

Leading tech firms join Apple suit over iPhone encryption

By Thomas Gaist
5 March 2016

US tech firms, including Facebook, Amazon.com, Google, Microsoft, Cisco Systems, Dropbox, Mozilla, Snapchat and others, filed legal briefs Thursday joining an Apple Inc. suit launched last month against the Federal Bureau of Investigation (FBI).

Apple filed legal challenges after the FBI demanded “backdoor” access to encryption systems used to protect iPhone data.

According to briefs filed by the corporations, the FBI’s demands are based on a false interpretation of a more than 200-year-old law, the All Writs Act, to effectively claim “boundless” power for the state to compromise electronic security systems. “The government’s order to Apple exceeds the bounds of existing law and, when applied more broadly, will harm Americans’ security,” a brief filed by a dozen tech firms, including Google, states.

The colonial-era All Writs Act has been radically reinterpreted by the government, according to the brief. The FBI and Justice Department cast the act as clearing the way for arbitrary decrees that would give the state access to new forms of security technology as they emerge.

“The All Writs Act was not designed to confer sweeping new powers,” the brief states. “Now, 200 years later, the government endeavors to reinterpret the All Writs Act as an open-ended source of new powers. It asks this Court to endorse an unprecedented expansion of the Act that would allow law enforcement and private technology companies to circumvent security features that protect customers’ sensitive information.”

The FBI’s demands also violate the 1994 Communications Assistance for Law Enforcement Act (CALEA), which authorized US government spying on communications but specifically excluded “information

providers,” according to a separate brief filed by a corporate faction led by LinkedIn, Twitter and eBay.

The ballooning corporate-government dispute over encryption emerged in relation to an iPhone belonging to one of the perpetrators of the terror attacks in San Bernardino. FBI representatives have claimed that unlocking the phone is critical to preventing further attacks.

San Bernardino County Attorney General Michael Ramos on Thursday issued an even more dire warning, saying that the iPhone in question could produce “a lying dormant cyber pathogen that endangers San Bernardino County’s infrastructure.” The attorney general’s office has declined to supply any evidence substantiating this claim.

The FBI-Apple conflict is fueling divisions within the corporate establishment and the state itself. Even within the US intelligence establishment, there is anxiety over the implications of advanced encryption hacking software for the state’s own information security. Leading pro-surveillance figures, including former National Security Agency Director Michael Hayden, have voiced misgivings over the FBI’s aggressive anti-encryption moves.

For their part, the tech giants seek to counter the damage done to their reputations in the wake of the 2013 leaks by Edward Snowden, which exposed their complicity in mass government spying.

Despite the divisions over encryption, the underlying solidarity of the corporations with the military and police apparatus of American imperialism was on full display this week, with appearances by Attorney General Loretta Lynch and Defense Secretary Ashton Carter at gatherings of tech leaders in Silicon Valley and Seattle.

In remarks Wednesday, Carter called for informal

arrangements to be worked out between the corporations and the government. “It would be better to work this out than have a law written,” he said. The defense secretary warned that failure to voluntarily cooperate would lead to the passage of formal laws that were less favorable to corporate interests.

He announced US military initiatives aimed at recruiting high-skilled tech professionals and firms on behalf of the Pentagon’s cyberwarfare and advanced weapons programs directed against Russia and China. He boasted of US plans to spend nearly \$72 billion on new military technologies in 2017, saying the funds would be used for “advancing our commanding lead in undersea capabilities and developing new hypersonic missiles that can fly over five times the speed of sound.”

The Pentagon was developing “artificial intelligence, autonomy and robotics,” Carter said. Automated weapons would ensure that “no matter what our enemies throw at our systems, they just work,” he added.

“The Defense Department is trying to break down barriers with commercial technology firms in an effort to speed weapons development and maintain its advantage over key adversaries, such as China and Russia,” the *Wall Street Journal* noted on Wednesday.

The appointment of Alphabet’s Eric Schmidt to chair the US military’s newly formed Defense Innovation Advisory Board (DIAB), announced Wednesday after a personal meeting between Schmidt and Carter, underscores the integration of the tech industry into the US global war agenda. The DIAB has been tasked with streamlining the US military’s technology acquisitions in tandem with the Pentagon’s research and development arm, the Defense Advanced Research Projects Agency (DARPA). The Pentagon-Silicon Valley collaboration is based out of a new facility in northern California, with a second research center now under construction in Boston.

The DIAB project aims to achieve technological breakthroughs on the order of the Internet or the jet engine, Secretary Carter said. The Pentagon’s latest budget includes a \$40 million item for the US intelligence-backed venture capital firm In-Q-Tel. The budget also calls for \$7 billion in funds for cyberwar, a \$1.5 billion increase from 2016.

Google and other firms that collaborate with the

Pentagon’s research will be handsomely compensated, DARPA Chief Arti Prabhaka made clear in her own remarks. “They’re going to go make money on it—that’s what they do as a private company,” she said.

In remarks in Seattle on Thursday, Secretary Carter further outlined the US military’s plans to bolster its presence in the world’s leading technology center, declaring his intention to build up “essentially, an outpost of the Pentagon on the West Coast.”

“This is the way it ought to be—the military community and the larger community together; the security imperative and our competitive and technological imperatives coming together, reinforcing one another,” Carter said.

“This meeting was Microsoft’s idea and I really salute you for it,” Carter continued. He went on to single out Microsoft for special praise for its previous cooperation with the security apparatus, saying the company has “built the bridge from the other direction.” He hailed the creation of Microsoft’s Cybersecurity Operations Center.

To contact the WSWS and the
Socialist Equality Party visit:

<http://www.wsws.org>