PROTECT AMERICA'S WIRELESS CONSUMERCHOICE alliance

PROTECTING AMERICAN NATIONAL SECURITY - FACTS ABOUT THE SPRINT/T-MOBILE MERGER

American national security is inextricably linked to our digital future. As we see nearly every day, foreign entities, competitors, and adversaries are targeting American networks to gain access to government secrets, economic information, and personal data – and we can only expect it to increase.

The Trump Administration has made it clear that the creation of a secure 5G network through a U.S. national security lens, stating in the administration's first National Security Strategy document (Dec. 2017): "We will improve America's digital infrastructure by deploying a secure 5G Internet capability nationwide."

Major mergers and transactions affecting America's public infrastructure have always required a robust debate on national security and foreign policy interests. No proposed merger should be approved without essential national security implications being fully vetted by the FCC, Congress, and through the CFIUS process. There are several national security and foreign policy concerns at the center of the proposed T-Mobile-Sprint merger that remain unaddressed.

The T-Mobile/Sprint merger, which purports to be America's pathway to 5G, requires intense scrutiny, especially when it is reliant on so much foreign investment. Whether Sprint and T-Mobile want to admit it, is a proxy discussion for a host of international issues that matter to policy makers and consumers alike, including vetting concerns about our interest, our security, and our values.

As former George W. Bush White House staffer and current Fox News contributor Bradley Blakeman explained in *The Hill* on September 2018:

> "Both Sprint and T-Mobile have a long history of using Chinese equipment suppliers Huawei and ZTE for devices integral to providing voice and data service, such as routers, servers, transmitters or receivers. These big suppliers — Huawei had more than $92 billion in revenue last year — have powerful tools at their disposal that could be used against the United States.
>
> As Sen. Tom Cotton (R-Ark.) and other members of Congress (including House Permanent Select Committee on Intelligence members) have warned for years, the Chinese government reportedly has the ability and propensity to compromise U.S. cybersecurity through Huawei and ZTE equipment embedded in our communications networks."

These attempts to infiltrate U.S. cyber networks continue and must be taken seriously, particularly given a series of Bloomberg Businessweek articles in October 2018, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," and "New Evidence of Hacked Supermicro Hardware Found in U.S. Telecom," that show how Chinese government-affiliated

technologies appear to be targeting critical U.S. technology and telecommunications companies and infrastructure.

> "A major U.S. telecommunications company discovered manipulated hardware from Super Micro Computer Inc. in its network and removed it in August, fresh evidence of tampering in China of critical technology components bound for the U.S., according to a security expert working for the telecom company."

T-Mobile and Sprint have an entangled history with Huawei and ZTE, Chinese telecom companies accused of hacking and spying on foreign networks. While the FCC deliberates the proposed merger between the two companies, the U.S., Australia, Germany, and New Zealand have banned Huawei, and both T-Mobile and Sprint are yet to provide support for their claims to having stopped using Huawei technology. While United States government has lobbied allies not to do business with these Chinese companies, the Chief Financial Officer of Huawei was recently arrested for alleged violations of Iran sanctions.

Still, T-Mobile and Sprint have not provided support for their claims to have stopped using Huawei technology.

Wall Street Journal: Canadian Authorities Arrest CFO of Huawei Technologies at U.S. Request

The U.S. has an extradition request over Iran sanctions violations; in addition to being CFO, Meng Wanzhou is also daughter of the company's founder

By Kate O'Keefe and Stu Woo

Canadian authorities in Vancouver have arrested Huawei Technologies Co.'s chief financial officer at the request of the U.S. for alleged violations of Iran sanctions, the latest move by Washington against the Chinese cellular-technology giant.

A spokesman for Canada's justice department said Meng Wanzhou was arrested in Vancouver on Dec. 1 and is sought for extradition by the U.S. A bail hearing has been tentatively scheduled for Friday, according to the spokesman. Ms. Meng, the daughter of Huawei's founder, Ren Zhengfei, also serves as the company's deputy chairwoman.

The arrest comes at a critical juncture in U.S.-Chinese relations. President Trump and Chinese President Xi Jinping last weekend agreed to a temporary truce in a trade spat to negotiate a settlement. The U.S. has raised other concerns with China, ranging from spying to intellectual-property theft to Beijing's military posture in the South China Sea. China has said its actions are appropriate.

The U.S. has undertaken a campaign against Huawei, which is viewed as a national-security threat because of its alleged ties to the Chinese government. In the past year, Washington has taken a series of steps to restrict Huawei's business on American soil and, more recently, launched an extraordinary international outreach campaign to persuade allied countries to enact similar curbs.

China strongly protests the arrest and has urged both U.S. and Canadian officials to free Ms. Meng, according to a statement released by the Chinese Embassy in Canada.

The U.S. is seeking Ms. Meng's extradition so as to have her appear in federal court in the Eastern District of New York, according to people familiar with the matter.

A Huawei spokesman said Wednesday that Ms. Meng was arrested at an airport during a layover. "The company has been provided very little information regarding the charges and is not aware of any wrongdoing by Ms. Meng," he said. "The company believes the Canadian and U.S. legal systems will ultimately reach a just conclusion."

The spokesman said that Huawei complies with laws and regulations everywhere it operates.

The Wall Street Journal reported in April that the Justice Department had launched a criminal probe into Huawei's dealings in Iran, following administrative subpoenas on sanctions-related issues from both the Commerce Department and the Treasury Department's Office of Foreign Assets Control.

In 2007, Ms. Meng served as a board secretary for a Huawei holding company that owned Skycom Tech, a Hong Kong company with business in Iran and employees who said they worked for "Huawei-Skycom," according to a person familiar with the matter.

U.S. authorities have suspected Huawei's alleged involvement in Iranian sanctions violations since at least 2016, when the U.S. investigated ZTE Corp., Huawei's smaller Chinese rival, over similar allegations. The Commerce Department released internal ZTE documents that showed the company studied how a rival, identified only as "F7," had conducted similar business.

A ZTE representative didn't immediately respond to a request for comment. The Commerce Department this year penalized ZTE for breaking the terms of a sanctions-busting settlement—nearly shutting down the company after banning U.S. firms from selling it supplies—but then gave it a reprieve after ZTE agreed to pay a fine, change its management and fund a team of U.S. corporate monitors.

A document dated August 2011 said F7's proposal to acquire U.S. company 3Leaf was opposed by Washington. That strongly indicated F7 was Huawei, which tried to acquire 3Leaf in 2010, only to back away after a U.S. national-security panel recommended against the deal.

Ms. Meng is a Chinese citizen who went by the English name of Cathy Meng before changing it to Sabrina Meng a few years ago. The company says she joined Huawei in 1993 and has held a variety of positions in accounting divisions.

"China will see this as an escalation against Huawei and as an extraterritorial rendition," said James Mulvenon, general manager at defense contractor SOS International. "There will be tremendous domestic pressure in China to get her back."

Huawei is the world's biggest maker of equipment for cellular towers, internet networks and related telecommunications infrastructure. It is also the world's No. 2 smartphone brand.

For years, Washington has alleged the Chinese government could compel Huawei to tap into the hardware it sells around the world to spy or to disrupt communications. U.S. officials say they are intensifying efforts to curb Huawei because wireless carriers world-wide are about to upgrade to 5G, a new wireless technology that will connect many more items—factory parts, self-driving cars and

everyday objects like wearable health monitors—to the internet. U.S. officials say they don't want to give Beijing the potential to interfere with an ever-growing universe of connected devices.

Huawei has long said it is an employee-owned company that has never conducted espionage or sabotage on behalf of any government, and that doing so would jeopardize its business. The company said it poses no greater risks than its rivals do, given they share a common supply chain.

Some of America's closest allies, including most of the countries in the "Five Eyes" intelligence-sharing pact among English-speaking countries, have followed the nation's lead. Australia in August banned Huawei from its 5G networks, while New Zealand last week blocked one of its major wireless carriers from using Huawei. In Britain, BT Group PLC said Wednesday that it was removing Huawei equipment from its network, two days after a British intelligence chief questioned whether the country should be using the Chinese gear.

Observer: Is Journalist-Murdering Saudi Arabia Your Next Cell Phone Provider? Why You Should Worry

DAVID WADE, FORMER STATE DEPARTMENT CHIEF OF STAFF

Last year, BlackRock's Larry Fink penned the investor letter heard around the world. In it, he stated: "Society is demanding that companies, both public and private, serve a social purpose."

Fink's letter seems prescient in light of the murder of Jamal Khashoggi. In 2018, this is not just a foreign policy story; the decisions that companies make have a wider range of impact than ever before, and this story has affected not just Washington, but also Wall Street and Silicon Valley.

Case in point: Saudi Arabia is currently hosting the Future Investment Initiative (FII), known as "Davos in the Desert." Now, the event might be better known for who *isn't* participating than for who is. High-profile CEOs have made a public show of dropping out, including, among others, the heads of Uber, Ford and JPMorgan. Even the Secretary of the Treasury withdrew his attendance.

The story made its way west to Silicon Valley, in part because of the massive Saudi investment in SoftBank's venture capital division. SoftBank has become a new, big player in Silicon Valley venture capital circles because of a $100 billion fund raised by its founder. Of that $100 billion, $45 billion comes from Saudi Arabia's Public Investment Fund (PIF)—chaired by Crown Prince Mohammed Bin Salman.

That makes SoftBank and Bin Salman significant business partners, to the point of one employee stating: "We are married to the Saudis." It also means the pressure has increased on SoftBank in the wake of the Khashoggi murder. SoftBank's COO Marcelo Claure dropped out of this week's three-day event, but in a way, the damage had already been done. SoftBank's share price has collapsed 16 percentsince the Khashoggi news first broke; the company's recently announced second fund is now in jeopardy; and one investor, Amir Anvarzadeh of Asymmetric Advisors in Singapore, even removed SoftBank from his list of recommended stocks.

The scrutiny of SoftBank may not be over. Consider: SoftBank is by far the largest shareholder of Sprint, the fourth-largest mobile provider in the United States. SoftBank isn't just *an* investor in Sprint; it is *the* investor, with a controlling interest of 85 percent of Sprint stock. And at present, Sprint is putting the finishing touches on a merger with T-Mobile, which would give SoftBank four of the 14 seats on the new company's board and a 27 percent stake overall.

Why might this be affected by the Saudi-SoftBank connection? Because the centerpiece of the deal is the creation of America's first-ever 5G network. That would give SoftBank and Sprint a direct hand in some of the nation's largest and most sensitive communications infrastructure.

Foreign entities getting close to our critical infrastructure has been a long-running matter of public concern, and we need only to look back at the 2002 Dubai Ports World controversy to see a similar situation. There, too, a piece of critical infrastructure was set to be sold to an entity based in the Gulf, and it led, not just to a national outcry, but also to the president and Congress battling over a deal that ultimately fell apart.

This case is not only similar, it's arguably more sensitive than the issues at stake in Dubai Ports World. The national security implications of a 5G network go beyond those involved in simply owning a port, including issues like surveillance of personal phone calls and the mining of private metadata.

The government isn't blind to these concerns. In fact, going back to the Kennedy administration, there's been an inter-agency process in place—called CFIUS, (Committee on Foreign Investment in the United States)—to review, investigate and block transactions that would create a national security risk. But until recently, no one would have thought to add a Saudi Arabia link to the list of concerns.

But the recent news changes that calculus. The SoftBank-Saudi connection could lead regulators, and the public, to ask understandable and hard questions about the Sprint-T-Mobile deal. Among them: What, if any, Saudi Arabian money or investments are involved? What protections are in place to make sure no foreign entities penetrate the cell phone grid? And how will SoftBank and Sprint ensure privacy and security going forward?

The public may ask the same questions—and they may go one step further and voice their own concerns about Sprint and SoftBank. Today, consumers can wield massive market power, and when they decide that a brand or product isn't living up to certain values, they can abandon that brand or company. We vote with our patronage—and consumers and investors may make a statement here that governments may be too afraid to make themselves.

More broadly, this situation illustrates a truth about our era: foreign policy isn't only the stuff of diplomats and wonks and generals—it's the stuff of Main Street America. Companies will increasingly be forced to answer for who their allies are and will have to weigh in on social issues they've never faced before. It means that a great deal of new leverage can be found on Wall Street and in corporate board rooms—not just in Washington.

PROTECT AMERICA'S WIRELESS CONSUMERCHOICE alliance

PROTECT AMERICA'S WIRELESS KICKOFF PRESS RELEASE

Former Intelligence Committee Chairman, Congressman Mike Rogers, Advises CFIUS To Closely Examine The National Security Implications of Sprint T-Mobile Merger; Experts Announced the Launch of Protect America's Wireless

For Immediate Release: November 5th, 2018
Press Contact: Nicky Vogt at nicole@npstrategygroup.com or 610-389-1314

Link to Audio Recording of Today's Press Call

Citing serious national security concerns, experts unveiled a public awareness campaign calling for President Trump, Congress, and the FCC to properly vet the merger and put America's national security interests first

Washington, D.C. - On a press call held today**,** foreign policy professionals called for additional scrutiny of the Sprint T-Mobile merger and announced the launch of ***Protect America's Wireless*****, a public awareness campaign lead by experts in the field including former senior State Department officials.** The speakers warned that the pending merger could give foreign countries unprecedented access to our networks through the use of foreign-made networking equipment and billions of foreign money.

The campaign aims to raise awareness of these national security risks and to protect American wireless networks by ensuring these concerns are properly vetted while the merger is under scrutiny by the Committee on Foreign Investment in the U.S. (CFIUS) and other U.S. agencies. Protect America's Wireless is calling on President Trump, Congress, and the FCC to protect our national security by denying these foreign interests access to America's wireless communications.

Former U.S. Rep. Mike Rogers said, "Huawei, ZTE and China telecom all work together in an ecosystem that is coordinated in a way that we would be absolutely naïve not to pay attention to in regards to companies with serious connections to Huawei and ZTE as they're building out in other places around the world, and what that would mean to the threat to our systems and our intellectual property here in the United States. I hope this is a big consideration, and I know CFIUS is going to look at this, and look at this hard. My encouragement is they should look at it hard, and if these companies ever wanted to move forward on anything, they would have to fundamentally make commitments, I would hope they'd be willing to make, but I'm not sure that they're willing to make at this point."

David Wade, former State Department Chief of Staff said, "Major mergers and transactions affecting America's public infrastructure have always provided forums to discuss a range of issues including national security and foreign policy interests. You don't have to reach far back to remember the year long public debate over Dubai Ports World. In a global economy and a dangerous world, a merger that would facilitate the creation of America's first 5G network, reliant on so much foreign investment, will be a proxy discussion for a host of international issues that matter to policy makers and consumers alike, including vetting concerns about our interest, our security, and our values. That's an important debate and I'm grateful to these respected and experienced foreign policy voices for contributing to it."

Ali Al-Ahmed, The Gulf Institute, said, "I am a long time customer of T-Mobile, so are many of my friends. This makes me extremely uncomfortable to see Saudi-backed control of my cell provider. I am a journalist, and critic of the Saudi government. Khashoggi was a T-Mobile customer too. According to the New York Times this past week, the Saudi authorities were looking for Khashoggi's phone after murdering him and kept asking the Turkish government for it. This shows that the Saudi government is extremely focused on obtaining phone records, contacts, and contents of their critics.The Saudi government is doing this even before they have several seats on the board of T-Mobile. Just imagine what they will try after they have some access. I do not feel safe now, and I will not feel safer if MBS and his men have access to my cell provider."

Dr. Trita Parsi, Adjunct Professor of International Relations at the Edmund A. Walsh School of Foreign Service at Georgetown University said, "The Saudi Crown Prince - besides ordering the murder of a Washington Post columnist - is actively destabilizing the Middle East and putting Americans at risk. To provide him with the leverage of being a key stakeholder in America's telecommunications infrastructure of the future is beyond unwise. Americans simply don't want to have the Saudi government anywhere near their cell phones."

Kyle Downey, former GOP leadership staff, said, "Regardless of Tuesday's results, I expect the incoming Congress to ask the tough questions it should about the safety and security of America's wireless networks surrounding this merger and beyond. These are the type of concerns that unite members from both sides of the aisle."