Questions for the Record for Maneesha Mithal

Hearing on "Examining Ways to Improve Vehicle and Roadway Safety"
House Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing and Trade
October 21, 2015

Questions from Chairman Burgess:

1. **You testified that the FTC has had several meetings with NHTSA staff related to data privacy and security issues. Please provide the names and titles of the individuals at NHTSA that the FTC has met with on data privacy and security issues.**

   FTC staff has met with NHTSA on a number of connected car issues as they relate to consumer privacy and data security, including Event Data Recorders ("EDRs"), vehicle-to-vehicle ("V2V") and vehicle-to-infrastructure issues, the FTC's Internet of Things workshop, and cybersecurity concerns. These meetings have included many NHTSA and FTC representatives. Some of the NHTSA representatives include the following:

   - David Strickland, then-NHTSA Administrator
   - Chan Lieu, then-Director, Office of Governmental Affairs, Policy and Strategic Planning
   - Dana Sade, Senior Attorney, Legislation and General Law Division, Office of the General Counsel
   - Thomas Healey, Attorney Advisor, Office of General Counsel
   - Alison Pascale, Director, Governmental Affairs, Policy and Strategic Planning
   - Frank S. Borris, II, Director, Office of Defects Investigation
   - Justine S. Casselle, Trial Attorney, Litigation and Enforcement, Office of Chief Counsel
   - Nathaniel Beuse, Associate Administrator, Office of Vehicle Safety Research

2. **You testified that the FTC uses Section 5 of the FTC Act to determine whether an auto manufacturer has tested the security of a car appropriately before putting it on the market for public consumption. What constitutes an unfair security practice that could cause or likely cause substantial consumer injury in the automotive sector?**

   Under Section 5 of the FTC Act, the Commission has authority to challenge companies' data security practices that are unfair or deceptive. A company engages in unfair acts or practices if its data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition. Whether a particular practice is unfair under Section 5 will depend on the facts and circumstances of each case. In determining whether a company's security practices are unfair, the Commission looks to the reasonableness of its security, in light of harms associated with potential vulnerabilities, the size and complexity of the company's data operations, and the cost of available tools to improve security and reduce vulnerabilities. The Commission has emphasized a process-based approach to data security that includes designating an individual or individuals responsible for data security; conducting risk assessments; designing a security program to address risks, including administrative, physical, and technical safeguards; and adjusting the program to address changes. A company's failure to implement these processes – whether in the retail, financial, software, or automotive sectors – can be unfair.

3. **How does the FTC define reasonable data privacy and security practices with respect to motor vehicles?**

   Reasonableness is not a one-size-fits-all approach. As noted above, what is reasonable will depend on harms associated with potential vulnerabilities, the size and complexity of a company's data operations, and the cost of available tools to improve security and reduce vulnerabilities. The Commission has

emphasized a process-based approach to data security that includes designating an individual or individuals responsible for data security; conducting risk assessments; designing a security program to address risks, including administrative, physical, and technical safeguards; and adjusting the program to address changes.

4. **In title three, Section 301, the staff discussion draft proposes that an auto manufacturer will be liable to a civil penalty of up to $5,000 per day with a maximum penalty of $1 million if it does identify that it will meet all seven of the requirements in its privacy policy or is found to have violated any of the terms of its privacy policy. How does the FTC currently enforce reasonable data privacy practices among auto manufacturers? What is the process the FTC must undertake to impose a civil penalty against an auto manufacturer that does not maintain reasonable data privacy practices? What is the maximum penalty the FTC can impose against an auto manufacturer found to have unreasonable data privacy practices?**

   Under Section 5 of the FTC Act, a company acts deceptively if it makes materially misleading statements or omissions about a privacy practice, and such statements or omissions are likely to mislead reasonable consumers. Further, a company engages in an unfair privacy practice if the practice causes or is likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition. If an auto manufacturer were to engage in an unfair or deceptive privacy practice, the Commission could seek injunctive relief against the manufacturer, along with equitable monetary remedies, such as redress to injured consumers or disgorgement of ill-gotten gains. Injunctive relief could include, among other things, a prohibition on future misrepresentations, requirements to provide choices, or corrective disclosures. If a manufacturer were to violate an existing FTC order, it could be subject to civil penalties in the amount of up to $16,000 per violation per day.

   Even though the FTC cannot obtain civil penalties for an initial violation of Section 5, I do not believe the bill would provide greater protection for consumers than under current law. Indeed, as noted in the Commission's written testimony, because the bill contains a safe harbor exempting a manufacturer from FTC oversight, and Section 32402(d)(2) provides a separate exemption from civil penalties, a manufacturer that submits a privacy policy that meets the requirements of Section 32402(b) but does not follow it would not be subject to any enforcement mechanism. Furthermore, although the privacy policy requirements only apply to information collected from vehicle "owners, renters, or lessees," the safe harbor would immunize manufacturers for privacy practices related to other types of consumers – such as collecting information from vehicle shoppers through manufacturers' websites. Thus, for example, the Commission could be precluded from bringing a Section 5 case based on any privacy and data security-related misrepresentation on a manufacturer's website, even if the misrepresentation is unrelated to vehicle data.

   Moreover, even in the limited circumstances where the discussion draft would make the auto manufacturer liable for civil penalties, these civil penalties would not serve as a strong disincentive for law violations because the maximum penalty is only $1 million. A data security violation could easily result in consumer injury in excess of $1 million."

5. **In the FTC's view, how should Congress penalize malicious hackers from exploiting cybersecurity vulnerabilities in vehicles without impeding the work of "white hat hackers" and good actors within the security research community who make responsible disclosures and help to improve vehicle security?**

   I strongly support the goal of deterring criminals from accessing vehicle data. However, security researchers provide an important role by uncovering vulnerabilities that companies can then voluntarily fix, thereby protecting consumers. Ideas to balance these interests include the possibility of penalizing only those hackers who access systems with "malicious intent" and including a specific exemption for researchers who disclose vulnerabilities to companies before making them public. Of course, I understand that protections for researchers must be carefully tailored so that illegal conduct is not immunized. FTC staff would be pleased to work with subcommittee staff to try to balance the interests involved.

   A. **How should white hat hackers and good actors within the security research community disclose cyber security vulnerabilities "responsibly"?**

In my experience, security researchers that wish to disclose vulnerabilities responsibly reach out to a business privately and give the entity an opportunity to voluntarily address the vulnerability prior to publishing their findings. I believe this would be a good approach.

6. **You testified that the FTC has focused on process with respect to maintaining cyber security across all industries and sectors. Should those processes be any different to secure critical safety systems in vehicles compared to other critical infrastructure? If yes, how so? If not, why not?**

As discussed above, companies should be required to implement reasonable data security measures. In its guidance to businesses, the Commission has emphasized a process-based approach to data security that includes, among other things, conducting risk assessments and designing a security program to address those risks. Certainly, the specifics of a risk assessment will differ depending on the risks (e.g., safety concerns or the types of information collected), the types of vulnerabilities that have been known to target a particular industry, the size and complexity of a company's operations, and the availability of tools to address the risks.

7. **Connected cars are a part of a larger Internet of Things ecosystem. Should the governance of connected cars be any different from other connected things?**

Earlier this year, Commission staff issued a report summarizing its November 2013 workshop and outlining policy recommendations on the Internet of Things ("IoT").[1] The recommendations included, among other things, encouraging companies to implement data minimization by taking a privacy-by-design approach, continued use of notice and choice, and implementing reasonable security for IoT devices. While the implementation of these recommendations may need to be tailored for specific industries, such as connected cars, the broader principles apply across the Internet of Things ecosystem. For example, the report encourages companies developing IoT products to implement reasonable security by building it into their devices at the outset, promoting it through hiring and training, and overseeing service providers. Companies should also conduct a risk assessment, and if the assessment identifies significant risks, they should implement a defense-in-depth approach, in which they consider security measures at several levels. These recommendations apply equally to connected cars as well as other connected devices. The report also emphasized that in the Internet of Things, companies need to address physical security and safety risks, not just risks associated with sensitive information. This point applies with particular force in the context of connected cars.

8. **Does the FTC believe that the privacy principles developed by the Alliance of Automobile Manufacturers and the Association of Global Automakers adequately protect customers' data privacy?**

I support the goals of the privacy principles developed by the Alliance of Automobile Manufacturers and the Association of Global Automakers. While these principles are a good first step to protecting consumer privacy, there is room for improvement. For example, the principles do not require affirmative express consent before any collection of precise geolocation information. As the Commission has stated previously, because geolocation information can reveal a consumer's movements in real time, as well as provide a detailed, comprehensive record of a consumer's movements over time, use of this sensitive information can raise privacy concerns.

[1] *See FTC Staff Report on the Workshop "Internet of Things: Privacy and Security in a Connected World"* (Jan. 27, 2015), *available at* https://www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things.