Hogan Lovells

Over-the-air software updates for IoT devices present companies with product liability and safety opportunities — and challenges

22 May 2018

Mobile devices within the Internet of Things (IoT) are continuously benefitting from rapid technological advancements. And once those devices are sold to consumers, over-the-air (OTA) software updates ensure they can be modified to stay current with new capabilities. Consumer electronics companies can remotely change product features, deliver messages or warnings, identify safety-related activities, gather data, and solve issues.

But OTA software updates also need to comply with existing and emerging regulations and laws. Companies are wondering whether the availability and ease of OTA updates could also lead to a legal requirement for them to monitor and act on issues — especially those involving safety — over the lifespan of the product. And when software updates can be installed automatically, will there be a need to obtain owner consent?

In this hoganlovells.com interview, Dr. Sebastian Polly, a partner in the Hogan Lovells Munich office, explores how OTA software updates are creating opportunities and challenges for companies in the product liability, safety, and compliance space.

What are OTA software updates and why are they unique?

Polly: OTA means wireless communications. It can be mobile, WiFi, radio — you name it. IoT devices pretty much all have capabilities that allow some form of OTA communications. OTA software updates are a way to allow a manufacturer, supplier, service provider, or another company to remotely access and change the product's programming. The unique feature is that they can change it, theoretically, whenever and wherever they want, even when the product is long gone — with a customer or user, out there in the field.

Many engineering, quality, and legal departments are just starting to explore opportunities. Remotely updating a product's software can solve many technical and legal issues. Moreover, OTA software updates can also deliver messages or send warnings directly on the devices to inform customers they're part of a safety campaign.

Also, once a product has already been on the market for a while, you can theoretically add new features to it or even change the entire way it behaves, or change existing functions and make them better or safer. And you can deactivate certain functions retrospectively. That, of course, goes along with certain legal challenges.

OTA software updates must comply with several areas of law. What are the concerns regarding civil law?

Polly: The impact of civil law is particularly in liability, under the Product Liability Directive (PLD), and general tort law, contract law, and warranty.

When we sell products to customers, we also promise that these products are fine and there is no discrepancy between the promise and the actual state. So if for whatever reason we learn that some features, aspects, or parts of the software or programming are not up to the task, we have a chance to retrospectively change something about the product.

But if, for safety reasons, we have to deactivate something, we might also create a warranty issue, because it takes something away from customers. You sell something and then at some point you figure out you need to change it to make it safer or better. So it's a legal opportunity, but a risk at the same time.

We have product liability and safety expectations that tell us that all the products we place on the market need to be safe. And when we talk about IoT products and connected devices, some people are already arguing that customers may have an expectation that these products can run certain updates and if there are safety challenges, they can be met by these ways of remotely accessing the devices.

What about the impacts of regulatory and criminal and administrative offense laws on OTA updates?

Polly: Regulatory law tells us again that the product needs to be safe. The General Product Safety Directive (GPSD) states that products aren't allowed to present any risk or only the minimum risk. But when products are evolving, you have moving targets. Of course every new product you are about to place on the market needs to be state of the art and absolutely safe, so you will probably already have new software updates on those devices. But what about devices that were sold weeks or months ago that are already out there: is it necessary, is it reasonable, or is there a duty to update those devices?

Regulatory law brings new questions. For example regarding customer communications, authority notifications, and CE conformity assessment implications in light of OTA software updates.

Think about how much energy, skill, and time goes into a product before you allow it on the market; typically, the legal department is part of this process. And once it's on the market, the same standards of interconnectivity and passion is necessary to safeguard any retrospective product amendments or changes, particularly through OTA software updates. This can be quite a challenge.

Every time we place a product on the market and figure out that there might be a safety risk, a company can also be — under the criminal and administrative offense law — obligated to minimize the risk, particularly by running an OTA software update.

What are the primary opportunities regarding OTA software updates?

Polly: One hot topic at the moment is the chance to use connectivity and OTA updates to swiftly and effectively identify and monitor safety-relevant activities. For example, data from products can be used to report on the intended use, misuse, or failures and defects. OTA software update capabilities allow companies to identify if their product actually behaves in the right way once it is in the field or if there is an issue.

They also give the option to directly reach potentially affected persons, so you can inform users about a recall. Many companies don't know the end-customer: you sell to a distributor, who sells to a retailer, and they sell over-the-counter to an end-customer, and the end-customer gives it to a friend. You have no idea who actually has the device. But even if it was an over-the-counter device, you still have the option to push something onto it. This is a strong argument that you can use for product safety authorities: you can say you've made a very effective recall action without publishing it in any newspaper or making any big public announcement, but just by specifically targeting the products. So this is a major chance — you just have to get it right from the business, technological, and legal angles.

It is also possible to effectively and swiftly solve potential product issues. If something might be wrong with the software, you can reprogram or deactivate features, or even deactivate an entire product if necessary. It's a strong tool; you just have to use it right and operate within the legal boundaries.

And the primary challenges?

Polly: From a legal angle, the challenge is to make sure that the whole certification approval or conformity assessment procedure is still in order, and that you figure out if and when you have to notify an authority. For example, there is no such thing as a "silent recall" in the consumer area if there is a mandatory authority notification obligation. Just because you are technologically able to directly access a user's product does not automatically mean that it is not necessary to notify an authority about the issue.

Another challenge is, when a product has OTA capabilities, what is the reasonable safety expectation? Can customers, users, or even the broader public expect that the products are kept safe for the entire life span? We all know that the product needs to be safe at the exact moment when you place it on the market, but does state of the art require that you keep it up to date and safe, particularly if you figure out that something can be done better?

Also, we know that OTA gives us the capability to collect data, but does it create or lead to a duty to collect and analyze the data? And if it does, will this lead to a duty to act and how can companies properly handle huge amounts of data in light of product safety?

And when does a company need someone’s consent to launch an OTA software update? This is a big issue when it comes to contractual terms and relationships. In a perfect world, a company would be able to simply push or force a safer software version on a device. However, the product is typically somebody else's property. And what about certain end-of-life aspects? How long does a company actually have to provide OTA software updates for its products in the field?

What is the main takeaway regarding the relationship between OTA software updates and product liability and safety?

Polly: Legal departments in particular should familiarize themselves with both OTA chances and OTA challenges. There are a lot of advantages, but there are also a lot of legal obstacles. It is important to address potential risks making sure that the company, its brand, and its decision makers — who actually make these update decisions — are legally protected.

About Dr. Sebastian Polly

Dr. Sebastian Polly’s key focus is on product liability, product safety, and product compliance law. He is particularly experienced in the automotive, chemical, consumer goods, electronics, and energy industries. Sebastian has assisted numerous clients with the rollout of innovative products. He assesses legal risks, develops preventive liability mitigation strategies, and is experienced in dealing with European market entry requirements.

Contacts

Dr. Sebastian Polly

Partner

> Read the full article online