SQUIRE
PATTON BOGGS

Automobile Over-the-Air Transmissions

A Global Perspective

Global – July 2021

The rising tide of technological innovation is lifting up almost every aspect of modern life, and it will soon revolutionize the very cars we drive. Working on the same principle as iOS updates for an iPhone, over-the-air (OTA) technology allows car manufacturers to wirelessly transmit information to a vehicle, eliminating the need for regular visits to the dealership for software updates.[1]

Although OTA has already been used to deliver updates to small appliances like phones for many years, it has recently gained the attention of automobile manufacturers. Many have already incorporated software over-the-air (SOTA) technology in their vehicles to remotely update user interfaces like infotainment and navigation systems, while pioneers like Tesla and Nio have rolled out vehicles equipped with much more advanced FOTA (firmware over-the-air) features that can directly impact the driving and handling of the vehicles by delivering changes to sensors and brakes.[2]

As a result, FOTA is far more controversial and the subject of heated debate as countries around the world consider how to respond to its risks. This article will provide a brief overview of the benefits and drawbacks of OTA technology before discussing how global authorities seek to regulate the emerging technology as a whole.

There are numerous benefits of OTA for both automobile manufacturers and consumers. Traditionally, drivers are required to visit their local dealerships for software or firmware updates.[3] Eliminating such visits by delivering updates to cars remotely would considerably reduce labor costs for manufacturers while saving significant amounts of time for consumers, a win-win for all parties. In addition, companies can regularly improve various features of a vehicle and resolve issues *en masse*, implementing anything from quality-of-life changes like updating maps to safety enhancements like increasing the responsiveness of brakes.[4] Tesla has even shown it possible to improve engine performance via FOTA transmissions, augmenting battery efficiency without requiring owners to visit a Tesla dealership.[5]

However, the many advantages of OTA are counterbalanced by the new issues and risks it brings. The first significant problem is that of cybersecurity; vehicles without OTA store limited information, rendering them unattractive and unrewarding targets for hackers. However, vehicles with OTA capabilities are connected to an entire network of other OTA-capable vehicles through the cloud, meaning that a successful hack can give a perpetrator access to or control over tens of thousands of vehicles. In a widely-cited 2015 study, researchers famously demonstrated the possibility of hacking and hijacking a Jeep in transit, controlling everything from its radio to its brakes.[6] The potential carnage of a large-scale hack is especially worrying if cybersecurity measures do not keep pace, although it is worthy to note that the convenience and flexibility of OTA also allows manufacturers to quickly deploy security countermeasures.

Aside from security issues, OTA also opens the door to many personal data and privacy concerns. With OTA technology, connected cars would store substantially more personal data inside their systems, such as coordinates, travel history and owner details.[7] In addition, weather information, traffic conditions and other metadata connected cars share with others in their network could help identify specific car owners, posing additional threats to personal privacy.[8] Thus, it is reasonable to conclude that the proliferation of OTA would result in significant amounts of personal data, some sensitive in nature, being stored in manufacturer databases that are themselves lucrative targets for hackers. Of course, there is also the possibility of companies themselves violating personal privacy by selling collected data to advertisers. While there has been significant progress in recent data privacy legislation like the European Union's General Data Protection Regulation (GDPR), the emergence of a whole new source of consumer metadata courtesy of OTA increases the likelihood of violations.

General safety concerns regarding OTA also cannot be ignored. Given how modern vehicles are essentially computers with wheels running on millions of lines of code that control everything from steering to seat position, any glitch or error in an update could prove disastrous as its effects are amplified and compounded over an entire network of OTA-capable cars.[9]

[1] Choksey, Jessica Shea. "What Are Over the Air Updates for Cars?" *J.D. Power*, March 22, 2021.

[2] Doll, Scooter. "Over-the-Air Updates: How Does Each EV Automaker Compare?" *Electrek*, April 1, 2021.

[3] Choksey, Jessica Shea. "What Are Over the Air Updates for Cars?" *J.D. Power,* March 22, 2021.

[4] Quain, John R. "The Pros and Cons of Over-The-Air Software Updates in Cars." *Digital Trends*, October 29, 2018.

[5] Barry, Keith. "Automakers Embrace Over-the-Air Updates, but Can We Trust Digital Car Repair?" *Consumer Reports*, April 20, 2018.

[6] Orbanek, Steve. "Hackers Who Remotely Hijacked a Jeep to Speak about Cybersecurity Threats." *Penn State News*, Penn State University, January 31, 2018.

[7] Zurschmeide, Jeff. "Updates to Automotive Functions Could Spell Privacy Troubles." *Digital Trends*, January 27, 2016.

[8] Ibid.

[9] Barry, Keith. "Automakers Embrace Over-the-Air Updates, but Can We Trust Digital Car Repair?" *Consumer Reports*, April 20, 2018.

In 2016, a botched navigation system update for Lexus RX350s caused thousands of screens to be stuck in a perpetual cycle of rebooting and shutting down, rendering navigation systems inoperable.[10] As FOTA becomes more widespread, the potential impact of such errors significantly increases. While a glitched infotainment system is mildly inconvenient, a malfunctioning steering or braking system can be fatal.

To address these potential pitfalls of OTA, officials around the world have introduced various rules, regulations and standards to provide oversight and guide its development and implementation. In 2020, the United Nations introduced a management system for automobile cybersecurity while creating a legal framework for OTA updates. Chief among these advancements is the "UN Regulation on Software Updates and Software Updates Management Systems," whose goal is to ensure that manufacturers diligently and effectively tackle any weaknesses in security that are identified. Specifically, its provisions call for the establishment and availability of a software update management system for vehicles in road traffic, adequate protection of the mechanism tasked with delivering software updates, and safeguards for the software identification number of a vehicle to ensure readability.[11] To address potential issues that may arise during and after OTA updates, the regulations also require a function for reverting to a previous version in case of failed or problematic updates, certain conditions to be met before the installation process begins, and notifying the user if the vehicle needs to be taken to a dealership for service.[12]

These recommendations have seen some success; Japan was among the first to implement them, with implementation in the Republic of Korea slated for the second half of 2021.[13] In addition, the European Union has plans to introduce similar regulations sometime between 2022 and 2024.[14] Overall, with the recommendations' short application timetable and sweeping coverage, countries and car manufacturers have no time to wait if they seek to be compliant.[15]

Despite there being no specific regulations that address automobile cybersecurity in the US, the National Highway Traffic Safety Administration (NHTSA) recently released an updated version of its "Cybersecurity Best Practices for the Safety of Modern Vehicles." Sharing noticeable similarities with the UN recommendations, it also calls for substantial efforts to manage cybersecurity risks by detecting and responding to security incidents and securing vehicles by design to reduce risks along the value chain, among other measures.[16] However, the NHTSA update differs from the UN Recommendations in that it explicitly defined OTA and provided two relevant directives: requiring manufacturers to maintain the integrity of OTA updates by updating servers along with transmission mechanisms (T.22) and to design their security measures with the risks of compromised servers, insider threats, men-in-the-middle attacks, and protocol vulnerabilities in mind (T.23).[17] Thus, the update essentially offers a more technical approach with specific guidelines since the target audience is stakeholders of the US automobile industry. As this update was released in early 2021, it is too early to comment on its impacts. However, given that the NHTSA has long been a global role model in automobile regulation, this update could have worldwide ramifications as regulatory agencies in other countries release their own recommendations modeled off the US example.

Chinese regulators have also tried their hand at regulating OTA. In November of 2020, the State Administration for Market Regulation (SAMR) introduced sweeping new regulations targeting OTA based on the Regulation on the Administration of Recall of Defective Auto Products. Like the US and UN, it included several provisions for automobile data security, which were included in a draft provision introduced in May 2021 that has yet to see implementation. It advanced five "advocative" principles of data collection, which mandated that the default setting of any vehicle should be the non-collection of data, in-car processing so that the information that is gathered comes from within the vehicle instead of outside, data anonymization, a maximum retention period for data, and an applicable scope of precision for data gathering.[18]

However, these provisions are not the main focus of the new Chinese regulations. Instead, the overarching goal is to strengthen regulatory oversight on manufacturers installing OTA technology in their cars. The main articles, which have already been passed, established a new reporting mechanism through which extensive OTA-related records are collected. Chinese manufacturers who send updates using OTA must notify the SAMR by filing a record.[19] Other actions that require a record to be filed include using OTA to fix an issue in a car, investigations into incidents of hacking or successful establishment of remote control, and the issuing of recall orders.[20] Consumers can also file reports to the SAMR if they suspect a manufacturer is using OTA to conceal design flaws and avoid recalls by issuing numerous small updates that attempt to address large issues hopelessly beyond the capabilities of OTA.[21] All of these measures encourage greater transparency and communication between the trifecta of government, manufacturer and consumer, allowing the rollout of OTA to be as safe as possible.

[10] Goetting, Brittany. "Botched Lexus OTA Software Update Cripples Vehicle Navigation Systems." *HotHardware*, June 8, 2016

[11] Wuhrmann, Daniel, et al. "New UN Regulations for Cybersecurity and Software Updates in the Automotive Industry." *Reuschlaw Legal Consultants*, July 30, 2020.

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] Ibid.

[16] Pingol, Ericka. "NHTSA Updates Cybersecurity Best Practice of Modern Vehicles." *IOT Security*, Trend Micro, January 25, 2021.

[17] Ibid.

[18] 金融界. "國家市場監管總局:關於進一步加強汽車遠程升級(OTA)技術召." *MdEditor*, November 25, 2020.
See《汽车数据安全管理若干规定(征求意见稿)》for more information.

[19] Ibid.

[20] Ibid.

[21] Ibid.

In general, the main difference between the Chinese regulations, UN recommendations and NHTSA update is the former's focus on accountability and the latter two's focus on technical regulation. Both the UN and NHTSA hone in on the safety of OTA-capable vehicles, stressing the enhancement of cybersecurity measures to prevent glitches and deter hackers. On the other hand, Chinese regulators prioritize accountability and oversight, creating a paper trail that incentivizes companies to conduct their OTA rollouts ethically and safely. But perhaps the most glaring difference is the differing degrees of enforcement backing each of the regulations. While the Chinese regulations are legally binding, the UN's recommendations are non-binding *per se*, and the NHTSA updates are, alas, only updates and thus do not have the force of law behind them.

Nevertheless, all three parties have introduced the necessary building blocks for an effective regulatory approach to OTA technology. As previously mentioned, the NHTSA updates could touch off similar progress around the world, especially in East Asia, the EU and other wealthy countries. Ideally, the UN directives would find their way into the legislatures and regulatory agencies of member nations and be turned into law. Such regulations should combine the UN and US emphasis on technical security with the Chinese focus on accountability to create a two-pronged approach that both protects consumers and keeps manufacturers in line. In the meantime, countries should also ensure their regulatory agencies for automobiles are sufficiently empowered to implement new regulations and provide legal oversight instead of being a rubber stamp. After all, progress with new regulations means nothing without the availability of proper and reliable enforcement.

In the near future, as 5G technology enables us to send larger and more frequent updates, we will be faced with many tough questions about OTA. Many lines in the sand will need to be drawn. To what extent should governments and regulatory authorities get involved to ensure proper protection of consumer interests? Are there any implications on national security that need to be considered? And where do the responsibilities of the manufacturer end and those of the driver begin? Thus, it is important to start discussions now instead of later lest governments be caught in a frantic game of regulatory catch-up. It is always important to balance the excitement of technological innovation with prudence and diligence.

Full List of References in MLA

Barry, Keith. "Automakers Embrace Over-the-Air Updates, but Can We Trust Digital Car Repair?" *Consumer Reports*, April 20, 2018.

Choksey, Jessica Shea. "What Are Over the Air Updates for Cars?" *J.D. Power*, March 22, 2021.

Doll, Scooter. "Over-the-Air Updates: How Does Each EV Automaker Compare?" *Electrek*, April 1, 2021.

Goetting, Brittany. "Botched Lexus OTA Software Update Cripples Vehicle Navigation Systems." *HotHardware*, June 8, 2016.

Newcomb, Doug. "The Upsides and Downside of Over-the-Air Software Updates for Automobile Dealers." *WardsAuto*, November 6, 2020.

Orbanek, Steve. "Hackers Who Remotely Hijacked a Jeep to Speak about Cybersecurity Threats." *Penn State News*, Penn State University, January 31, 2018.

Pingol, Ericka. "NHTSA Updates Cybersecurity Best Practice of Modern Vehicles." *IOT Security*, Trend Micro, January 25, 2021.

Quain, John R. "The Pros and Cons of Over-The-Air Software Updates in Cars." *Digital Trends*, October 29, 2018.

Wuhrmann, Daniel, et al. "New UN Regulations for Cybersecurity and Software Updates in the Automotive Industry." *Reuschlaw Legal Consultants*, July 30, 2020.

Zurschmeide, Jeff. "Updates to Automotive Functions Could Spell Privacy Troubles." *Digital Trends*, January 27, 2016.

金融界. "國家市場監管總局：關於進一步加強汽車遠程升級(OTA)技術召." *MdEditor*, November 25, 2020.

Contacts

David S. K. Goh
Partner, Hong Kong
T +852 2103 0350
E david.goh@squirepb.com

David has been significantly involved in the automotive industry for many years. He has represented OEMs, assemblers, dealers, parts suppliers, and other automobile-related services companies in a wide variety of work. He is our lead partner throughout Asia-Pacific for a leading global manufacturer of passenger cars and commercial vehicles for all product and safety-related matters. He also acts for and advises various entities in a variety of regulatory, corporate and commercial matters.

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.