SHEARMAN & STERLING LLP

Connected Cars and Data Privacy:

Global Regulatory Challenges

Jeewon Serrato, Counsel
Privacy & Data Protection

We also need to think about what kinds of laws and regulations are coming into play outside of the US. The European General Data Protection Regulation was adopted – it's going into effect in 2018. It sounds like we have a couple of years to really comply with it, but the work needs to happen now.

The regulation applies not only to manufacturers in Europe, but it applies to any manufacturer that could be handling the data belonging to European citizens. If there is a US automotive manufacturer – or really any global automotive manufacturer – that's dealing with connected cars and data being collected of European citizens, the EU GDPR is also another layer of complexity that we need to think about.

Before 2018 – when the EU GDPR comes into effect – the manufacturers and the suppliers, and everybody that's involved in the ecosystem, needs to be conducting privacy impact assessments in how the systems are being designed and what the impact of privacy would be for each of these decisions that are being made.

In addition, there is a requirement called the Data Processing Register, and also the Data Breach Register. Again, these are two tools that a lot of the companies have been probably implementing, but what this does in the EU regulation, is that it formalizes it, and now it's a requirement.

If the automotive manufacturer is handling data belonging to EU citizens, the fact that certain third parties are involved, and the data is being transferred outside of EU – going to the US, for example, or to Asia, to Latin America – in all of those situations, the data being collected and processed needs to be formally documented and registered in the Data Processing Register.

This will be, perhaps, a good framework for US automotive manufacturers to look at when they are implementing not only the EU requirements, but looking at the US policies as well.

Perhaps the reason that the US framework and the EU framework seems to be slightly different right now is that there is a philosophical difference in how we treat privacy in the EU and in the US.

In the US, we start with the premise that the data can be used unless there is some kind of exception, or unless it has been prohibited. In the EU, it's the opposite. In the EU, you start with the premise that data cannot be shared unless some kind of permission or consent was given.

We're going to have to really think about – as manufacturers and suppliers, part of the ecosystem – how do you work with different frameworks and different thinking about what privacy means, let's say in the EU versus the US. And how do you come up with a global privacy framework that really works with and meets the requirements in both jurisdictions, and really, in global jurisdictions.

Everyone, globally, is trying to figure out – in very complex data situations – what jurisdiction will really be dominant: Is it a US law that's going to apply or is it an EU law or is it Asia? And these kinds of questions are coming up all the time. The question about these jurisdictional overlaps – and perhaps different conflicting jurisdictions having different requirements and how data is transferred – these are the kinds of questions that our clients are asking us to really think about.