More data, more risk: The automotive industry rethinks its privacy strategies

17 November 2020

As the risk of ransomware attacks and data breaches continues to escalate, it's also raising greater concerns about data privacy. The automotive industry has been steadily increasing the amount of data it collects from car owners and drivers, prompting manufacturers to question how well their strategies and business practices can protect that information. Many companies within and outside the European Union are looking to one of the world's strictest regulatory privacy regime — the General Data Protection Regulation (GDPR) — as a template on which to build their own policies.

In this hoganlovells.com interview, Hogan Lovells partner Dr. Martin Pflueger and senior associate Charlotte Le Roux discuss data privacy restrictions and the new challenges they're creating for car and original equipment manufacturers (OEMs), as well as for the actors and stakeholders involved.

Cars are connected now more than ever before. They communicate with the Internet, smart phones, other cars, and networks. What data is being collected, and how is this creating new privacy and security challenges for the automotive industry?

Martin Pflueger: We are looking at a very complex ecosystem with a broad set of different types of data captured and processed, a variety of data subjects concerned and wide spectrum of players and stakeholders involved.

Vehicles are becoming increasingly connected and are collecting more and more data through various sources, such as vehicle sensors, telematic boxes, via mobile devices and infotainment systems, or via communication with other cars, infrastructure and networks. This means we are looking at a large variety of data: For instance, you have location and movement data, such as the speed or navigation of the car; status and behavioral data, such as tire pressure, fuel consumption and driving style; and your life habits data, like Internet use and infotainment systems preferences.

Then you have different categories of data subjects concerned by the processing of their data — the driver, the owner, the passenger, but also other individuals captured by your car's sensors and recordings, like pedestrians, cyclists and drivers in other cars. And you have the wide

spectrum of actors and stakeholders involved — OEMs, car manufacturers, digital service providers, repair services, dealers, and telecommunication operators – all of which may have access to personal data.

This leaves companies with a very complex actual landscape that they have to consider, in addition to the very complex legal requirements they need to comply with governing the privacy and security of data processed in the context of connected vehicles.

With the GDPR, companies face a European-wide law with very high standards, strict rules, and extensive accountability principles for the processing of personal data. But there are other legal regimes that come into play. For instance, you also have the e-Privacy Directive, with rules for electronic communication service providers, and the legal regime for the telecommunications sector. To give you one example, in certain cases, the authorities consider the car as "terminal equipment," like the computer or device you use to access the internet. This means that the same rules that apply to placing or reading cookies on your computer may also apply to data being stored or accessed in your car, just as if your car was a mobile device. And with new and very strict interpretations from the European data protection authorities, which put limitations on how companies can use and commercialize the data processed or collected through connected vehicles, it puts all of the responsibility on the companies to ensure compliance with this challenging legal environment.

How are we helping clients plan for and respond to these complexities?

Charlotte Le Roux: One important matter that Hogan Lovells is helping companies with is building a data governance framework.

Not only are car manufacturers making cars now, they are also making data and becoming data-centric organizations. They are collecting data from multiple sources to create value and serve different purposes, such as building customer loyalty, improving vehicle performance, and providing connectivity and mobility services.

In order to create this value, they need a strong data governance strategy. At Hogan Lovells, clients are offered assistance and advice way beyond the mere compliance with GDPR. It is well known that data is really highly regulated, whether it's personal data or not. There are various rules that can be taken into account, such as the rules concerning safety and security of the vehicles, its passengers and its data, e.g. event data recorders and vehicle-to-vehicle and vehicle-to-infrastructure (V2X) systems in the upcoming EU type-approval framework and the EU Cooperative Intelligent Transport System (C-ITS) framework. Other factors should also be borne in mind, like competition issues related to the use and sharing of data, commercial and contractual issues for the use of data that the OEMs "own," even though such a legal concept of data ownership gives rise to lengthy legal debates, and obviously, data privacy issues are at the top of all these strands. Therefore, the car manufacturers' data strategies must consider all these different regulations and issues, and different legal bases when it comes to personal data processing, which are then applied to different data usage scenarios.

Who owns the data, and who has the right to use it?

Pflueger: As Charlotte said, there's no clearly defined legal concept of ownership of data; it's not an absolute right like property. Ownership is rather determined by a bundle of different rights and restrictions, based on actual access and control as well as contractual and legal rights and constraints, which define how companies can use and commercialize data.

Developing a reliable data governance and use strategy is one of the most important aspects of enabling companies to make use of the greater value of their data and to comply with legal regimes. It requires implementation of actual safeguards to protect and manage access to data, the setting up of appropriate contractual agreements, and also a strategy that reflects the different legal regimes for the protection of data, like under intellectual property laws, trade secrets, and criminal law. In addition, all the regulatory constraints we have need to be managed, such as under data protection or competition law. That requires companies to develop a comprehensive data use strategy at an early enough stage enabling them to set up an appropriate framework to use and commercialize their data but also to exclude others from using it.

Can you explain the specific challenges companies are facing in making use of data collected through vehicles?

Pflueger: From a data protection law perspective, the challenges follow from the principle of purpose limitation and the requirements for the lawfulness of any secondary use of data. So imagine you have a car and you collect data from a driver for providing specific services. But you may also want to use the data for other purposes — not only to provide those specific services, but also for research and development purposes, such as to understand how your car functions, how to optimize your services, or how to train your AI systems.

The European data protection authorities stress the principles of purpose limitation and data minimization, which set high requirements for companies that wish to process personal data for purposes other than for which the data had been originally collected. For instance, if the optical sensors of your car capture images of pedestrians walking down the street for a driver assistance system and you want to use that data for purposes beyond providing the actual functionality, the authorities may expect you to blur and anonymize the data, which is technically tricky and often reduces value, such as where the training of a system requires a clear set of validation data. Sometimes you also can't comply with blurring the information because you need clear details of individuals. For example, you may need to understand the eye movement of the driver in the car, whether the driver got sleepy in case of an accident, or the facial expressions of pedestrians to train your system to understand how they react to the car. This is where we help clients to set up a concept and implement the necessary safeguards to be able to demonstrate that they can still process the data in a personally identifiable form in compliance with laws, as necessary for their business operations.

What are some other areas where Hogan Lovells has particular expertise with the challenges clients are facing?

Le Roux: One of the most challenging hurdles clients have to deal with is the extended territorial scope of the GDPR, which poses certain difficulties. This involves personal data collected from, for example, cars in Japan, which could be in some cases subject to GDPR. This could be a real business issue, especially when local data protection rules are more flexible than the GDPR.

When it comes to these stakes, it is important to work closely with the clients in order to avoid such a situation. The question of data localization is therefore key, and to get back to the client's data strategy, OEMs should also be taking this into account.

Pflueger: Yes, that's a big issue for many international companies. First of all, cars don't stop at any borders; you drive in different countries. But also the way data is collected, shared, and communicated to other cars, digital services, infrastructure, and networks might trigger the application of different legal regimes and multiple laws that you need to comply with. Therefore, as Charlotte said, the international component is an important aspect of an appropriate compliance strategy, and our team makes sure to work closely with clients early enough in their design, manufacturing, and marketing process to enable them to take into account the requirements stemming from strict European and other laws.

And data sharing is also an important issue for the auto industry.

Le Roux: Data sharing is undeniably another main challenge our team is currently working on. There is no doubt that data sharing is everywhere — it's a fact of life. Indeed, car manufacturers are sharing their data with multiple stakeholders, such as suppliers; partners; connectivity providers; infrastructure entities, such as private road managers; and public authorities, such as authorities organizing services. Access to data by other entities has been overly challenging; everyone wants to have a stake at the data.

When working with clients on these matters, it is important for them to be advised on the different regulations and also on new equipment obligations that are coming into force, notably those regarding the C-ITS framework.

It is also significant that many partners are claiming a form of ownership of the data. As such, Hogan Lovells is assisting car manufacturers to develop solely contractual arrangements to protect connected data for car manufacturers, but also for other stakeholders.

Another data-sharing issue relates to older regulations which are now coming into force. For the French government, for instance, it has consisted in its ability to regulate various situations regarding data sharing. Such situations are or will be regulated at European levels, so there's a risk here that discrepancies may come up between the national and the European frameworks, which should be avoided.

Pflueger: Data sharing is also a special challenge where we are looking at international data transfers outside the EU/EEA where specific requirements apply that need to be overcome, and courts and authorities have set high bars for transferring data.

As another aspect, we've also recently seen is a very strict interpretation of laws by the European data protection authorities affecting the sharing of data, such as in the current guidance of the European Data Protection Board on processing personal data in the context of connected vehicles and mobility related applications. There is obviously a demand to make use of the increasing amounts of data generated by connected vehicles, not only for providing a specific functionality or service, but also for further purposes, such as product optimization, which brings us back to the question discussed earlier in relation to secondary use.

While the GDPR allows for the use of data collected for one purpose also for compatible further purposes, provided very specific requirements are met, the situation becomes even more complex where also the rules of the e-Privacy Directive apply. The data protection authorities stress that in scenarios where the car qualifies as a "terminal equipment," falling under the scope of the e-Privacy Directive, data stored in the car may only be further processed and shared in very limited scenarios. More specifically, according to the authorities, the rules enabling further compatible use under the GDPR cannot be relied upon because their application would undermine the protection awarded by the e-Privacy Directive. That leaves companies in most cases with no other option than having to obtain consent which triggers enormous practical challenges. Applying this rather strict interpretation of the law, you significantly limit the scope of what companies can do with the data in the future.

What aspects of cybersecurity are particularly critical for clients to understand in this context?

Pflueger: As a car manufacturer, your security considerations are no longer limited to your own car. You need to consider your car's interfaces and connections with other cars, infrastructure or networks, digital service providers, and the internet. And you need to take into account that many actors involved have potential access to the data. This of course increases the number of potential vulnerabilities you have within the car. It opens possibilities for hackers and ransomware attacks, and potentially also very serious cybersecurity incidents, such as intruders taking control over driving functionalities and critical systems, which could trigger enormous road safety concerns.

That requires companies to rethink their cybersecurity and data security concept, including all players involved — the whole chain of subcontractors, suppliers, and third parties. They all need to be included in a comprehensive cyber strategy to enhance the security and protection of the overall ecosystem; and this applies over the whole lifetime of the vehicle. It's not like a car manufacturer can simply stop to provide support for critical services of an older vehicle model because it has been driven already for a long time. Since cybersecurity has become an essential element of the road safety of a connected vehicle, companies need to ensure the cybersecurity of

the car over the whole lifetime of the vehicle. And all these considerations need to be made against a fragmented and evolving legal landscape with different cybersecurity requirements following from various legal instruments.

Le Roux: There is no central cybersecurity framework or a general framework under the GDPR since the GDPR only provides for broad security obligations regarding personal data, regardless of the activity or the industry. Rather, different pieces of a cybersecurity framework come into play. One of them is the Directive on security of network and information systems (NIS Directive), which is quite key and relates to operators of essential services. Although car manufacturers are not really impacted by this regulation, they will surely and progressively become affected by this regulation when autonomous cars are operated on public roads.

It is likely that a new cybersecurity framework emerges, once it is more clear in regulators' minds what they want to have. In France, for example, the cybersecurity framework of operators of essential services could serve as a basis to be applied to automated vehicles' and automated driving systems' manufacturers. It is something that will be key to follow as well, because it will result in substantial changes with regard to the obligations that will apply to manufacturers.

Pflueger: That's a very good point. We see various developments at the European and international level in this area, from different regulatory and industry bodies, including the endeavors at the European Commission and also the recent United Nations ECE proposal for uniform provisions concerning the approval of vehicles with regard to cybersecurity. An interesting aspect will also be the development of standardization and certification processes, which could provide for a more comprehensive umbrella. But it's all just starting, and we are unfortunately still not there yet.

Le Roux: What is also noteworthy with new services is that car manufacturers are providing connectivity to end-users, so they could be considered as telecommunication services providers. They could therefore fall under another legal category that is quite highly regulated, and such category provides for a huge number of cybersecurity obligations that may be imposed on car manufacturers.

About Charlotte Le Roux:

As a senior associate, Charlotte Le Roux focuses her practice on commercial contracts and regulatory matters relating to information technologies, data, and cybersecurity, mobility/transportation, and telecommunications. She works on innovative subjects such as artificial intelligence, connected objects, autonomous vehicles, and, more generally, digital transition. She works closely with both French and international clients by providing them with regulatory advice or by assisting them in negotiating and setting up contractual schemes in various industry sectors, such as IT, automotive/transportation, energy, and financial institutions.

About Martin Pflueger:

Since the early days of his career, Martin Pflueger has been focusing his practice on advice in the areas of information technology, the Internet, e-commerce, and data protection, with a focus on the life sciences, technology, and the automotive industry. Not only from his various secondments with clients in the technology and pharmaceutical sectors, including as European privacy counsel for a worldwide leading cloud computing service provider, Martin brings extensive experience in drafting and negotiating IT agreements and evaluating new technologies and business models, as well as advising clients on all aspects of European and German data protection law.

Contacts

Dr. Martin Pflueger

Partner

Charlotte Le Roux

Counsel

> Read the full article online