US attorney general says encryption creates security risk

July 23 2019, by Tami Abdollah

U.S. Attorney General William Barr addresses the International Conference on Cyber Security, hosted by the FBI and Fordham University, at Fordham University in New York, Tuesday, July 23, 2019. (AP Photo/Richard Drew)

Attorney General William Barr said Tuesday that increased encryption

of data on phones and computers and encrypted messaging apps are putting American security at risk.

Barr's comments at a cybersecurity conference mark a continuing effort by the Justice Department to push tech companies to provide law enforcement with access to encrypted devices and applications during investigations.

"There have been enough dogmatic pronouncements that lawful access simply cannot be done," Barr said. "It can be, and it must be."

The attorney general said law enforcement is increasingly unable to access information on devices, and between devices, even with a warrant supporting probable cause of criminal activity.

Barr said terrorists and cartels switch mid-communication to encrypted applications to plan deadly operations. He described a transnational drug cartel's use of WhatsApp group chat to specifically coordinate murders of Mexico-based police officials.

Gail Kent, Facebook's global public policy lead on security, recently said that allowing the government's ability to gain access to encrypted communications would jeopardize cybersecurity for millions of law-abiding people who rely on it. WhatsApp is owned by Facebook.

U.S. Attorney General William Barr addresses the International Conference on Cyber Security, hosted by the FBI and Fordham University, at Fordham University in New York, Tuesday, July 23, 2019. (AP Photo/Richard Drew)

"It's impossible to create any backdoor that couldn't be discovered, and exploited, by bad actors," Kent said.

Allowing government access to encrypted devices also wouldn't prevent people from switching to any new services that may crop up around the world that U.S. agencies can't access, Kent said.

Encrypted communications are ones that are only available to users on either end of the communications. The increasing use of this technology has long been coined by the Justice Department as the "going dark"

problem .

Barr's remarks also acknowledged the need for encryption to ensure overall cybersecurity that has enabled people to bank relatively securely online and engage in e-commerce.

Barr said that to date, law enforcement in Garland, Texas, have been unable to access 100 instant messages sent between terrorists who carried out an attack there in May 2015.

U.S. Attorney General William Barr addresses the International Conference on Cyber Security, hosted by the FBI and Fordham University, at Fordham University in New York, Tuesday, July 23, 2019. (AP Photo/Richard Drew)

"The status quo is exceptionally dangerous, it is unacceptable and only getting worse," Barr said. "It's time for the United States to stop debating whether to address it and start talking about how to address it."

Ex-FBI director James Comey championed the need for a law enforcement workaround to encrypted devices and communications. He led a highly publicized push to gain access to an iPhone belonging to a perpetrator of a terrorist attack in San Bernardino, California, that killed 14 people in 2015.

From the Senate floor on Tuesday, Sen. Ron Wyden, D-Ore., responded to Barr's remarks in New York calling it an "outrageous, wrongheaded and dangerous proposal."

Wyden said Barr wants to "blow a hole" in a critical security feature for Americans' digital lives by trying to undermine strong encryption and advocating for government backdoors into the personal devices of Americans. He said strong encryption helps keep health records, personal communications and other sensitive data secure from hackers.

Effectively banning encryption in the U.S. by not allowing companies to provide unbreakable encryption, doesn't prevent it existing and flourishing elsewhere, and only makes Americans less secure against foreign hackers, Wyden said.

U.S. Attorney General William Barr addresses the International Conference on Cyber Security, hosted by the FBI and Fordham University, at Fordham University in New York, Tuesday, July 23, 2019. (AP Photo/Richard Drew)

"Once you weaken encryption with a backdoor, you make it far easier for criminals, hackers and predators to get into your digital life," Wyden said. He said he fears and expects that Barr and President Donald Trump would abuse the power to break encryption if they were allowed to do so.

Given their records "it is clear to me that they cannot be trusted with this kind of power," Wyden said.

Noah Theran, a spokesman for the Internet Association, said "strong

encryption makes us all safer and more secure" and protects Americans from daily cyberattacks that can compromise personal information. The trade association represents internet companies—including Facebook, Google, Twitter and LinkedIn—on public policy.

"Companies must not be required to engineer vulnerabilities into their products and services that could put us all at risk," Theran said.

Critics of the Justice Department position also point out that law enforcement agencies have been able to use unencrypted metadata to solve crimes and hired a private contractor to ultimately gain access to the iPhone linked to the San Bernardino attacks.

U.S. Attorney General William Barr approaches the podium to address the International Conference on Cyber Security, hosted by the FBI and Fordham

University, at Fordham University in New York, Tuesday, July 23, 2019. (AP Photo/Richard Drew)

"There is no way to give the FBI access to encrypted communications without giving the same access to every government on the planet," said Brett Max Kaufman, senior staff attorney with the ACLU's Center for Democracy.

"Technology providers should continue to make their products as safe as possible and resist pressure from all governments to undermine the security of the tools they offer."