The Internet of Things and connected cars: new opportunities and risks

Technology Sector Alert

29 JAN 2018
By: Vincent Man

The automotive industry is undergoing tremendous change, both in the technology it employs and in the way it does business. People and companies are changing the way they think about cars and car travel. A big part of this change arises from the increasing connectedness of cars.

Car connectivity started as a way for car owners to call for emergency roadside assistance. Today, it can enable advanced car features, such as repair/maintenance management, autonomous driving and in-car entertainment. Cars are fast becoming an integrated part of the Internet of Things. With that evolution comes both risks and opportunities for all companies in the car industry.

Automobile manufacturers are rapidly improving the connectivity of cars via technology. Features that have been available for many years include remote control of locking/unlocking doors, GPS directions and smartphone connectivity. Other more recent developments include connectivity with IoT devices (such as wearables), connectivity between cars to enhance autonomous driving capabilities and technology that allows car manufacturers and third parties to monitor the health of your car and invite you in for maintenance or repair.

As the name suggests, autonomous driving allows cars to operate with varying levels of user intervention. Though not yet fully autonomous, cars have been equipped with certain autonomous features for many years, such as
anti-lock brakes, adaptive cruise control and stability control. More recently, features such as automatic lane change, self-park and limited auto-steering have also been introduced.

These technological changes are propelling the way car companies are investing in their future. Car companies are filing more patents than ever before, and they are doing so in electrical and software fields at a higher rate than ever before. At the same time, car companies are also collaborating with technology startups, by way of partnership or acquisition. The evolution of cars into the Internet of Things will only accelerate as demand grows for connected and autonomous cars, while the deployment of reliable 5G networks will also enable vehicles to share rich, real-time data that would support fully autonomous driving experiences.

Happening in parallel is a shift in the way consumers, particularly in urban areas, use cars. In the past, cars were owned, leased or rented. Now, consumers in urban centers are as likely to car-share or ride-share as they are to own, lease or rent. Greater car connectivity is likely to continue transforming how consumers use cars.

**Opportunities and risks**

**Patents and litigation**

As in any area of rapidly developing technology, car companies, their partners and their suppliers are in a race for the patent rights to take advantage of cars in the Internet of Things. Companies that build a strong portfolio of patents are likely to reap the benefits through licensing/partnership opportunities and lower patent litigation risk.

The car industry has experienced a significant increase in the amount of patents filed by car manufacturers\(^1\). At the same time, technology companies not traditionally associated with the auto industry are also developing extensive patent portfolios related to automobiles. The increase in patent filings is indicative of technological innovation. However, with that innovation comes increased patent litigation risk.

In the last five years, in the US alone, there has been a surge in patent suits filed by non-practicing entities for everything from touch screens to LED headlights, and many things in between. Car companies have also been sued in recent years for patent infringement by technology companies.

Patent litigation activity relating to Internet of Things technology is only likely to speed up, given how cars are increasingly using non-automotive IoT technology. Car companies will be at risk from both non-practicing entities and technology companies that are developing IoT technology (for cars or otherwise).

Many tactics can be used to manage (and hopefully lower) patent litigation risk. Developing a strong patent portfolio is a given. A strong patent portfolio can lower the risk involved in patent litigation, particularly as it relates to competitors, since patents can be used as both a sword and a shield. In such cases, patents are the currency used in negotiations to resolve disputes.

Among other approaches: monitoring what other players are doing, and using patent pooling strategies.

Knowing who the players (ie, the potential patent litigation threats) are is becoming increasingly complex. As car companies partner with technology companies to develop advanced technology for their cars, potential patent litigation threats become more numerous and less easy to track. However, there are ways to use patent research tools to track who is patenting what.

A patent pooling strategy may also be beneficial. One well-known patent pool is operated by the LOT (License on Transfer) Network, which describes itself as “a non-profit community of companies that was formed to preserve the traditional uses of patents while providing immunization to the patent troll problem.” Companies can become part of the LOT Network by offering a royalty-free cross-licensing agreement that grants a license to all the other participants in the Network when/if a patent owned by a participant is transferred to a non-participant (eg, a non-practicing entity). As a result, participants are immunized from patent litigation by non-practicing entities that later purchase a patent from an LOT participant.

A related tactic and one employed by some patent pool managers is for the manager to purchase patents on behalf of one of its members.

A tangential benefit of participating in such patent pools is that car companies can gain access to patents that are
not necessarily directed at cars. This is beneficial because IoT technology is applied to many industries beyond cars.

**Liability from manufacturing defects or design defects**

Another area of legal risk associated with emerging IoT technology (and in particular autonomous driving technology) is product liability. While the car industry is no stranger to product liability litigation, the introduction of autonomous driving technology to cars raises the stakes.

Some of the legal issues will be novel. For example, what is the standard of care to be applied to car companies when an autonomous car is introduced to the market? What will be required of car companies when it comes to designing, testing and implementing cars before they go on the road? Most jurisdictions around the world have yet to implement a regulatory regime for governing autonomous cars. When implemented, how will such regulations impact a car companies’ liability?

The issue of whether a particular defect is a manufacturing defect or a design defect is also interesting. A design defect arises when the product is manufactured as intended, but the design gives rise to a malfunction or creates an unreasonable risk of harm that could have been reduced or avoided through the adoption of a reasonable alternative design. A manufacturing defect occurs when a product is not manufactured in accordance with the manufacturer’s own specifications and requirements. Given that the company making the car may not be the same as the company designing the software and systems enabling connectivity, the issue of whether a defect is one of manufacturing or one of design can have an impact on who is liable for a particular defect.

Car companies will also have to consider how to address liability associated with software bugs. Almost any software has bugs, but a bug in an autonomous car could have serious implications. Manufacturers must come up with fail-safe protocols and backup software to ensure software bugs do not cause serious harm.

Whether a defect is a manufacturing one or a design one, there may be liability for a “failure to warn” in cases where a manufacturer knows, or ought to know, of a danger associated with the use of its product and fails to warn consumers of the potential danger.

Advances in connected technology also have the potential of increasing risk in a number of security-related areas, including risks from: hacking, software defects (or bugs) and decision making based on algorithms.

Any unconnected car may be hacked (ie, have its systems subverted and controlled by a third party), but a connected car is far more vulnerable. No physical interaction is necessary. In one case, researchers discovered a vulnerability in a car’s entertainment system which allowed the researchers to gain control of the car’s internal computer network and remotely manipulate various systems. If hackers were able to gain control of a connected and autonomous car, the safety of passengers could be at serious risk.

Another category of design defect which may give rise to liability is the use of algorithms to make navigation decisions which impact the safety of those both in the car and outside the car. Unlike human drivers who are required to make instinctual real-time decision while driving, an autonomous car’s decisions are governed by its programming. As a result, difficult ethical questions may arise – for example, when a situation arises in which the car is forced to choose between two or more bad outcomes. For example, should the car be programmed to prioritize minimizing loss of life or protecting the car’s occupants?

Given the lack of legislation in many countries governing connected and autonomous cars, there is an opportunity to participate in the development of rules and regulations so that risk is appropriately allocated between manufacturers, consumers, government, insurance and the public.

**Liability from breaches of privacy legislation**

Car companies envision a future where cars are capable of providing a fully personalized mobility experience. To do so, cars will need to be capable of collecting, storing and processing data about their users. Some car makers are unveiling prototype apps that are able to, for instance, use personal contact and appointment information to calculate an optimal route to an agreed meeting place. Such personalized functionality is supported by the car’s connectedness and ability to obtain data from external systems. However, when obtaining and storing personal data, car companies must consider the privacy issues that may arise, particularly if such personal data is used for
purposes other than those the user has approved.

**Canadian case study**

In Canada, the federal statute *Personal Information Protection and Electronic Document Act* (PIPEDA) regulates how private-sector organizations collect, use or disclose personal information in the course of commercial activities in all jurisdictions that do not have substantially similar legislation. Currently, substantially similar legislation exists in Alberta, British Columbia and Quebec.

The obligations under PIPEDA include:

- An organization is responsible for personal information under its control
- Personal information shall be protected by security safeguards appropriate to the sensitivity of the information
- The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected
- Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law
- The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate

PIPEDA is not the only legislation governing personal information in Canada. If a vehicle collects information regarding biometric and health information, the personal information will likely be regulated by other legislation, such as *Ontario’s Personal Health Information Protection Act*, which governs the protection of personal health information that is collected, used or disclosed by health information custodians. Another consideration for car companies is the fact that vehicles travel across jurisdictions. As manufacturers collect and store data, they need to be aware that this act of travel may implicate an array of governing privacy laws. As a result, manufacturers may need to restrict what information is transmitted and where it is transmitted, depending on where the car is located at any given time.

To manage the legal risks, car companies should consider what data will be collected, how that data is being protected and whether the protection is appropriate given the relevant statutory obligations.

**Facing challenges and opportunities in a time of rapid change**

The legal risks and challenges faced by automotive manufacturers will continue to evolve and become more complex as cars use more IoT technology. At the same time, car companies have an opportunity to transform not only how they build their cars, but how they manage their legal risk.

For more information about issues raised in this article, please get in touch with the author.

DLA Piper’s Connected and Self-Driving Car group advises on the full range of business legal issues arising from connected and self-driving cars. Our multidisciplinary global team draws on the firm’s vast global experience in data protection and privacy, intellectual property licensing, environmental, regulatory, government affairs, litigation and tax to help stakeholders mitigate risk and take advantage of new opportunities.

Follow our DLA Piper LinkedIn Tech Sector showcase page and stay up to speed with our latest content dedicated to sector-specific legal and commercial issues.

*The author wishes to thank Aleksandar Kaludjerovic, a summer student at DLA Piper (Canada) LLP, for his contributions to this article.*

See also:

- DLA Piper Internet of Things (IoT) practice summary on our website
- DLA Piper has formed a global Connected and Self-Driving Car group
- DLA Piper's Technology's Legal Edge® blog
- DLA Piper's Privacy Matters blog

Articles relating to IoT and AI / machine intelligence from the DLA Piper Tech Sector thought leadership programme FY 2017-18:
- Regulatory Challenges for Electronic Communications Operators Offering IoT Connectivity Services
- Are banks ready for the Internet of Things revolution? Part 1: The rise of the Bank of Things
- Are banks ready for the Internet of Things revolution? Part 2: New legal issues created by the Internet of Things
- DLA Piper TechLaw Podcast Series
- DLA Piper TechLaw Podcast Series: Automation and AI: the legal issues