Before the
FEDERAL TRADE COMMISSION and NATIONAL HIGHWAY TRANSPORTATION SAFETY ADMINISTRATION

Connected Cars Workshop	)
P175403	)
	)
	)
	)

COMMENT OF THE INTERNET COMMERCE COALITION

The Internet Commerce Coalition (ICC), a coalition of major Internet companies, including both ISPs and edge providers, is appreciative of the opportunity to file a comment on questions and issues regarding the Federal Trade Commission (FTC) and National Highway Traffic Safety Administration (NHTSA) Connected Cars Workshop. The ICC recognizes the value of this joint workshop. We encourage both agencies to approach connected and automated vehicles—an implementation of the Internet of Things (IoT)-- with the goal of avoiding differing, sectorial, agency-by-agency regulation. Differing, sectorial, agency-by-agency regulation would create confusion and risk stifling growth in this strategic sector, as would potentially create unintended consequences for other IoT technology and services. These negative consequences can best be avoided by preserving the FTC's exclusive role regarding IoT privacy and security while recognizing NHTSA's exclusive role regarding vehicle safety.

Connected and automated vehicles (including vehicle-to-vehicle, vehicle to infrastructure, vehicle to smartphone, and vehicle telematics technology) has the potential to generate a considerable amount of data. In some cases, it could be sensitive information, such as persistent precise geolocation information. It is essential that this information be protected in a manner consistent with the FTC's privacy framework.

As the federal government's expert agency on privacy and security, the FTC has been and should continue to be the exclusive agency responsible for privacy and security issues relating to all IoT implementations. This holds true for connected vehicles. FTC guidance on privacy and security applies to and should apply to connected vehicles just as it does to other IoT implementations. Likewise, FTC protection of privacy and security through enforcement is a far more effective solution than an *ex ante* rulemaking that would attempt to address IoT in specific sectors. Not only does rulemaking not keep pace with the rapid innovation of IoT, it results in different data privacy and security requirements across the various actors in the IoT ecosystem, even when the same data may be involved.

NHTSA, with its expertise in vehicle safety, can play the primary role in that area, while leaving privacy and security to the FTC. FTC guidance and enforcement, combined with industry engagement in voluntary and collaborative processes and adherence to best practices, provides the most effective framework for protecting privacy and security of connected and automated vehicle data and systems. This approach will provide consumers with the best protections and will be conducive to further innovation.

Respectfully submitted,

/s/ **Sydney M. White**

Sydney M. White
Counsel to the Internet Commerce Coalition

May 1, 2017