SHEARMAN & STERLING LLP

Connected Cars and Data Privacy:

Thinking Through the Federal Automated Vehicles Policy

Jeewon Serrato, Counsel
Privacy & Data Protection

In the privacy section, the seven principles that are enumerated in the federal policy are nothing new. It tracks very closely to the seven principles that were agreed to in 2014 with the Alliance of Automotive Manufacturers – they include: Transparency, Choice, Respect for Context, Minimization and Data Security, Integrity and Access, and Accountability.

This is meant to be a really high level, best practices document. But where it really matters is how these are implemented. If you look at the kind of ecosystem issues that are involved in connected vehicles, the questions that we are getting from our clients is related to the supply and risk.

What that means is it's not just the manufacturers – but the parts manufacturing, the software, the folks that are involved in the infotainment systems, and really, all of the different suppliers and third parties that are involved in putting together the connected systems – need to abide by these privacy principles.

The biggest challenge in implementing these privacy principals with the ecosystem and with the third parties and the suppliers – is that there needs to be a close coordination. It cannot be just, let's say, one of the OEMs – the original equipment manufacturers – imbedding these privacy principles into their product design – but also having really good relationships with the third parties, and having contracts that really spell out what it means, and the responsibilities of each of the parties in thinking these principles through.

And it's not enough to just have the legal department involved in thinking these through at the contract level and the agreement level – it needs to be really imbedded through the design cycle, from the engineers, who are designing these systems, and then also down to the technical level, who are building these systems.

This might sound really complicated and overwhelming, but there are some simple steps that each of these parts manufacturers and software manufacturers – that manufacturers can do. First of all, it starts with a conversation. It starts with relationship building.

By really talking about what kind of data is being collected, and "where is it going?" "how is it stored?" and "to whom will you be sharing?" – by asking these questions and recording them, and by having these conversations between the third parties and the manufacturers, you can start really designing what kind of privacy programs and policies need to be in place.

This is not just privacy – it really goes into cyber security questions as well. There's been a lot of press and media attention to what

would happen if a connected car was hacked. There have been, in the last couple of years, a couple of "white hats," so to speak – engineers have shown that a vehicle that is connected can be hacked into, and that can have really drastic consequences on the safety of the vehicles.

Now, in talking about cyber security and privacy – those things really are connected. It goes into how these systems are going to be designed, so that privacy and security is embedded from the beginning, and that has to be really something thought-out and coordinated from everybody that is involved in building the systems and putting them together.