May 1, 2017

Intelligent Car Coalition
1155 F St, NW
Suite 1050
Washington DC 20004

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Suite CC-5610
Washington, DC 20024

RE: Request for public comments Project No. P175403
Submitted online to: https://ftcpublic.commentworks.com/ftc/connectedcarsworkshop/

I. Introduction.

The Intelligent Car Coalition (ICC) respectfully submits these comments ahead of the workshop to be held by the Federal Trade Commission (FTC) and National Highway Traffic Safety Administration (NHTSA) on Privacy and Security Issues Related to Connected and Automated Vehicles to be held June 28, 2017.

The merging of communications technologies with automotive transportation is creating exciting opportunities to make us safer on the roads, reduce our carbon footprints, and improve our quality of life. The ICC was formed to address public policy questions created in this new space. The ICC gathers leading stakeholders in the automotive, communications and technology industries for cross-industry discussions of policy issues and advocates for innovation in connected and automated vehicles.¹ We believe these technologies will benefit not only

¹ Members of the Intelligent Car Coalition include AT&T, the Alliance of Automobile Manufacturers, CTIA, Drive Spotter, HARMAN, the Association of Global Automakers, and Verizon.
individual consumers, but also our society as a whole, and we want public policies that speed beneficial technologies to market.

We have entered a transformative age of automotive mobility characterized by use of a new tool: digitized data. Data – flowing over wireless infrastructure between vehicles and the road, between vehicles and road infrastructure, between the vehicle and trusted third parties over the internet, and among vehicles – is the backbone of automated and connected vehicle systems. Therefore, it is important that the ecosystem provides consumers the confidence that the data flowing through vehicle and infrastructure systems is protected. This will encourage advanced technologies adoption – which is vital for society to fully realize the benefits of these technologies.

Vehicles that can communicate with other vehicles, road infrastructure, first responders, and vulnerable road users will provide many efficiencies and save us time, money, and frustration. But chief among the benefits of automated and connected technologies is safety. It is estimated that over 35,000 people die on our roads each year.\(^2\) The use of automated and connected vehicles has the potential to significantly reduce that number.\(^3\) In addition, other high-speed, low-latency wireless connections that deliver people the data they need to make better decisions on our roads can save even more lives – by performing functions such as alerting pedestrians and cyclists to nearby vehicles, notifying owners to vehicles’ mechanical problems before they break down on the side of the road, alerting emergency medical services to crash locations, allowing cities to time traffic lights to reduce crash risk, giving drivers real-time information about road and weather hazards, and much more.\(^4\)

II. Data is Different.

In some ways data is a unique tool. First, data has unique power: the capture, analysis, and deployment of data allows for far better decision-making. This is a particularly powerful tool when it comes to driving; a driver or machine with greater situational awareness has the best chance of avoiding a crash or mitigating injury. With 94% of crashes attributable to human error, even lower levels of automated vehicle systems can leverage data to support the driver, and therefore improve in the chance that a crash could be avoided or mitigated.

Second, data is unique in its speed of evolution. The ability of data to rapidly be compiled into a beneficial technology, or help a product evolve into a better form, means that when


\(^{4}\) *Id.*, p. 9-11.
applied to the field of transportation, data technologies can speed us to achieve what no other tools have yet – safer mobility, cleaner air, and more efficient movement on our nation’s roads. Of course, mechanical tools also have the ability to be improved. But the exponentially faster production cycle of digital, data-based technologies means that stopping to examine them at every stage of evolution will impede their growth, and potentially keep their life-saving benefits from the public. In other words, allowing fast-developing data-based technologies to ‘hit the road’ sooner can lead to safer outcomes for road users.

Third, data possesses a unique growth effect: it can be fruitful and multiply in an environment made safe for sharing. Take, as one example, real-time traffic information services. By crowdsourcing data, it is possible to provide information on traffic conditions, potential road hazards, traffic signage and on-street parking in real time. Drawing data from a voluntary ‘crowd’ of sensors allows multiple drivers to create a new ‘product’ of situational awareness for every other driver who utilizes the data in a different location.

Fourth, data-based technologies have significant collateral benefits: the ability of data to be shared means its benefits can be shared too. In the crowdsourced data example, each individualized data ‘product’ can be used by a driver to avoid congestion, or even avoid a crash. In this way, the crowdsourced data flows to an individual’s benefit, but it also creates societal benefits – by reducing traffic congestion, reducing crashes, and possibly saving lives.

### III. Consumer Data Accelerates Technology Development.

The traditional automotive ecosystem counted OEMs, suppliers and regulators as the main arbiters of automotive technology. However, in the connected, automated ecosystem consumers play a more powerful role. Technologies in this new ecosystem can be quickly created and may be speedily modified to account for consumer demand. In addition, thanks to the internet, consumers can interface with manufacturers of technology both more directly and more extensively than in the past. Consumers have more opportunities for input – and as a result, better leverage in the marketplace.

Consumers’ feedback can inform a shortened design process for the overall vehicle platform, and enable updatable digital components and modifiable consumer-discretion technologies such as plug-ins and apps. In this way, consumers influence product design through insights from the data they generate. Examples include everything from data gleaned by manufacturers on the performance of automated vehicle systems, to information on the performance of individual auto components, and more.

In addition, this new marketplace has attracted companies that compete to provide an expanding array of services by leveraging technologies in this new ecosystem. In turn, this competition expedites development of even more technologies. In other words, the pace at which many of these technologies can be created and modified to fit the consumer – combined
with consumers’ power to personalize the driving experience and the increased market presence of companies willing to create new solutions for drivers – means that consumers are now placed at the center of the automotive value chain.\(^5\)

**IV. Consumers Make Risk/Benefit Calculations When Deciding Whether to Share their Data**

Just as better data can help lead us to better outcomes, restricting the flow of data can limit its usefulness. Flow can be restricted by curtailing the means by which it moves (for instance, because of lack of spectrum, or absence of the physical infrastructure necessary for robust communications networks). Inappropriate regulation also restricts data flow by dis-incentivizing those who create it and allow it to be shared.

One way consumers may be dis-incentivized to share data is if they believe it is subject to collection by government agencies without consumers’ permission. Consumers see a difference between sharing information with an entity to which they have given permission to access data, versus having data about them used without their prior agreement\(^6\),\(^7\) (as can happen in the case of government surveillance). Consumers are able to control their relationships with private parties by via specific terms in user agreements, but consumers have no such control when it comes to government collection of their information.

We know that this is one of the factors consumers consider when evaluating the information they may want to share. Research by the Pew Research Center notes that “For most


\(^6\) “C]ustomers are increasingly aware of and interested in the benefits related to car data-enabled features and services...[they are m]ore willing to consciously grant access to their data (79 percent of globally surveyed)...however...[a] more granular look at consumer openness to data sharing reveals persistent cautiousness and fear that certain data types, perceived as privacy critical, could be misused.” *Monetizing Car Data: New Service Business Opportunities to Create New Customer Benefits*, McKinsey & Company, p. 14 (Sept. 2016). http://www.mckinsey.com/industries/automotive-and-assembly/our-insights/monetizing-car-data

\(^7\) “93% of adults say that being in control of who can get information about them is important; 74% feel this is ‘very important,’ while 19% say it is ‘somewhat important.’” *Americans’ Attitudes About Privacy, Security and Surveillance*, Pew Research Center, Mary Madden and Lee Rainie, p. 4 (May 20, 2015). http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

“Americans say they do not wish to be observed without their approval; 88% say it is important that they not have someone watch or listen to them without their permission (67% feel this is “very important” and 20% say it is ‘somewhat important’),”...Just 6% of adults say they are ‘very confident’ that government agencies can keep their records private and secure, while another 25% say they are ‘somewhat confident.’” *Id.*, pp. 4, 6.
Americans who are making decisions about sharing their information in return for a product, service, or other benefit, the context and conditions of the transactions matter... Risk-benefit calculations that enter people’s minds during the decision process include the terms of the deal... whether they consider the company or organization involved to be trustworthy...

Unfortunately, Pew has found that the government is not well-trusted to keep consumers data private and secure. One statistic cited by a September 2016 Pew survey found that 54% of Americans are ‘not too confident’ or ‘not at all confident’ that government agencies can keep their records private and secure. In addition, Pew found consumers want control over how their information may be used. Specifically, the survey said 74% of respondents said it is ‘very important’ to them that they be in control of who can get information about them, and 65% said it is ‘very important’ to them to control what information is collected about them.

V. Automakers and their Technology Partners have been Working Individually and Together to Make the Connected and Automated Vehicle Ecosystem a Safe Place to Share Data

The wireless industry, which has protected consumer data use for many years, has long been committed to privacy practices that empower consumers to make choices about how their data is shared. Likewise, when it became clear the future of the auto industry would involve connected and automated vehicles, the Alliance of Automobile Manufacturers and Association of Global Automakers gathered their members and issued their Consumer Privacy Protection Principles, which apply to the collection, use and sharing of information in association with vehicle technologies. These principles cover identifiable information that vehicles collect, generate, record or store, or personal subscription information provided by individuals subscribing to registering for vehicle technologies and services.

In addition to working with their agencies of regulatory jurisdiction on cyber security issues, both the wireless and automotive industry have been proactive and driving forces behind many other initiatives to secure networks, vehicles, and wireless software and devices. For instance, much of the $150 billion wireless providers have spent since 2010 to build and improve the networks relied upon by connected and automated vehicle technologies has been aimed at making those networks secure for consumers.

---

9 Id.
In addition, wireless carriers, device manufacturers and software providers participate in cybersecurity information sharing activities like the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the automotive industry’s Automotive Information Sharing and Analysis Center (Auto-ISAC), which automakers established in 2015 as a secure forum to voluntarily share threat information among members. The Auto-ISAC is also creating and maintaining a series of Automotive Cybersecurity Best Practices that expand on a framework established by the Auto Alliance and Global Automakers in 2016.14

VI. Conclusion.

Our nation is likely on track to lose over 35,000 Americans on our roads this year.15 While newer cars provide enhanced safety protections,16 the vast majority of crashes are still attributable to driver error.17 For these reasons, adoption of connected and automated technologies that reduce the chance of errors in the driving task will play a major role in reducing that number.

When data is interrupted by inappropriate public policy, it can be made unusable. Many of the societal benefits of these systems come from sharing vehicle data voluntarily with trusted private parties. Without this sharing, we miss out on benefits not just as individual consumers, but also for our society as a whole. Any regulatory action in this area should be thoughtful, and should be calculated to avoid inappropriate intrusion into an ecosystem that has created a beneficial flow of data.

Respectfully Submitted,

Catherine McCullough, Executive Director, Intelligent Car Coalition

13 See https://www.automotiveisac.com/
14 See https://www.automotiveisac.com/best-practices/
16 An analysis published by NHTSA in 2013 concluded that drivers in vehicles 15 years old or older are at least 50% more likely to be fatally injured compared to a driver in a new vehicle, i.e., a vehicle 0 to 3 years old. How Vehicle Age and Model Year Relate to Driver Injury Severity in Fatal Crashes, National Highway Traffic Safety Administration, U.S. Department of Transportation (Aug. 2013). https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/811825