Close

THE CONVERSATION

Academic rigour, journalistic flair

Huawei's ability to eavesdrop on Dutch mobile users is a wake-up call for the telecoms industry

May 10, 2021 2.40pm BST

viewimage/Shutterstock

Author

Greig Paul
Lead Mobile Networks and Security Engineer, University of Strathclyde

Chinese technology provider Huawei was recently accused of being able to monitor all calls made using Dutch mobile operator KPN. The revelations are from a secret 2010 report made by consultancy firm Capgemini, which KPN commissioned to evaluate the risks of working with Huawei infrastructure.

While the full report on the issue has not been made public, journalists reporting on the story have outlined specific concerns that Huawei personnel in the Netherlands and China had access to security-essential parts of KPN's network – including the call data of millions of Dutch citizens – and that a lack of records meant KPN couldn't establish how often this happened.

Both KPN and Huawei have denied any impropriety, though in the years since the 2010 report, Huawei has increasingly found itself labelled a high-risk vendor for telecoms companies to work with, including by the UK's National Cyber Security Centre.

To better understand this story, and to consider whether other telecoms networks may have had similar security vulnerabilities to KPN's, we need to look at how complex mobile networks are run. KPN essentially granted Huawei "administrator rights" to its mobile network by outsourcing work to the Chinese firm. Legislation is only now catching up to prevent similar vulnerabilities in telecoms security.

Commercial pressures

Huawei is one of the three dominant radio equipment providers in the world, alongside Ericsson and Nokia. These giant technology companies provide the base stations and equipment that deliver mobile phone signals. Operators like KPN increasingly pay these companies not only to buy the equipment, but also for them to support and maintain it.

The telecoms market in which KPN operates is one of the most price-competitive in the world. European mobile operators saw average revenues per user in 2019 of €14.90 (£12.85) a month, compared with €36.90 a month in the USA. European spend on telecoms services are also reducing year-on-year as operators compete to offer the best deals to consumers.

Lower revenues force operators to carefully manage costs. This means that operators have been keen to outsource parts of their businesses to third parties, especially since the late 2000s.

Large numbers of highly skilled engineers are an expensive liability to have on the balance sheet, and can often appear underused when things are running smoothly. Such jobs are often outsourced, with personnel transferring to the outsourced provider, to help operators to cut their payroll costs.

Outsourcing gone too far

When everything is working, very few people notice outsourcing. But when things go wrong, outsourcing can often significantly complicate recovery, or create a large "single point of failure" or security issue.

In the UK, for instance, mobile operator O2 has seen at least one outage which has been linked to the use of outsourced functions. Where large numbers of operators rely on the same outsourcing partner, any issue or security breach affecting the outsourced provider can have a widespread impact.

Still, outsourcing by mobile operators is widespread. And firms in the UK and across Europe have often turned to Huawei to provide IT services and to help build core networks. In 2010, Huawei was managing security-critical functions of KPN's core network.

Administrator access

At the same time, equipment suppliers like Huawei are trying to move away from merely selling equipment and towards providing a managed service, including installation, maintenance and support. This helps them create recurring revenue in an industry that has generally been dominated by large five-year or ten-year purchasing cycles.

But as these vendors add services to their repertoire, they gain wider access to the mobile networks they work with. This could include certain security-critical parts of telecoms networks, which are often designed to work in trusted, secure environments.

In the scenario where a vendor like Huawei also provides a managed service, they find themselves sitting in a uniquely privileged position, with inside knowledge of their own equipment, and with direct access to trusted management interfaces.

This creates the high-tech equivalent of putting all your eggs in one basket. It's akin to giving the combinations of the bank vault to the same security guard in charge of the CCTV camera footage. It's difficult to reliably monitor operations carried out by the vendor without relying on that vendor's own software.

In cases where a vendor has been designated as high-risk as a result of their own product security practices, it's very difficult to know whether that vendor didn't do anything untoward. This is the situation KPN apparently found themselves in with Huawei back in 2010.

Huawei's privileged access to KPN's network could have allowed the Chinese firm to listen to calls made by Dutch citizens. viewimage/Shutterstock

Are changes needed?

With at least one operator aiming to reduce European operating expenditure by €1.2 billion, and 5G deployments bringing new opportunities for managed services and software-based solutions to be used in networks, decisions around outsourcing will continue to play an important role for mobile operators going forwards.

But legislation is rapidly catching up. The UK has proposed a telecoms security bill, and associated draft secondary legislation includes requirements for network operators to monitor all activity carried out by third party providers, to identify and manage the risks of using them, and to have a plan in place to maintain normal network operations if their supplier’s service is disrupted.

For some operators, it’s conceivable this might mean bringing key skills back in-house to ensure there’s someone watching the (outsourced) watchmen. In the case of KPN, these measures would likely have prevented Huawei from having seemingly unchecked and privileged access to its customers’ mobile data.

Mobile phones **Outsourcing** **Huawei** **Cyber Security Centre** **Telecoms** **Mobile network**