CONNECTED CARS USA 2016
Washington D.C.
February 4, 2016
Keynote Remarks of Commissioner Terrell McSweeny

Good morning. Thank you Nigel for that kind introduction. It is exciting to be here at the first Connected Cars USA conference.

The Harvard Business Review has proposed a five-stage life cycle of innovation- beginning with discovery and ending with "adoption by laggards". I propose inserting a new stage: "Washington policy conference." For many of us in the room, that is the best signal of when a technology has truly arrived.

The age of connected cars has begun, and, I believe, will only accelerate from here. The answers for what that means for consumers, for the automotive industry, and for the job market will be shaped by how regulators, enforcers, legislators, and most importantly, the innovators approach issues of safety, security, and privacy.

As I get into the meat of my speech on connected cars, I want to make one thing known. I drive an old, relatively unconnected car. I approach this subject not just as an FTC Commissioner, but also as an envious consumer. I'll note that my remarks today reflect my own views and are not the view of the Federal Trade Commission or my colleagues.

As a consumer, I'm looking forward to getting a new car. I want hands free communication; advanced safety features; a choice of Android, Windows, or iOS operating systems; and an ability to analyze my trips to see how I can save time or fuel or emissions. I'd like to have mobile Wi-Fi hot spot so my kids can play their favorite apps on long drives.

These are marvelous innovations. All this connectedness is placing remarkable capabilities at our fingertips and will allow transformative innovations – like truly self-driving cars – that have the potential to make our streets safer, our air cleaner, and revolutionize urban planning and design.

But to get there, these wonderful offerings must be safe, secure, and offer reasonable privacy.

So what is the Federal Trade Commission's role in all of this? For years, the FTC's role in the auto sector has been in policing advertising claims and warranties, and ensuring that consumers received fair treatment in dealer financing. These activities drew on our 101-year history of enforcing against unfair or deceptive acts and practices. If a business makes a deceptive claim in its advertising, or treats consumers unfairly in the terms and conditions it offers, we can launch an enforcement action against that business.

The marketplace has evolved in the century since our founding, and our enforcement has evolved with it. We followed consumers as they moved from the brick and mortar world to the Internet. Our mission broadened to include protecting consumer privacy – and, ultimately, their data security. At first, this meant the FTC focused on holding companies accountable for privacy promises to consumers and the security of information they collected on websites or mobile. Now, the FTC is increasingly focused on the so-called Internet of Things.

In 2002, the FTC brought its first case concerning the security of consumer data. Since then we have brought more than 50 data security cases. With each case, and with programs like our "Start with Security" initiative, we have developed the framework for what it means to reasonably secure consumer data by applying sound security practices when developing new products and putting procedures in place to keep security current and address vulnerabilities that may arise.

These cases are important for two overarching reasons. The first, obviously, is that they protect consumers. Consumers do not know the data security practices of the companies they patronize. They should be able to have a reasonable expectation that if they purchase a product or a service, the personal information they provide will be protected. The same principle applies to the Internet connected devices, the web services, and mobile applications they use, and the connected cars they drive.

The second reason goes to the actual marketplace. If consumers don't feel secure providing their information, or cannot trust the products they buy, the marketplace for new innovations cannot function. Recent surveys of consumers indicate that concerns about security and privacy are top reasons that consumers shy away from adopting new connected products.

Privacy and security are increasing in importance to consumers as more of our products, and more functions in our vehicles, become Internet enabled and behave more like information age computers than like industrial age machines. The software, microprocessors, and Internet connectivity of today's vehicles allow them to gather massive amounts of diagnostic, passenger, and trip data. That data is used to improve the performance of the car and the experience of the passengers.

The data capabilities of today's on-board computers and the emerging cloud-based vehicle applications will improve all facets of the vehicle experience, from fuel economy to music selections. But they also increase vulnerabilities.

For years, the FTC has advocated for data minimization – both as a privacy principle and security principle. The idea is simple: Companies should only collect what they need to in order to provide a particular service or product. Minimizing data collection – along with clear notice and choice – can also help ensure that consumers can fully understand what data are being collected.

These practices not only protect consumers, but they also put automakers and developers at less risk. A breach is less costly if there is less information stolen. A vehicle can conceivably collect precise geolocation data, health information, and voice identifiers of frequent passengers. But once collected, that information must be protected. The more information collected, the more resources that need to be deployed to protect it.

In many cases, not collecting the data, or deleting it once it is used, is the most sound cyber-security strategy. This leads very quickly into how the auto industry should guard against security breaches.

Since becoming an FTC Commissioner, I have become a frequent visitor to the various hacker conferences where car hacking has been prominently featured. Some have dismissed these exploits as stunts. But I think it would be wiser to treat these revelations as an important wake-up call to the auto industry. Indeed, even before these flaws were made public, a Senate report found a wide range of security practices in the auto industry. For example, some used third-party testing to check vehicle security, others did not. Most did not have technology to monitor a car's systems for malicious activity.

What I've learned from visiting with security researchers is that cars are prominent targets – but also that this prominence can create a real opportunity to enhance the safety and security of cars and the trust of consumers. The auto-industry would be well served by following the lead of the information technology industry, which has developed ways to work with security researchers – hackers – rather than against them.

For years, technology companies fought a losing battle on security by threatening hackers, and now many firms have established bounty programs and conferences where researchers are invited to find and report flaws in programs and products. They recognize that bringing researchers to the table and crowd sourcing solutions can be effective in staying ahead of cyber threats.

I am convinced that the white hat hacker can be an ally in the technology development process. Security researchers can work to uncover flaws and vulnerabilities in vehicles. They are like white blood cells, spotting viruses, infections, and flaws in the system, then communicating to the brain the best way to respond.

I find it promising that some in the auto industry are recognizing the value of forming partnerships as a part of their security programs. Last month, General Motors took the step of partnering with HackerOne, a security research collective, to undertake a program to use researchers to spot flaws and correct them before they become critical.

This also builds upon the necessary work that the industry is already doing with the creation of the Auto ISAC to share among the industry cyber threat information, as well as the creation last year of industry Consumer Privacy Protection Principles. The ISAC recognizes that cyber risk affects all companies equally. A cyber incident with one manufacturer will have negative reverberations throughout the industry. The Privacy Principles are also important. The FTC takes seriously our responsibility in helping signatories adhere to industry best practices. Not only are the principles a mission statement for the industry, but they also contain important protections for consumers.

While these developments are positive, I do want to express my disappointment with some ideas I’ve heard, such as a blanket safe harbor from meaningful privacy oversight or the criminalization of security research, both of which were included in the original version of NHTSA reauthorization considered last year. Thankfully, these provisions did not make it into the final bill. Let me stress that, in my view, not only would these have been bad for the consumer, but they also would have been bad for the industry.

The connected car will revolutionize mobility as profoundly as the first cars did. They can save lives, save the environment, save consumers money and time, change the way cities are designed, and even calm my kids' fights in the back seat. But we can only get there if consumers trust the product they are getting into. I'm optimistic we are on the right road – and I'm grateful for the opportunity to talk to you today about the important role security and privacy play in building that trust.