

United States Senate

WASHINGTON, DC 20510

October 7, 2019

Brad Smith
President
Microsoft
One Microsoft Way
Redmond, WA 98052

Dear Mr. Smith,

We're writing in response to a recent article in *Bloomberg Businessweek*, which includes your remarks about the Chinese telecommunications company Huawei. You encouraged the United States government to disclose additional intelligence about Huawei's espionage, so that business leaders "can decide for ourselves" whether to continue dealing with the company.

We appreciate Microsoft's communications with our offices and your understanding of the threats posed by Huawei. We also understand that many American companies have conducted business in good faith with Huawei and other Chinese telecommunications companies. While the U.S. government and American industry must take certain steps to protect our people and our telecommunications infrastructure, we do not want to cause undue harm to those American companies.

We believe, however, that a review of publicly available evidence indicates that the security concerns about Huawei are real and urgent. To highlight those concerns to American citizens and businesses, we list below just some of this evidence:

Espionage Activities

- Huawei's president and founder, Ren Zhengfei, is a former engineer for the People's Liberation Army and a member of the Chinese Communist Party (CCP). The CCP has office space and minders inside Huawei's Shenzhen headquarters.¹
- Beginning in 2006, the Chinese government financed and built the African Union (AU) headquarters in Addis Ababa, Ethiopia. Huawei servers inside the building secretly transferred data to servers in Shanghai every night for five years until the theft was discovered.² The AU replaced its Huawei servers at great expense, and declined an offer by China to help configure its new servers.

¹ Davies, Rob. "The Giant That No One Trusts: Why Huawei's History Haunts It." *The Guardian*. 8 December 2018. <https://www.theguardian.com/technology/2018/dec/08/the-giant-that-no-one-trusts-why-huaweis-history-haunts-it>

² Cave, Danielle. "The African Union Headquarters Hack and Australia's 5G Network." Australian Strategic Policy Institute. 13 July 2018. <https://www.aspistrategist.org.au/the-african-union-headquarters-hack-and-australias-5g-network/>

- Last year, Huawei technicians collaborated with Ugandan intelligence officers to hack an encrypted messaging platform used by a political opponent of the regime.³
- Earlier this year, Polish authorities arrested a Huawei sales director and former Chinese diplomat on charges he was spying for the Chinese government.⁴
- An independent research firm in the United States examined hundreds of Huawei products and “found Huawei devices to be less secure than comparable devices from other vendors” with “hundreds of cases of potential backdoor vulnerabilities, ... a large number of known vulnerabilities... and hundreds of potential 0-day vulnerabilities.”⁵
- A recent think tank study reviewed the resumes of 25,000 Huawei employees and found several who were simultaneously employed by Chinese intelligence services.⁶

Technology Theft & Economic Warfare

- Huawei has received tens of billions of dollars in grants, export finance, and loan guarantees from China’s state policy banks, which indicates the government’s vested interest in Huawei’s overseas expansion.
- Huawei allegedly used shell companies in Iran and Syria to deceive European banks into clearing hundreds of millions of dollars in transactions that violated U.S. sanctions against doing business with the repressive regimes in Tehran and Damascus.⁷
- Earlier this year, the U.S. government indicted Huawei for stealing advanced robotics technology from T-Mobile in the United States.⁸ The company allegedly offered rewards to employees who stole trade secrets from competitors.
- In 2003, Cisco filed suit against Huawei, alleging “systematic and wholesale infringement of Cisco’s intellectual property.”⁹ It was later established that Huawei copied proprietary source code from a Cisco router down to the letter, including coding errors, help screens, and user manuals. A third-party expert concluded the similarities between the two sets of code were “beyond coincidence,” despite Huawei’s claims to the contrary.¹⁰ The case was settled out of court.

³ Parkinson, Bariyo, & Chin. “Huawei Technicians Helped African Governments Spy on Political Opponents.” 15 August 2019. <https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017>

⁴ Gera, Vanessa & Chan, Kelvin. “Huawei Fires Sales Manager Who Poland Charged With Spying.” Associated Press. 12 January 2019. <https://www.apnews.com/4eeef2461614b93aca237b728c22baa>

⁵ Finite State. “Finite State Supply Chain Assessment: Huawei Technologies Co., Ltd.” <https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf>

⁶ Hille, Kathrin. “Huawei CVs Show Close Links With Military, Study Says.” Financial Times. 7 July 2019. <https://www.ft.com/content/b37f0a9e-a07f-11e9-a282-2df48f366f7d>

⁷ Stecklow, Dehghanpishah, & Pomfret. “Exclusive: New Documents Link Huawei to Suspected Front Companies in Iran, Syria.” Reuters. 8 January 2019. <https://www.reuters.com/article/us-huawei-iran-exclusive/exclusive-new-documents-link-huawei-to-suspected-front-companies-in-iran-syria-idUSKCN1P21M11>

⁸ FT reporters. “Huawei Accused of offering bonuses to staff to steal secrets.” Financial Times. 29 January 2019. <https://www.ft.com/content/9bb5d5da-239a-11e9-b329-c7c6ceb5ffdf>

⁹ Ferry, Jeff. “Top Five Cases of Huawei IP Theft and Patent Infringement.” Coalition for a Prosperous America. 13 December 2018. <https://www.prosperousamerica.org/top-five-cases-of-huawei-ip-theft-and-patent-infringement>

¹⁰ Chandler, Mark. “Huawei and Cisco’s Source Code: Correcting the Record.” Cisco. 11 October 2012. <https://blogs.cisco.com/news/huawei-and-ciscos-source-code-correcting-the-record>

- In 2010, Motorola filed suit against Huawei after a Motorola employee with ties to Huawei was stopped from boarding a flight to Beijing with a carry-on bag full of confidential documents from Motorola.¹¹ The lawsuit revealed that Motorola employees created a company to funnel Motorola's trade secrets to Huawei. The case was settled out of court.
- A former cybersecurity executive for Nortel has implicated Huawei in the company's downfall, warning other companies against doing business with Huawei. He alleges Huawei was involved in cyberattacks that emanated from China, stealing business plans and intellectual property. These attacks contributed to Nortel's bankruptcy.¹²

This evidence, in conjunction with testimony from U.S. government officials and our allies, Britain, Japan, and Australia, makes a compelling case that Huawei serves as an intelligence-gathering apparatus for the Chinese state. As Secretary of Defense Mark Esper has said, "Huawei is the means by which China would get into our networks and our systems, and either attempt to extract information or to corrupt it, or to undermine what we're trying to do."¹³

Of course, the government has more classified evidence to support this case, and we sympathize with your expressed concern that Microsoft and other businesses are not privy to this intelligence. We believe the Federal Bureau of Investigation or the intelligence community could share more of this intelligence in an appropriate fashion to affected businesses. We would welcome further conversation with Microsoft and other businesses about coordinating such briefings.

Thank you again for Microsoft's cooperation with our offices. And thank you for the many ways in which Microsoft works with our military, intelligence community, and law enforcement agencies.

Sincerely,

¹¹ Ferry 2018.

¹² Payton, Laura. "Former Nortel Exec Warns Against Working for Huawei." Canadian Broadcasting Corporation. 11 October 2012. <https://www.cbc.ca/news/politics/former-nortel-exec-warns-against-working-with-huawei-1.1137006>

¹³ Rogan, Tom. "Mark Esper Suggests Britain Should Ban Huawei, Mike Pompeo Should Do the Same With Israel." Washington Examiner. 06 September 2019. <https://www.washingtonexaminer.com/opinion/mark-esper-suggests-britain-ban-huawei-mike-pompeo-should-do-the-same-with-israel>



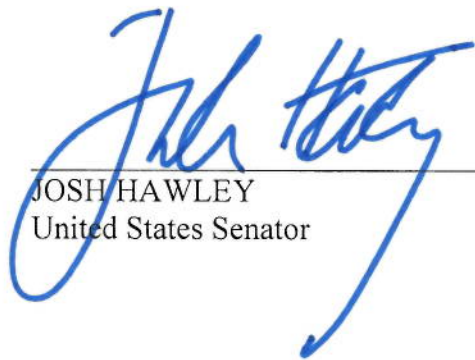
TOM COTTON
United States Senator



MARCO RUBIO
United States Senator



RICK SCOTT
United States Senator



JOSH HAWLEY
United States Senator



MIKE BRAUN
United States Senator