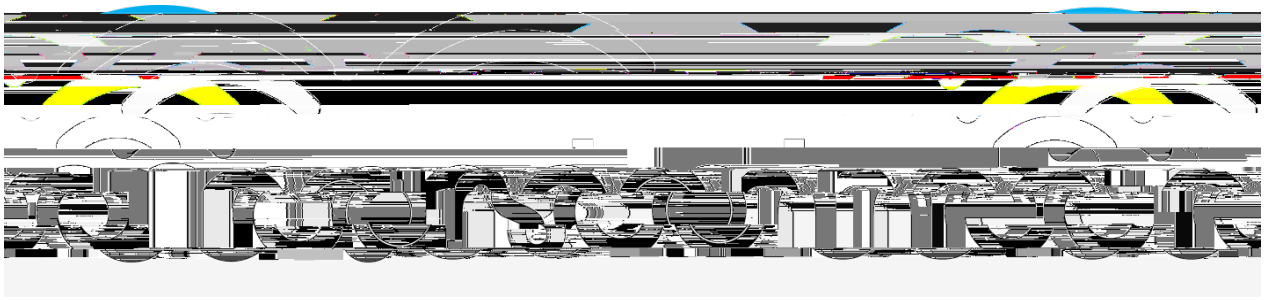
Introduction

Modern motor vehicles increasingly are equipped with technologies that enable them to access information via the Internet and gather, store, and transmit data for entertainment, performance, and safety purposes. Automated vehicles, those with vehicle-to-vehicle (V2V) communications technology, and other forms of wireless connectivity can provide important benefits to consumers and have the potential to revolutionize motor vehicle safety. At the same time, these technologies raise privacy and security concerns.

On June 28, 2017, the FTC and the National Highway Traffic Safety Administration (NHTSA) hosted a workshop in Washington, DC to discuss these issues. The day-long event featured representatives from consumer groups, industry, government, and academia, and explored the benefits and challenges of this growing market and its effect on consumer privacy and cybersecurity.



Key Takeaways

Several important points emerged from the workshop. First, many companies throughout the connected car ecosystem will collect data from vehicles, much of which will be used to provide important benefits to consumers. The car manufacturers themselves will collect data for a variety of purposes, such as to provide services for vehicle owners. For example, they may collect precise geolocation data to direct emergency personnel to the scene of a crash. To ensure safe operation and to prevent crashes, they may also broadcast location information to each other in real time. In addition, manufacturers of infotainment systems on vehicles will use data to enable consumers to use apps such as navigation or music apps, access their contacts, or connect to the Internet. Finally, some third parties provide "dongles" that connect to a port in cars, which collect and transmit consumer data. Such data may include information about consumer driving habits, such as if a driver regularly speeds or slams on the brakes. As one workshop participant noted, some of this information can be used for diagnostic purposes, to indicate a vehicle's state of health and determine whether certain subsystems are behaving properly. Other participants noted that auto insurance companies can use this information to determine rates for consumers: consumers who demonstrate good driving habits can qualify for insurance discounts. Some pargi3i(om)-2(8)4orgnesh222omer(r)3(m)-2(4(om)-2(pF2(a)6(r)g4m0l)-2(e1)4(h2( )]c69e)Tw T1m0l)- (m)-m(of 4(l)-2consih

initiatives, such as the Consumer Privacy Principles jointly introduced by the Alliance of Automobile Manufacturers and Global Automakers in 2014, are an important step in this process. Similarly, the National Automobile Dealers Association has partnered with the Future of Privacy Forum to produce consumer education that explains the kinds of information that may be collected by consumers' cars, the guidelines that govern how it is collected and used, and the options consumers may have. Some consumer advocates expressed concern, however, that it is not easy for consumers to figure out what kind of information their cars may be collecting or sharing and suggested the development of a central portal where consumers could compare automakers' different privacy policies.

Participants suggested that different approaches may be needed depending upon whether the data in question is safety-critical or not. For example, V2V and automated safety technologies will require vehicles to regularly transmit "Basic Safety Messages" about their speed, direction, brake status, and other vehicle information to surrounding vehicles, and receive the same information from them. That information is necessary for the safe operation of all vehicles on the road. In such cases, consumers' ability to opt out of such information sharing may not be appropriate. Other data, such as the data generated when a consumer syncs her smart phone to the car's infotainment system to access her phone book, are not safety-critical. In those instances, participants agreed that consumers should be provided with clear, easily understandable information about if and how their information is being collected, stored, or transmitted and how they can access or delete that information.

Fourth, connected and autonomous vehicles will have cybersecurity risks that can potentially be exploited. Before cars' computer systems were connected to the internet, a hacker