken.

A rating system for vehicle cybersecurity and privacy

NHTSA introduced the five-star Safety Rating system in 1993. The Agency is very vocal about the positive impact the rating system has had on saving lives, reducing injuries, and even on economic growth. Consumers have benefited from being able to chose safer vehicles. Businesses have benefited by being able to differentiate their product through safety: an important and valued quality for buyers, but something that was hard for a consumer to individually assess in absence of a rating system. NHTSA's Safety Rating system truly created a virtuous cycle in which businesses built better and safer cars, offered more choice to consumers, and in return were rewarded for their efforts.

Since this Subcommittee already recognized that Connected and Autonomous vehicles pose not only the "traditional" challenges of vehicle safety, but also of cybersecurity and privacy-by-design, we encourage you to follow this successful precedent, and ask NHTSA (o another agency) to be in charge of designing and administering a 5-star rating system for both vehicle cybersecurity and vehicle privacy-by-design. Much of the groundwork has already been laid by NIST who published the aforementioned IoT Cybersecurity guidelines as well as their Privacy framework just last month[28].

Other countries such the UK and Australia already passed a security rating for IoTs, which has already attracted rating agencies to address the development of such tests[29] and has been hailed as a very positive development for the industry and their citizens.

[26] NHTSA Event Data Recorder review https://www.nhtsa.gov/research-data/event-data-recorder#overview-10516

[27] Georgia's Supreme Court issues a landmark decision on vehicle data privacy https://www.cnet.com/roadshow/news/georgia-supreme-court-vehicle-data-privacy/

[28] National Institute of Science and Technology Privacy Framework https://www.nist.gov/privacy-framework

[29] New IoT Security Ratings a Positive Development for Internet of Things https://www.cpomagazine.com/cyber-security/new-iot-security-ratings-a-positive-development-for-internet-of-things/

Federal empowerment to enforce cybersecurity and privacy standards

All the recommended measures above would have little impact without federal oversight. Once again, the historical successful precedent is the role NHTSA has played in watching over vehicle safety. While some argue cybersecurity issues *could* be under the supervision of NHTSA, and privacy issues *could* be addressed by the FTC in collaboration with NHTSA, our experience is that the current setup and non-explicit mandate of those agencies is not conducive to adequately protecting consumers, nor to ensuring a fair and equal application of cybersecurity and privacy guidelines and frameworks for all industry players who today see little incentive to take proactive measures to improve their stance on security and privacy.

We'd like to illustrate this point with an example: in 2018, when our founder responsibly disclosed to 23 automakers and the Auto-ISAC the "CarsBlues" infotainment vulnerability that makes it easy to expose and potentially exploit the personal information of previous drivers without their knowledge, very little action was taken. Some automakers decided to fix the vulnerability… but only for the cars that had not been manufactured yet. Nobody was notified that a potential data breach was easy to perform: not the consumers who bought those vehicles, not the dealers that were reselling them, not the rental and corporate fleets that were putting their customers and employees behind the wheel. NHTSA was notified (as was DHS) in the summer of 2018, but since this hack *only* affects the privacy of the users and not the narrowly defined safe operation of the vehicles (steering, breaking, etc.), the agency had no authority to demand action. This is why, based on our experience, we firmly believe NHTSA (or another federal agency) needs to be officially appointed to oversee the implementation of the other two "pillars" identified by this Subcommittee, cybersecurity and privacy-by-design, in a similar manner and with similar powers as NHTSA does and has in regards to vehicle safety.

Lastly, we want to thank you for the opportunity to provide these comments. Privacy4Cars looks forward to working with any and all stakeholders to address the challenges of safety, cybersecurity, and privacy in this exciting era of Connected and Autonomous Vehicles. We welcome the opportunity to be a resource for this Subcommittee in the areas of industry data, insights, or expertise.

Respectfully submitted,

Privacy4Cars, LLC
info@privacy4cars.com