Obama administration pushes cybersecurity law to expand corporate-government collaboration

Ed Hightower
15 January 2015

Speaking at the National Cybersecurity and Communications Integration Center (NCCIC) on Tuesday, US President Barack Obama called on Congress to enact new "cybersecurity" legislation in response to alleged hacking attacks on US corporations, including Home Depot, Target and Sony Pictures.

Sweeping measures are necessary to address the threat posed by hackers to US financial, digital and physical infrastructure, Obama told the assembled officials.

"The problem is that government and the private sector are still not always working as closely together as we should," Obama said. "Neither government nor the private sector can defend the nation alone. It's going to have to be a shared mission—government and industry working hand in hand."

The legislation proposed by the Obama administration appears to be a repackaged version of the Cyber Intelligence Sharing and Protection Act (CISPA) of 2013 and the Cyber Intelligence Sharing Act (CISA) of 2014. Though presented to the public as a necessary security measure designed to protect citizens against identity theft and defend US infrastructure against hackers, the laws further expand the ability of the US government to acquire massive quantities of personal data without seeking specific warrants.

The intelligence sharing legislation, which the Obama administration is now seeking to push through Congress once again, gives legal immunity to corporations that grant the US government direct access to their networks and databases. In exchange for real-time access to their information systems, the big tech corporations would receive protection from state laws and constitutional privacy guarantees, as well as private contracts between individuals and communications firms.

"The proposal would shield companies from liability if they share information about cyber threats with the Department of Homeland Security, which has been setting up special units for threat analysis and sharing," according to a statement issued by the White House.

The Obama administration claims that the legislation includes protections to ensure that the state-corporate data sharing arrangements are not used to collect personal information. In practice, however, top government officials will be empowered to determine at any given time what is considered security-relevant data and what is strictly personal data, according to the Electronic Frontier Foundation (EFF).

"It [the legislation] is written so broadly that it allows companies to hand over large swaths of personal information to the government with no judicial oversight—effectively creating a 'cybersecurity' loophole in all existing privacy laws," the EFF wrote in a public statement.

Extensive information sharing within the US government already occurs through a number of mechanisms. The DHS NCCIC facility where Obama gave his remarks—referred to in the media as the US government's "cybersecurity nerve center"—coordinates information sharing between the National Security Agency (NSA) and a network of Information Sharing and Analysis Centers (ISACs) established to aggregate personal and consumer data for sharing with law enforcement and federal agencies.

In defense of the bill, Obama referenced the Sony Pictures Entertainment hacking episode—which the

government has blamed on North Korea—and other instances of hacking attacks on corporations as evidence that more spying and bulk data collection by state and private entities are necessary to prevent attacks against critical electronic infrastructure.

"With the Sony attack that took place, with the Twitter account that was hacked by Islamist jihadist sympathizers yesterday, it just goes to show how much more work we need to do, both public and private sector, to strengthen our cybersecurity," Obama said.

The new legislation also expands the government's power to prosecute internet users. The bill further entrenches draconian penalties for petty cyber crimes established by the Computer Fraud and Abuse Act (CFAA). The legislation provides for severe punishment against would-be publishers of copyrighted materials under the CFAA, a measure designed to protect entertainment conglomerates and corporate interests.

Activist Aaron Swartz was charged under the CFAA for distributing scientific journal articles online. Under the new proposals, Aaron Swartz, an Internet activist who committed suicide while facing a possible sentence of 35 years in jail and over $1 million in fines, could have received a 100-plus year sentence.

Obama's speech Tuesday sets the stage for his annual state of the union address next week, where "cybersecurity" will once again feature prominently.

All of the reasons offered to justify the Obama administration's new cybersecurity proposals are lies. The US government is the world's primary cyber-aggressor and is preparing for all out cyberwarfare against rival states, including Russia and China, in line with its openly stated objective of military dominance on land, at sea, in space and cyberspace. The cybersecurity measures are linked with the government's war preparations and are one more piece in the police-state scaffolding erected by the US ruling elite.