SQUIRE
PATTON BOGGS

Connected Cars

10 Issues to Consider

Global – 26 January 2024

Connected cars blur the line between previously separate sectors. As a result, it is possible that the same car is subject to the laws and regulations on consumer regulation applicable to the automotive sector, as well as telecommunications regulatory obligations.

The Internet of Things (IoT) has increased the amount of information organizations handle and has changed the way this information is collected, stored and used.

The collection, storage and use of IoT information also requires organizations to comply with a host of legal and regulatory obligations, which vary around the world.

Connected cars and intelligent transportation systems (ITS) provide a specific IoT application that blurs the line between previously separate sectors. As a result, it is possible that the same car is subject to the laws and regulations on consumer regulation applicable to the automotive sector, as well as telecommunications regulatory obligations.

Given the significant growth in the market for connected cars, it is important to keep in mind the following key considerations:

1. Design for security – Laws, regulations and regulators' expectations mandate implementing appropriate security into connected devices. For example, in the US, the Federal Trade Commission (FTC) emphasizes the need to implement security in the design process rather than an as afterthought, and California now specifically requires it. Similarly, in the UK, Ofcom and the National Protective Security Authority (NPSA) have also advised that such secure design principles are followed in developing a secure ITS. Relevant questions include:

- What is the capability of the product to resist cyberattacks and are there exploitable gaps?
- Is your security program reasonable (e.g., do you use industry-standard encryption; how effective are any security measures taken; and are there sufficient redundancies and safeguards built into the product)?
- Have you implemented industry-standard security controls such as the CIS Critical Security Controls (e.g., configure securely, update continuously, block access and test and plan response)?
- Have well-known and easily preventable security flaws been addressed (e.g., where regulators will look first)?
- Do you have an incident response plan to govern the disclosure of information in the event of an incident involving security or safety?

- If you operate in the EU, have you checked whether tightening the security measures for internet-connected cars or machine to machine services (M2M) could restrict the free movement of your equipment or services within the EU?

2. Design for privacy – Regulators also expect privacy to be considered, beginning with product design, and they have penalized companies that fail to see obvious privacy flaws. It is important to assess the personal information you handle and evaluate compliance with state, federal and foreign (if applicable) privacy laws from the outset and thereafter. Regulators are particularly interested in vehicle-generated data and whether such data might include personal data, such as location data.

- Have you mapped and assessed how information from the product will be collected, retained, used and shared?
- When does your product begin to collect personal information (out of the box without further consent)?
- Does your product collect information for a limited purpose and then delete the information it no longer needs?
- Have you provided appropriate notice to consumers (in advertising, by dealerships and in website privacy statements) that complies with the law, best practices and regulators' expectations?
- What personal information could your product receive from consumers overseas and what procedures are there to handle compliance with foreign law (e.g., data transfer restrictions and localization requirements)?
- If you have EU consumers, are you complying with and providing "adequate" data transfer protection under the EU General Data Protection Regulation?
- Can compliance obligations be eased by participation in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system?

3. Design for safety – In order to comply with regulations that protect passengers from physical harm, you should build your product so that it is safe for consumer use.

- Have you considered which laws, regulations and industry standards govern your product that protect consumers from physical harm)?
- Have you designed your product to be safe to human health for all foreseeable uses and misuses?

4. Protect intellectual property rights – In order to prevent litigation and protect your investment, seek national and international patent, trademark and/or copyright protection for your product, including with regard to infotainment and telematics.

- Have you determined what aspects of the product are eligible for intellectual property protection?
- Have you secured the rights to all aspects of the product design to reduce litigation risks upon launch?

5. Request authorization from telecoms authorities – Determine whether your connected car provides electronic communications or telecommunications services (e.g., M2M communications or in-vehicle Wi-Fi or internet access services) subject to licensing or authorization requirements. This may depend on whether the type of connectivity includes only M2M connectivity, whether it also provides internet access services to the end user (in-vehicle Wi-Fi), or whether it can connect into public communications networks. It may also depend on the business model adopted for the resale of M2M connectivity. You should also determine whether any other regulatory obligations apply (e.g., security, interoperability and net neutrality in the EU).

- Has your product been properly tested and classified (under all applicable laws)?
- Are additional equipment authorizations necessary to import and market eSIM devices and other RF equipment embedded in the connected car?
- Is your product correctly labeled according to the relevant statutory equipment authorization and local custom requirements, if necessary?
- Do you require a license or a waiver of applicable rules to operate on any radio frequencies utilized in your services (e.g., in the US, a radio license subject to Title III of the US Communications Act may be necessary depending upon the services provided, and in the UK, a Business Radio IoT license may be required)?
    - If a license is required, what regulations and obligations (for example, Universal Service Fund contributions and data security) may apply to your M2M or in-vehicle Wi-Fi services?

6. Create accurate and truthful advertisements – Ensure that all representations of product functionality and data security can be substantiated, in order to safeguard the company from false or deceptive advertising claims.

- Have you considered how your advertising will impact the regulatory classification of your product?
- Have you ensured that your advertisements accurately reflect the performance, security and safety of your product (without overpromising on security)?

7. Data retention and data localization – In-vehicle data should only be kept for as long as there is an administrative need to keep it, in order to carry out your business or support functions (e.g., billing); or it is required to demonstrate compliance for audit purposes or for legislative requirements (e.g., in case of an order to intercept communications for law enforcement). A recent judgment of the Court of Justice of the EU (CJEU) on the German data retention law offers a reminder that keeping data for longer than necessary is risky. The problem is that different data retention periods apply to different situations – there is no one-size-fits-all solution.

8. Set-up a continuous improvement loop – Regulators expect companies to monitor post-sale complaints and safety or security incidents to identify vulnerabilities in either the safety or security of products and to make improvements.

- Do you have formal procedures to monitor post-sale incidents for safety and security risks, as well as clear criteria for prioritizing escalation and repair?
- Do you have a product development plan to advance next generation designs and software patches to protect consumers?

9. Examine license agreements closely – Review all licensing agreements to determine whether your company is protected in the event of litigation over the intellectual property, safety or security issues that may arise after product launch.

- Do you have formal indemnity provisions in the license agreement and how do they flow?
- Have you ensured that your licensing partners have adequate design protections on security and safety in connection with products bearing your mark?
- How will information be shared, and incident responses handled in the event of security or safety events?

10. Antitrust and competition – Consider competition law as a tool to challenge or defend your IoT strategy regarding, for example, big data capture, portability and interoperability.

- Does the connected car create a database that is too powerful?
- Is the connected car based on proprietary platforms with limited ability to talk to smart products of other suppliers?
- Does the connected car platform include or create standard essential patents (SEPs)?

Moreover, special rules exist outside the US – e.g., in Europe and the UK – governing access to in-vehicle data from independent third-party repairers.

Special rules exist outside the US – e.g., in Europe and the UK – governing access to in-vehicle data from independent third-party repairers.

The opinions expressed in this update are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.