February 23, 2018

LAW BUSINESS TECHNOLOGY
BUSINESS TECHNOLOGY LAW
TECHNOLOGY LAW BUSINESS
THE RECORDER
daily at www.therecorder.
An ALM Publication

International Privacy Regulation for Connected and Autonomous Vehicles

By Xiaoyan Zhang

Each year, more connected and autonomous vehicles (CAVs) enter the road, yet the governing legal framework seems to lag behind. This is particularly true for cybersecurity and privacy. While several jurisdictions have recently released voluntary guidelines or draft bills on cybersecurity, binding privacy regulation remains overdue. This article compares privacy regime in Germany, United States, and China, and purports to inform global CAV players, users, and others what to anticipate in this hot yet gray space.

The Unique Nature of Intelligent Vehicles

Thanks to rapid innovations in Internet of Things, sensor technologies, and data analytics, traditional automakers have allied with technology leaders in a manic race to build intelligence into driving machines from connected cars to autonomous vehicles (AVs). Intelligent vehicles are only starting to evolve, yet already they generate a complex array of cybersecurity and privacy issues.

CAVs are particularly vulnerable to cybersecurity attacks. A modern car has 50 to 150 electronic control units, each with roughly 100 million lines of code and potentially 1.5 million bugs ripe for exploitation. The addition of mobile, wireless, and Internet technologies needed to turn a car into a CAV opens up countless new access points for hackers. These vulnerabilities are multiplied by a highly fragmented supply chain with over 20 different suppliers (more than a mobile phone) where imperfect parts integration may lead to further compromises.

Xiaoyan Zhang

But CAVs are both vulnerable sheep and voracious wolves. Using their powerful sensors, CAVs can intrude privacy through ubiquitous data collection on public roads. Depending on the level of automation, an AV relies on three types of sensors: radars on bumpers to identify traffic; cameras for color identification, lane and pedestrian alerts; and a light detection and ranging sensor on the roof to generate a 3D map of the environment. While these sensors collect location and movement data needed for navigation, such data intake can easily scale without any additional infrastructure, resulting in expansive secondary uses. Data unnecessary for navigation may also be collected, leading to surveillance by a non-government entity. Finally, non-users on public roads may have their information captured without practical ways to receive notice or give consent.

Indeed, cybersecurity and privacy concerns are among the biggest obstacles to the growth of the CAV industry. Germany and the US are leading the development while China seems to possess the highest potential for growth. Although none of these jurisdictions has formally adopted any CAV-specific privacy laws, a review of existing regime reveals that a different approach appears to be taken.

Germany

In July 2017, the Federal Minister of Transport and Digital Infrastructure of Germany issued ethical guidelines on CAV, addressing key privacy issues:

- CAV owners and users may decide whether and how their vehicle data are to be shared and used;
- Consent shall be properly obtained from parties present in the vehicle's surroundings, such as passers-by or other road users before the collection and use of their data;
- CAV manufacturers should install factory settings that suppress the collection and use of data irrelevant to navigation under the principles of privacy by design and privacy by default;
- New techniques should be considered over time to determine whether data have been sufficiently anonymized;
- CAV drivers, owners, and users should be informed of the purpose and legal basis for processing data unnecessary to navigation;
- Vehicles data usage should be monitored by independent testing institutes and relevant stakeholders under the principle of transparency.

United States

Although the September 2017 SELF DRIVE Act passed by the House of Representatives mainly addresses safety of CAV, it contains a brief provision on privacy. Specifically, Section 12 requires that manufacturers, prior to making, selling, or importing CAVs into the US, develop a privacy plan disclosing the following practices, among other things:

- How data concerning vehicle owners or occupants are collected, used, and stored;
- Data minimization, de-identification, and retention;
- Data sharing with third-party entities;
- Data deletion upon ownership transfer.

The privacy plan requirement may be waived if the data is anonymized or encrypted such that information can no longer be linked to the vehicle. Section 12 also requires a method to notify vehicle owners or users about privacy policy. Finally, the Federal Trade Commission would supervise the privacy plan's implementation and prosecute violations.

Separately, in 2014 members of the Alliance of Automobile Manufacturers and the Association of Global Automakers agreed to a set of consumer privacy protection principles targeting a compliance date no later than the 2017 model year. Key principles include requiring affirmative consent from owners and users regarding use of their geolocation, biometric, or driver behavior data for marketing or third-party sharing purposes.

China

China's Cybersecurity Law (CSL, effective June 1, 2017) applies to network operators and critical information infrastructures, which may cover CAV manufacturers and suppliers. The CSL generally require, *inter alia*, giving notice and obtaining consent before personal information is collected, shared, or transferred cross-border.

On December 29, 2017 China issued the final Guidelines for the Establishment of National Standards System of Telematics Industry, detailing 95 standards for the construction and testing of CAVs, among which 16 are related to cybersecurity and privacy. One key standard to watch for is entitled "General Requirements on Vehicles Data Privacy and Cybersecurity Protection," which is currently being drafted.

A Comparative Study

Among the three countries, Germany provides the broadest privacy protection and in turn imposes the most restrictions on manufacturers by addressing CAV-specific issues. For example, it distinguishes data necessary for navigation from other data; grants the vehicle owner and user maximum rights to their data; and acknowledges the need for practical solutions to obtain consent from non-users present in the vehicle's environment, and to ensure sufficient anonymization to combat scalability. The US treats CAV data similarly to other sector data and fails to address CAV-specific issues except for the moderate attention to the segmented supplier chain. While we are waiting for China's CAV privacy rules, we should bear in mind that Chinese government is strongly motivated to promote next-generation vehicles, and such sentiment will likely be reflected through legislative enactment as well as juridical enforcement.

A San Francisco-based counsel in Reed Smith's global IP, Tech & Data Group, ***Xiaoyan Zhang*** *advises clients on privacy, cybersecurity, and IP related to complex and emerging technologies such as connected and autonomous vehicles. Xiaoyan has an advanced degree in Computer Science, and was an ethical hacker for several businesses prior to her legal career. She is a Certified Information Security Systems Professional (CISSP), a Certified Information Privacy Professional in the United States (CIPP/US) and in Europe (CIPP/E) recognized by the International Association of Privacy Professionals (IAPP).*