

28 April 2017

Input on Benefits and Privacy and Security Issues Associated with Current and Future Motor Vehicles

Re: Connected Cars Workshop and P175403; CDT Submission to the FTC and NHTSA joint workshop on connected cars

The Center for Democracy & Technology (CDT) thanks the FTC and the NHTSA for the opportunity to provide input on the benefits and privacy and security issues associated with current and future motor vehicles. This call for input is, in of itself, a welcome recognition of the issues that this impending wave of technological change is likely to bring. It is also an important step in informing and preparing decision-makers in the public and private sectors for these changes so as to maximize its benefits while mitigating the costs linked to vehicle security, driver privacy and autonomy, and other risks that will emerge.

The continuing shift toward automated, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) -enabled, and otherwise connected vehicles (collectively “connected vehicles”) involves five linked changes:

1. Addition of new software to motor vehicles;
2. Addition of internet connectivity in the operation of motor vehicles;
3. Addition of a new role for critical information infrastructure operators in the broader motor vehicle stakeholder group;
4. Creation of dependence/reliance on the reliable functioning of critical information infrastructures; and
5. Creation of new systemic risks, due to greater connectivity and centralized control from critical information infrastructures.

With this in mind, our comments focus on the following issues:

(1) a need for measures to ensure more secure software in motor vehicles;

(2) a need to consider the new and vital role that critical information infrastructure providers will play with connected cars, and the associated systemic risks associated with this role; and

(3) a need for additional transparency with respect to data privacy in motor vehicles, specifically as to how vehicle data can be used and shared, and further thinking over what controls and rights to vehicle data are appropriate for drivers and vehicle owners.

A nonprofit advocacy organization, CDT works to promote democratic values by shaping technology policy and architecture, with a focus on the rights of the individual. CDT supports laws, corporate policies, and technological tools that protect privacy and security and enable free speech online. Based in Washington, D.C., and with a presence in Brussels, CDT works inclusively across sectors to find tangible solutions to today's most pressing technology policy challenges. Our team of experts includes lawyers, technologists, academics, and analysts, bringing diverse perspectives to all of our efforts.

Ensuring more secure software in motor vehicles

Software in motor vehicles is not new. Digital security expert Bruce Schneier refers to motor vehicles as, “a computer with four wheels and an engine.”¹ Unfortunately, the security issues with the complexity and interdependence of the software systems within motor vehicles (and more broadly in the software industry) have not been resolved.

Unfortunately, there is no way to design a ‘simple’ modern motor vehicle. In the past, software-based components were functionally and technically isolated and did not relate (or connect) to one another. There were few nodes within the vehicle running relatively little software with a minimum amount of abstraction applied.

Over the intervening 30 years, vehicles have evolved substantially. The average vehicle on the road today has upwards of a 100 separate electronic control units (ECUs) that monitor and control individual vehicle systems. These systems are comprised of hundreds of millions of lines of code.² Alfred Katzenbach, the director of information technology management at Daimler, reportedly said that the radio and navigation system alone in the S-class Mercedes-Benz requires over 200 million lines of code.³ This code provides for 270 user functions, which are a result of combining 2000 software functions (which are not all directly user interaction functions). Many functions are reliant on other functions, which implies complex interdependencies, and results in unintentional feature interaction. Functions are also grouped into subsystems, which are typically allocated to the majority of mechanical components of the vehicle (e.g. engine, drivetrain, body, comfort systems). These subsystems are dependent on decisions made by functions in other subsystems, further increasing the complexity of the interactions.

Given this complexity, it is likely that there are already a substantial number of bugs in existing motor vehicle software. This problem will become more acute as more software is added. A speculative estimate suggests that software bugs in motor vehicles are already numerous. Steve McConnell

¹ Bruce Schneier (2017), “Security and the Internet of Things”, https://www.schneier.com/blog/archives/2017/02/security_and_th.html

² David Gelles, Hiroko Tabuchi & Matthew Dolan, Complex Car Software Becomes the Weak Spot Under the Hood, N.Y. Times (Sept. 26, 2015), <http://www.nytimes.com/2015/09/27/business/complex-car-software-becomes-the-weak-spot-under-the-hood.html>.

³ Robert Charette (2009), “This car runs on code”, IEEE Spectrum, <http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code>

estimates that programmers make between 10 and 50 errors in for every 1,000 lines of code. Careful checking at big software companies, he says, can push that down to 0.5 per 1,000 or so.⁴ With these assumptions, one might estimate that the typical motor vehicle on the road already has at least 50,000 bugs in its software. These bugs will vary in their relative seriousness. Estimates converge at approximately 15-25% of bugs being deemed critical in any given year.⁵ That equates to perhaps 15,000-25,000 such bugs in a motor vehicle with 200 million lines of code. While not all software on cars is safety critical, the interdependencies between ECUs, and the difficulties in understanding these interdependencies owing to multiple suppliers providing each individual software component, mean that unpredictable outcomes relating to safety-critical software may eventuate and impose severe costs or injury⁶. Examples of this have already occurred. In 2011, security researchers, “remotely attack[ed] multiple [GM] vehicles’ safety-critical systems through short- and long-range wireless channels without physical access to the target vehicles.”⁷ In 2015, a recall of 1.4 million Chrysler, Dodge and Jeep vehicles was conducted due to a security vulnerability in the UConnect entertainment system, which allowed a malicious actor to turn off the engine, unlock the car, and control the steering wheel, brakes, transmission, and acceleration.⁸ More such incidents will be highly likely in the future as additional software is added to motor vehicles.

As we noted in comments regarding NHTSA’s Federal Automated Policy Guidance,⁹ motor vehicle security research is in its infancy, and public information about the state of automotive security is lacking in general. This is a concern given the very high likelihood of extensive bugs in existing motor vehicle software. No studies about bugs in vehicle software have been made publicly available at present.¹⁰ This is perhaps the result of a lack of collaboration, auditing and cybersecurity information

⁴ The Economist (2017), “Why computer security is broken from top-to-bottom”, <http://www.economist.com/news/science-and-technology/21720268-consequences-pile-up-things-are-starting-improve-computer-security>

⁵ Symantec (2016), “Internet Security Threat Report 2016”, <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>; Risk Based Security (2016), “Year End Vulnerability Quickview Report”, <https://pages.riskbasedsecurity.com/2016-ye-vuln-quickview>; Jim Bird (2011), “Bugs and Numbers: How many bugs do you have in your code?”, <http://swreflections.blogspot.com/2011/08/bugs-and-numbers-how-many-bugs-do-you.html>

⁶ Manfred Broy, Ingolf Kruger, Alexander Pretschner and Christian Salzmann (2007), “Engineering Automotive Software”, Proceedings of the IEEE, Vol. 95, No. 2, February 2007.

⁷ Stephen Checkoway, Damon McCoy, Danny Anderson, Brian Kantor, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno, Comprehensive Experimental Analyses of Automotive Attack Surfaces, Proceedings of the USENIX Security Symposium (San Francisco, CA: August 2011); in GAO (2016), “Vehicle Cybersecurity: DOT and industry have efforts under way, but DOT needs to define its role in responding to a real-world attack”, GAO-16-350, March 2016.

⁸ Andy Greenberg (2015), “Hackers remotely kill a Jeep on the highway - with me in it”, Wired, <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

⁹ Comments by the Center for Democracy & Technology on the Federal Automated Vehicles Policy, NHTSA Docket No. 2016-0090-0001, at 8 (Nov. 22, 2016), https://cdt.org/files/2016/11/NHTSA_FAVP_Comments_11_22_16.pdf.

¹⁰ Why no such studies are available, after over 30 years of software being in motor vehicles, is an interesting but separate matter.

sharing between stakeholders. A GAO report that surveyed motor vehicle stakeholders found that parts suppliers feel that, “the security requirements they receive from automakers often lack sufficient context about the broader component or system.”¹¹ Other stakeholders claim that, “it can be difficult for automakers to oversee and exert control over suppliers’ software code.” The incorporation of additional technologies associated with connected vehicles on top of this legacy automotive software architecture will add new threat vectors to what is already a very large attack surface.¹² Connectivity will subject vehicles to an increasing and systemic risk of attack that could pose potential economic costs (and loss of life) more traditionally associated with those presented by aviation. It is therefore essential that these long-standing issues in software industry be better addressed before layering further complexity on this already highly complex system.

As software has become more-and-more a part of the modern motor vehicle, the safety and reliability of the software has not been held to as high a standard as that in other transport fields, like aviation. This needs to change. The amount of error diagnosis and error recovery in cars is limited. In avionics, hardware and software redundancy are standard techniques. In motor vehicles though, such extensive error treatment is not found. According to the GAO, “there are no widely accepted cybersecurity performance metrics, and it is difficult to prove that a vehicle with up to 100 million lines of code is secure... testing every line of code in a vehicle would take several months, which is not feasible or practical.”¹³ The reliability of software in cars does not reach the high level of avionics software, which has to reach a reliability of 10^9 hours mean time between failures. Such a reliability standard in motor vehicles, as of 2007, was not known.¹⁴

Automotive safety rules and regulations are well established. A system of standards, testing, product liability and other public policies have been developed and implemented since the 1970s to raise the level of automotive safety. However, a similar body of safety (or security) rules and regulations have not been developed and implemented for software development. The “security vulnerabilities” that currently affect connected computing platforms are still present, 30 years after the first personal computers went on the market and 20 years after the commercialization of the internet, partly because of the lack of a body of safety (or security) rules and regulations in this area.¹⁵

¹¹ GAO (2016), “Vehicle Cybersecurity: DOT and industry have efforts under way, but DOT needs to define its role in responding to a real-world attack, GAO-16-350, March 2016.

¹² Alex Kreilein (2017), “Dedicated Short Range Communications (DSRC) Expose Critical Gaps in Security and Privacy”, SecureSet, <http://glenechogroup.isebox.net/securesetaccelerator/dedicated-short-range-communications-dsrc-expose-critical-gaps-in-security-and-privacy>

¹³ GAO (2016), “Vehicle Cybersecurity: DOT and industry have efforts under way, but DOT needs to define its role in responding to a real-world attack, GAO-16-350, March 2016.

¹⁴ Ibid.

¹⁵ For a more complete explanation of some of the reasons for the current poor state of digital security, see p20-24 of MIT Center for International Studies and MIT Internet Policy Research Initiative (2017), “Keeping America Safe: Toward more secure networks for critical sectors”, Report on a series of MIT workshops 2015-16 with recommendations for a new administration”, available from: <http://internetpolicy.mit.edu/reports/IPRI-CIS-CriticalInfrastructure-2017-Brenner.pdf>

This is an ideal time to begin considering how such a body or safety rules and regulations might be developed for software in connected vehicles. Without development of these rules and regulations, we risk repeating the mistakes of the past, where poor safety standards in motor vehicles led to tens of thousands of unnecessary deaths as well as avoidable personal injury and property damage.¹⁶ CDT recommends that discussion on measures to address and reduce these security issues/risks be undertaken through the Automotive Information Sharing and Analysis Center (Auto-ISAC). The Auto-ISAC has made great strides in short time, releasing a framework for automotive cybersecurity best practices in January 2016 and announcing in July 2016 that it had established a set of industry best practices. It also recognizes the need to collaborate and engage with “appropriate third parties.” This makes it a suitable forum for stakeholder engagement. Specific areas for discussion include, but are not limited to: development of minimum ‘safe’ software development standards; development of agreed upon software testing standards; and allocation of liability to developers of ‘faulty’ or ‘defective’ software. CDT is undertaking research and engaging stakeholders in order to determine whether there are critical protections that must be in place and plans to further identify such protections in the future.

Additional vehicle connectivity creates new security risks

While software in automobiles is not a new phenomenon, connecting vehicular technologies to the internet for the purposes of basic vehicle operation is. Over the past decade, motor vehicles have transitioned from a pure information hub to an information/communication hub.¹⁷ As the joint workshop’s detailed public notice acknowledges, “These internet-connected vehicles may face many of the same security vulnerabilities as other connected computing platforms”. Moreover, in recent study by the Government Accountability Office, the majority of industry stakeholders (23 of 32; ~72%) acknowledged the risk of, “wireless attacks, such as those exploiting vulnerabilities in vehicles’ built-in cellular-calling capabilities, would pose the largest risk to passenger safety.”¹⁸ CDT agrees that protecting the security of these vehicle technologies is crucial to maintaining adequate privacy and safety protections. Moreover, CDT would like to emphasize that these security vulnerabilities are likely to be compounded due to the additional complexity that will characterize the intricate interactions between software within motor vehicles; between motor vehicles; and between motor vehicles and critical information infrastructure providers.¹⁹

¹⁶ It should be noted that these rules and regulations only came into effect 50 years after the first Ford Model T cars reached the market. It was only after the widespread adoption of motor vehicles, coupled with acknowledgement of the poor design and manufacturing practices that characterized these motor vehicles, and the deaths that this caused, that the rules and regulations were implemented.

¹⁷ Ibid.

¹⁸ GAO (2016), “Vehicle Cybersecurity: DOT and industry have efforts under way, but DOT needs to define its role in responding to a real-world attack, GAO-16-350, March 2016.

¹⁹ Schneier (2017); “More complexity means more people involved, more parts, more interactions, more mistakes in the design and development process, more of everything where hidden insecurities can be found.”

The increasingly central role of critical information infrastructures and new systemic risks

The automotive industry is characterized by its many stakeholders, which in the FTC/NHTSA workshop notice include, “vehicle manufacturers, parts supplies, technology companies, and other stakeholders.” With increasing connectivity, a new stakeholder group is entering the mix: critical information infrastructure providers.

This sub-set of technology companies includes network-level connectivity (internet service providers, wireless providers), transport-level connectivity (TCP/UDP, Domain Name System), and application-level connectivity (TLS, HTTPS, etc.). This broad variety stakeholders will play a vital role in ensuring the reliable and smooth functioning of a network of connected vehicles.

As software and connectivity continue to be integrated into motor vehicles, these vehicles will subsequently become dependent on functions such as access provision, DNS translation, and application-level connectivity with the car manufacturer. Consider the consequences on connected vehicles if the Domain Name System were to be disrupted as it was on 21 October 2016, when DNS provider, Dyn, was subject to two unprecedentedly high-powered distributed denial of service (DDoS) attacks. The attack was linked to the Mirai botnet, which exploits well-known attack vectors, such as default passwords and the outdated TELNET service, contained in ‘Internet of Things’ devices (e.g. DVR players, surveillance cameras), then uses these devices to send enormous amounts of traffic to certain targets.²⁰ The attacks flooded the Dyn servers with over one terabyte of traffic per second until the system could no longer handle the high level of traffic. Once down, an estimated 1,200 websites could no longer be accessed by end users on both sides of the Atlantic. Some notable sites included PayPal, Twitter, Amazon, Netflix and Spotify.²¹ Were such an incident to occur, with connected vehicles relying on the DNS, the outcome would result in severe disruption of connected vehicles themselves and possible damage or injury to individuals. Moreover, without sufficient security measures being implemented, connected vehicles themselves run the risk of becoming part of such botnets (or, worse, other attacks such as ransomware).

The Dyn/DNS example points to the need for connected vehicles to be able to operate without guaranteed access to these resources, short of regulations to ensure 100% uptime.

²⁰ Eyal Ronen, Colin O’Flynn, Adi Shamir and Achi-Or Weingarten (2017), “IoT goes nuclear: creating a ZigBee chain reaction”, <http://iotworm.eyalro.net>

²¹ Gallagher S. (2016), “How one rent-a-botnet army of cameras, DVRs caused Internet chaos”, Ars Technica, available from: <https://arstechnica.com/information-technology/2016/10/inside-the-machine-uprising-how-cameras-dvrs-took-down-parts-of-the-internet/>

Moreover, vehicles will have to have some capability to communicate with other vehicles and infrastructure without global network connectivity. This communication capability will, in turn, create even more systemic risks. In an example from an adjacent 'Internet of Things' field, security researchers were able to bypass security measures, like encryption, and exploit the Zigbee protocol, which is a radio link between many IoT devices, in a way that reset and could potentially 'brick' (render inoperable) thousands of Philips Hue smart lamps.²² After disclosing the bugs that allowed this exploit to the manufacturer, the researchers warned that, "this is only a small example of the large scale problems that can be caused by the poor security offered in many IoT devices." Connected vehicles are one such example where such large-scale problems might emerge for similar reasons.

An underappreciated safety property of the current motor vehicle/traffic system is that it is highly distributed and adaptive. That is, the end 'nodes' (the cars and the drivers within them) are not reliant upon other cars – or a central planning entity – to operate safely and avert emergent hazards or dangers. The downside to this system is that each 'node' (driver) has to pass a basic driving test in order to be certified to drive. The motor vehicles themselves have undergone substantial design changes over many decades in order to accommodate important safety features so as to mitigate the impact of accidents.

These new dependencies and their associated systemic risks, associated with critical information infrastructures and connectivity protocols, can't be controlled or reduced through mandated basic competence for human drivers and the existing regulations governing car manufacturers own responsibilities to ensure fitness for purpose. New policy measures have to be instituted to manage these dependencies and risks.

Much attention is paid to the safety benefits that will accrue from moving to the automation of motor vehicles. Increasingly the task of driving will not be done by a human in the car but, rather, will be done by some other entity (some combination of algorithms and artificial intelligence in the cloud controlling on-board software and hardware). It is thought that this will provide efficiency gains, due to less traffic, and reduce motor accidents and associated injury or death (some estimates place the proportion of accidents due to human error at 94%).²³

Yet at the same time, these incremental efficiency gains come from optimizing a system using connectivity. In turn, this reduces redundancy and the ability to localize failure. When failure occurs, it can do so quickly, owing to less redundancy, and can propagate through a network with high connectivity between nodes. This is typical of a so-called 'fat-tailed' domain.²⁴ By avoiding a large

²² Eyal Ronen, Colin O'Flynn, Adi Shamir and Achi-Or Weingarten (2017), "IoT goes nuclear: creating a ZigBee chain reaction", <http://iotworm.eyalro.net>

²³ GAO (2016), "Vehicle Cybersecurity: DOT and industry have efforts under way, but DOT needs to define its role in responding to a real-world attack, GAO-16-350, March 2016.

²⁴ This is a property of domains characterized by 'fat tailed' outcomes. See: Nassim Nicholas Taleb (2006), "The Black Swan: The Impact of the Highly Improbable", Random House: New York.

number of small accidents, if appropriate measures are not taken, the outcome is likely to be a small number of large, system-wide accidents, larger by orders of magnitude and potentially system-ending.

Given that this is an emerging phenomenon, a framework for crisis planning and response does not currently exist for critical information infrastructures with relation to connected vehicles. The GAO recommended that DOT define its role in responding to a real-world attack in a March 2016 report.²⁵ CDT suggests that the FTC and NHTSA convene relevant stakeholders (DOT, automotive companies, critical information infrastructure operators, software developers, etc.) to develop such a crisis framework based on a discussion of: the probability of certain incidents; measures to mitigate these incidents and, in instances where mitigation is deemed infeasible or excessively costly, development of crisis response measures to be taken once an incident occurs.

Further transparency and control over vehicle data use and sharing

Privacy and security features can be important differentiators in vehicle purchasing decisions, but this requires much more meaningful transparency across the automotive ecosystem.²⁶ Security challenges may predominate regulatory interest and public discussion, but the privacy and autonomy interests of vehicle drivers and owners should not be discounted.

Connectivity significantly impacts privacy and autonomy. Forty-five percent of new car buyers are concerned about the privacy impacts of new in-car technologies,²⁷ yet NHTSA, in its proposed V2V rulemaking, acknowledged only a “perceived privacy loss” as a cost of V2V communications.²⁸ Though the exact impact on individual privacy may be difficult to measure or predict, there is no doubt that connectivity poses a real loss of privacy. The automotive industry has not traditionally had access to the steady stream of digital information available to other consumer-facing technology companies, and

²⁵ GAO (2016), “Vehicle Cybersecurity: DOT and industry have efforts under way, but DOT needs to define its role in responding to a real-world attack, GAO-16-350, March 2016.

²⁶ *E.g.*, Ben Stanley, How To Protect Data Privacy Of Connected Cars As Their Popularity Accelerates (Jan. 11, 2017), <https://www.forbes.com/sites/ibm/2017/01/11/how-to-protect-data-privacy-of-connected-cars-as-their-popularity-accelerates/#418785775e95> (noting that 56% of consumers state that privacy and security are key differentiators in future vehicle purchasing decisions). As suggested above, transparency around data and device security will be especially important. Automakers should commit to providing more details about vulnerabilities and offer consumers tools to validate whether their connected car is up-to-date and secure. *Ibid.*

²⁷ McKinsey & Co., *What's Driving the Connected Car?*, <http://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car> (last visited Nov. 15, 2016).

²⁸ See Comments by Leonid Reyzin, Anna Lysyanskaya, Vitaly Shmatikov, and Adam D. Smith, and the Center for Democracy & Technology on the NHTSA Notice of Proposed Rule for FMVSS No. 150, V2V Communications, Docket No. NHTSA-2016-0126 (Apr. 12, 2017), <https://cdt.org/files/2017/04/FMVSS150CommentsOnPrivacy-as-submitted.pdf>.

it recognizes that connectivity offers ample opportunities to engage in forms of driver monitoring and highly-tailored marketing.²⁹

Responding to these concerns, nineteen automakers adopted in 2014 a set of “Privacy Principles for Vehicle Technology and Services” that went into effect for model year 2017.³⁰ When announced, CDT was supportive of the principles, while noting that further steps could be taken to improve the framework.³¹ Two-and-a-half years later, it continues to be unclear what precisely the principles require of automakers. Automakers have argued that the principles go beyond similar industry efforts, and this joint workshop offers a timely opportunity to reexamine and reassess their efficacy.

Several issues worth considering include:

- (1) What sorts of notice and transparency are being provided with respect to vehicle connectivity?** The principles place significant emphasis on providing clear and meaningful notice of vehicle data practices, yet privacy advocates have cautioned that the principles generally encourage longer and more confusing policy documents and terms of service rather than clear or meaningful notice of in-car data practices.³² While legislators have called for “cyber dashboards” and other types of data collection comparison tools, industry has generally defaulted to providing notice via online privacy statements or user manual addenda.
- (2) What data use and sharing options are being provided to vehicle owners?** The principles provide for user choice in the collection, use, and sharing of certain limited types of information, but include broad exceptions for such controls when data is used for safety, operations, or compliance purposes. The sphere of vehicle functionality that is captured by this exception will only grow as vehicles add further connectivity features, leading some critics to suggest that car buys are being forced to consent to the sharing of their data simply as a condition of being a new car, which is hardly a meaningful choice.³³

²⁹ Richard Viereckl et al., PwC, Connected Car Report 2016 (Sept. 28, 2016), <http://www.strategyand.pwc.com/reports/connected-car-2016-study> (PwC’s report encourages companies to “use your data,” calling it “an opportunity not to be missed.”).

³⁰ Consumer Privacy Protection Principles, Alliance of Automobile Manufacturers (Nov. 12, 2014), *available at* <http://www.automotiveprivacy.com> [hereinafter Privacy Principles].

³¹ Brian Fung, *A Privacy Policy for Cars*, Wash. Post (Dec. 9, 2014), <https://www.washingtonpost.com/news/the-switch/wp/2014/12/09/a-privacy-policy-for-cars-what-automakers-know-about-you-and-what-theyre-doing-with-it/>.

³² BC Freedom of Info. & Privacy Assoc., *The Connected Car: Who Is in the Driver's Seat?* 94 (2015), https://fipa.bc.ca/wordpress/wp-content/uploads/2015/05/CC_report_lite-1v2.pdf; *see also* Comments of the Electronic Frontier Foundation on NHTSA’s Federal Automated Vehicles Policy, Docket: NHTSA-2016-0090 (Nov. 22, 2016).

³³ Ryan Beene & Gabe Nelson, *Automakers adopt protocols to handle, protect consumer data in connected car era* (Nov. 13, 2014), <http://www.autonews.com/article/20141113/OEM11/141119926/automakers-adopt-protocols-to-handle-protect-consumer-data-in>. For instance, Tesla, which is not a signatory to the Privacy Principles, explains that failure to share vehicle data may result in not just reduced functionality but serious damage or interoperability problems.

- (3) How are automakers operationalizing the data minimization, de-identification, and retention principles?** It remains unclear what constitutes effective de-identification of vehicle data. Researchers have shown that it is possible to accurately identify drivers using limited amounts of sensor data collected from existing vehicles on the road. (Drivers could be identified with 87% accuracy, using only the positioning of the brake pedal after monitoring fifteen minutes' worth of driving; the number jumped to 99% accuracy when access was granted to additional driving behavior and sensor data.³⁴) Like similar sorts of digital fingerprinting based upon device or browser settings, an “automotive fingerprint” can be derived based on individual driver patterns or vehicle usage. It is also unclear how effective automakers and their suppliers' methods of de-identification are. One GAO study concluded that in-car location based services were using different de-identification methods, impacting the extent to which drivers could be easily re-identified or otherwise exposed to privacy risks.³⁵
- (4) Which entities and services are outside the scope of the Privacy Principles?** The “Accountability Principle” obliges automakers to take steps that entities that receive certain covered information also abide by the principles, but the principles also concede that their obligations apply only to signatory automakers. As a result, the principles do not cover car dealerships, insurers, or aftermarket suppliers, and as car companies engage with startups and other technologies companies to provide connectivity products and services, the functional reach of the principles may be limited.

While the principles may provide a floor with respect to vehicle privacy, automakers had suggested that the principles would facilitate turning privacy into a market differentiator. Features such “private driving modes” akin to private web browsing were touted as one potential mechanism to explore to give drivers control over sensitive driving episodes (e.g., driving to a hospital or rehabilitation facility), but little has come of this. CDT recommends that the joint workshop explore how automakers have implemented the privacy principles and address where specifically there remains room for improvement. If drivers are not afforded suitable controls – or ownership – over the data their vehicles generate, use restrictions will be necessary to ensure connectivity does not come at the cost of constant surveillance and diminished consumer privacy and autonomy.

Conclusion

Connected vehicles have tremendous potential to reshape the transportation landscape – bringing benefits but also creating new security and privacy risks to be managed. Long-standing issues with the software that is already within motor vehicles today will be compounded as even more software is layered on top of this legacy code. There is a need to address these software-related issues, potentially through the Auto ISAC. Connectivity brings with it systemic risks due to increased dependence on

³⁴ Miro Enev et al., *Automobile Driver Fingerprinting*, Proceedings on Privacy Enhancing Technologies (2016).

³⁵ GAO (2013), “In-Car Location-Based Services: Companies Are Taking Steps to Protect Privacy, but Some Risks May Not Be Clear to Consumers,” GAO-14-81, Dec. 2013 <http://www.gao.gov/products/GAO-14-81>.

critical information infrastructures. There is a need to better plan for the inevitable disruption or potential failure of these critical information infrastructures. Car owners and drivers also need to be further empowered to control these connectivity features, and regulators should encourage the automotive ecosystem to be more transparent about how it is deploying and security these technologies and to offer additional control over how vehicle data is collected, used, and ultimately shared.

CDT encourages the FTC and NHTSA to consider the privacy and security concerns highlighted in these comments. Thank you for the opportunity to provide comments on this most important subject area. We welcome any questions or comments and look forward to the workshop in June 2017.

Sincerely,

Benjamin C. Dean
Ford/MDF Technical Exchange Fellow, CDT

Joseph W. Jerome
Policy Counsel, Privacy & Data, CDT