Connected cars merge with payment technology

As connected cars proliferate, auto, tech and financial companies will form alliances that raise familiar legal issues in new contexts

By Howard Wettan

An estimated 125 million connected passenger cars are expected to ship worldwide by 2022, a 270% increase since 2018. In addition to using connected navigation and entertainment systems, and transmitting safety and performance data to insurance companies and car dealerships, their drivers may pay for everything from gas to dinner without pulling out their phones.

Before that happens, the automobile and payment industries will need to persuade merchants, who are reluctant to incur the costs associated with upgrading their payment acceptance technology, to continue to adopt new platforms to accept these types of payment solutions. It will take substantial investments and thoughtful partnerships between automobile manufacturers and payment technology providers to develop these solutions and enable their wide adoption. These partnerships will raise various concerns for carmakers and fintech industry players, who will need to consider a number of key legal issues as they negotiate the terms of these relationships.

Liability and risk

The parties must agree on how to allocate various risks, both between one another and with third parties. This poses particular challenges for automobile manufacturers and payment platforms because each must consider significant risks that have not previously been relevant to their product offerings. Automobile manufacturers must weigh the risks and potential costs that may arise from payment fraud, while payments companies now have to assess the risk of physical harm or property damage that can arise from vehicle use.

While new payment technologies have raised safety concerns in the past, these pale in comparison to the risks that arise when users perform transactions in moving vehicles.

Fraud

In the traditional debit or credit card model, banks and merchants allocate and bear the risk of fraud. Nevertheless, this model does not hold technology providers harmless to the extent, for example, that payment technologies fail to authenticate users properly and payment fraud results. In the connected car context, automobile manufacturers may look to payment technology providers for their authentication technologies and fraud prevention expertise, and require them to bear such risks. The cost of doing so will be allowing payment technology providers significant rights to test and control authentication technologies in the vehicle. On the other hand, to the extent automobile manufacturers consider proprietary wallets for their dashboards that involve any kind of stored value, or where automobile manufacturers stand in as merchants-of-record, their potential exposure to consumers for losses could increase.

Physical harm or property damage

While new payment technologies have raised safety concerns in the past, these pale in comparison to the risks that arise when users perform transactions in moving vehicles. Moreover, payment companies may be ill-equipped to evaluate these risks. Payment technology and service providers should carefully consider how consumers will use their technologies, demand that all uses be incorporated into an automobile manufacturer's safety testing and, if possible, require the automobile manufacturer to take responsibility for any potential safety issues. On the other hand, automobile manufacturers may want to hold any technology provider fully responsible for any software in the vehicle that results in malware or other security vulnerabilities that affect the vehicle's safe performance.

Data

For years, automakers have collected data, including geolocation, vehicle performance and maintenance data. Now, they will have to consider the new players, data categories and legal obligations regarding the collection, use and processing of data that arises from in-vehicle payment technology. While conflicts will inevitably arise as to who owns the data generated in the connected car payment technology ecosystem, ownership is less relevant than what data each party will contribute, how the data will be collected, each party's rights to use the data and each party's obligations to secure it.

Collection, contribution and use

Both parties will likely have extensive overlapping personal information regarding users. Partnerships between automakers and payment technology providers may also enable each party to gather data regarding financial transactions and geolocation that they would not otherwise have. Parties will likely bargain carefully regarding how to use data to target offers to customers, share data with third parties and ensure that users give informed consent based on clear and conspicuous disclosures regarding data retention and use.

The parties may also wish to use data for aggregated purposes. In doing so, they should consider stringent criteria for the aggregation of "de-identified" data so that the ability to "re-identify" data does not undermine commitments not to use or improperly disclose personally identifiable information.

Regulation

Since privacy regimes vary by jurisdiction, automakers will need to consider not only the legal requirements in their target markets but also those of the markets where their inherently mobile products may end up. When payment solutions put personal data in the possession of automakers, the EU's GDPR and other jurisdictions' laws may impose various requirements regarding data processing, and grant users significant rights regarding their data. These may include the rights to request the deletion of data and to prevent an entity from processing the subject's data.

The automotive industry has also provided guidance in this area. The Alliance of Automobile Manufacturers and the Association of Global Automakers published the *Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services*. Published in 2014, these relate to the collection, use and sharing of personal and vehicle information generated by vehicle technologies. Among other things, the principles require that automakers and manufacturers use personal information in a way that is consistent with the context in which it was collected, and only collect data needed for legitimate business purposes.

Data security

The security of payment card transactions will also warrant careful consideration. While laws and industry guidance address cybersecurity as to automakers, they do not articulate the detailed and extensive requirements that the Payment Card Industry Data Security Standards impose on all participants in the payment card process. These standards may extend to automakers (and original equipment manufacturers) whose systems and components enter the payment card processing transaction flow. Lax or inadequate security could destroy the confidentiality of payment card information, but may also enable access to the car's larger computer system, which controls other data sources and the car's operation. Automakers and payments companies will need to continue to craft creative security solutions, for example, devising methods to authenticate user payment requests in moving vehicles where near-field communication or EMV chip authentication technologies are unavailable.

Brand display

Automobile manufacturers and payment technology providers will likely have competing priorities regarding the display of their respective brands. Automakers may need to reconcile their highly valued full control of the driver experience with the demands of payment technology and service providers. While automobile manufacturers will generally control the environment where credentials are displayed, payments companies typically insist on making their brands visible when payments are made.

Auto manufacturers may also want user interfaces (e.g., display screens) that they tightly control, and such manufacturers may also want to double as broader platform service providers. User interfaces for drivers vary. For example, different automobiles provide different opportunities to display card art. Such displays typically double as opportunities to provide user terms and conditions that can be critical to proper collection of data. As a result, carmakers may have strong incentives to include payment technology providers in the experience, requiring them to share responsibilities regarding fraud risk and data collection.

Regulatory oversight

The parties bring their own industry regulators and oversight to the relationship. In the United States alone, payment technology solutions can be subject to review from the Federal Reserve Bank, Consumer Financial Protection Bureau and US Treasury Department, as well as the regulators of the 50 states. Meanwhile, automotive companies must contend with the National

Since privacy regimes vary by jurisdiction, automakers will need to consider not only the legal requirements in their target markets but also those of the markets where their inherently mobile products may end up.

Highway Safety Board and each state's Department of Motor Vehicles. Any commercial transaction between parties that are regulated differently can be challenging, but the disparity between the automotive and financial services industries will likely heighten these tensions.

As mobile purchasing expands into automobiles, the related risks concerning data, payment fraud and safety will receive extensive scrutiny from regulators around the world. Partners must consider questions that arise when one party's regulators impact the other. For example, if one party is subject to a regulator's request for information, will the other party voluntarily share information, or require a subpoena? Will the parties waive confidentiality rights? If a regulator requires changes to a joint product offering, how prepared are both parties to make the changes to ensure the product's viability? A product offering between automotive and payment technology partners will not survive regulatory oversight without a robust understanding between partners on how they intend to respond.

In particular, automobile companies should consider carefully how they design any proprietary digital wallet solutions in their vehicles. If the solution causes an automobile company to hold currency value, the company may become a money transmitter and need to seek licenses in nearly every state. Payment technology providers, on the other hand, should consider carefully how their proposed interfaces affect safety. Will transactions occur only after a vehicle comes to a complete stop, or only while moving at slow speeds through a toll plaza? Will transactions occur while traveling at high speeds while ordering ahead, for example, from a fast-food restaurant?

As mobile purchasing expands into automobiles, the related risks concerning data, payment fraud and safety will receive extensive scrutiny from regulators around the world.

IP ownership

Any two major technology platform companies will grapple with intellectual property ownership issues that may arise from their collaborations. While some companies place a high premium on acquiring and enforcing intellectual property, blocking competitors and seeking royalties, automobile manufacturers and financial services companies often place less emphasis on these concerns. Rather, both types of companies usually prioritize their freedom to operate.

Automobile companies may be more accustomed to dealing with technology providers who agree to limit the availability of their technology to one or a few automakers. While such limitations are typically not feasible for payment networks or issuers of payment cards as their business models require wide adoption, some payment technology providers may offer enhanced features to certain partners.

Automobile companies and payment technology providers may also argue for ownership of any developed technologies in their respective fields, while other companies may simply prefer to have ownership follow inventorship. In either case, two other considerations are important. First, all players will desire arrangements that allow for as much freedom to operate as possible, which may involve both broad licenses of co-developed creations, and also possibly licenses of pre-existing IP held by the partners (background IP). Second, even absent a heavy emphasis on which partner owns particular IP, it is important to settle the matter early. Too often, technology partnerships stall when specifications and other early-stage concepts are co-developed, and the parties begin to argue over who owns the IP rights.

The road ahead

As the world becomes more connected, automakers will increasingly offer drivers and passengers the ability to engage in an expanding range of online activities. Paying for goods and services will be chief among them.

Partnerships between and among automotive, fintech and technology companies will be required to bring payment technologies into passenger vehicles. For the companies involved, it is critical that they not only anticipate issues, but also understand how those issues will play out in new contexts ■

Contact

Howard Wettan
Partner, Silicon Valley
Technology Transactions Practice
M&A

T +1 650 213 0354
E howard.wettan@whitecase.com

whitecase.com