# Huawei Had Access to 6.5 Million Dutch KPN Users' Data and Phone Calls Including Prime Minister's: Report


The Chinese military-affiliated technology firm Huawei, which supplied telecom equipment to Netherlands' largest mobile phone network KPN, had unlimited access to the Dutch company's 6.5 million users including the then Dutch Prime Minister's phone calls and personal data.

On April 17, Dutch newspaper de Volkskrant reported that in 2010 KPN commissioned the Capgemini consultancy firm to do an internal investigation on the security of its Huawei core network. However, Capgemini's confidential report was so damning that KPN buried it until recently when it was brought to light, according to de Volkskrant.

Capgemini reported that Huawei staff had penetrated to the core of KPN's systems and they could, and did have access to and eavesdrop on any subscriber number, including then Dutch prime minister Jan Peter Balkenende, from both within KPN's offices and from China. Chinese state security operatives based in China could do the same. They also had unlimited access to the personal data of all KPN users, said the report.

The KPN subscribers include the prime minister, cabinet ministers, politicians, businesses, individuals, and Chinese dissidents, which are the main targets of the Chinese communist regime's surveillance.

Huawei also knew which numbers were being tapped by the Dutch police and intelligence and security service—the AIVD (Algemene Inlichtingen en Veiligheidsdienst), according to the report.


The Huawei logo is pictured at the IFA consumer tech fair in Berlin, Germany, on Sept. 6, 2019. (Hannibal Hanschke/Reuters)

There were six Huawei employees who worked at KPN's former HQ in The Hague when Huawei's core network technology was being installed in

KPN's systems in 2009. The suspicion is that at least some of them were engaged in espionage activities, said the report.

KPN contracted Capgemini to investigate and report back in 2010 after being repeatedly warned by the AIVD that Huawei was suspected of widespread technological infiltration and espionage and that its network equipment was highly suspect. Based on the Capgemini report, KPN decided to refrain from outsourcing the full maintenance of the mobile core network to Huawei. Apart from that, the Dutch company took no further action but kept the report under wraps, according to de Volkskrant.

The Dutch newspaper also reported in March that Huawei also had unlimited access to the customer data of KPN's subsidiary Telfort as early as 2004. Despite an audit that confirmed and warned KPN in 2011 about the leak of Telfort's customer data, KPN didn't do further investigation nor did it warn Telfort's customers.

On April 19, KPN acknowledged the existence of the report and said that it had "never observed that Huawei took client information," and none of its suppliers had "unauthorized, uncontrolled, or unlimited access to our networks and systems."

After KPN's statement came out, inside sources told de Volkskrant that KPN's core might still be exposed to spies, because Huawei still has access to and some control over KPN's 4G network now. Huawei employees have "administrator rights" on KPN's core platform due to Huawei's equipment being installed there.

As the main supplier of KPN's 3G and 4G mobile network equipment, Huawei denied any claims of improper monitoring on KPN users. "We have never been accused by government bodies of acting in an unauthorized way," it said, according to The Guardian.

Huawei with close ties to the Chinese communist regime's military has caused widespread security concerns in many western countries. The U.S. government has blacklisted and put sanctions on Huawei and its suppliers, while the Chinese tech firm is vying for domination in the global 5G network.

## Sen. Warren Speaks out on Treatment of Jan. 6 Capitol Breach Detainees in Isolation