US government prepares new attacks on Internet privacy

Marcus Day
17 May 2012

Over the past month, the US government has ramped up its efforts to create a legal basis for the surveillance of Internet and electronic communication.

On April 26, the House of Representatives passed the Cyber Intelligence Sharing and Protection Act (CISPA). The bill was introduced as an amendment to the 1947 National Security Act, which as yet did not contain provisions pertaining to "cyber threats."

CISPA would require the Director of National Intelligence to create a system wherein members of the intelligence community would share "cyber threat information" with corporations and private organizations and "encourage" those organizations to do the same. The deliberately broad language of the bill would further institutionalize efforts to penalize government and corporate whistleblowers, in addition to creating heavy incentives for Internet Service Providers (ISPs), such as Comcast or AT&T, to police their users' communications and data.

The legislation proposes that cyber threats are constituted by certain types of information, namely those kinds "directly pertaining to a vulnerability of, or threat to, a system or network of a government or private entity, including information pertaining to the protection of a system or network from either efforts to degrade, disrupt, or destroy such system or network"; or "theft or misappropriation of private or government information, intellectual property, or personally identifiable information." In other words, nearly any kind of "information" could be defined as posing a cyber threat, and therefore would be the legitimate subject of government and corporate surveillance.

The American Library Association noted that the legislation would have severe consequences for the privacy rights of any person who makes use of electronic communication: "This bill would trump all current privacy laws including the forty-eight state library record confidentiality laws as well as the federal Electronic Communications Privacy Act, the Wiretap Act, the Foreign Intelligence Surveillance Act, and the Privacy Act."

Since CISPA has been passed by the House, it moves to the Senate, where it may be voted on as early as this summer. However, President Barack Obama has threatened veto the bill in its current form. Predictably, supporters of the Obama administration have claimed that the veto threat represents some newfound admiration for civil liberties on the part of an administration which has institutionalized the assassination and indefinite detention of American citizens.

In fact, the main point of criticisms from the Obama administration is that it wants the Department of Homeland Security to be in charge of monitoring communications. A report in Bloomberg noted, "Obama advisers including Howard Schmidt, the White House cybersecurity coordinator, have said information-sharing alone cannot provide adequate protection against hackers and spies. The White House supports a bill from Senator Joseph Lieberman, a Connecticut Independent, that would put the Department of Homeland Security in charge of regulating cybersecurity of the nation's vital systems and networks such as power grids."

Lieberman's bill, the Cybersecurity Act, would apply to any company "whose operations, if disrupted, would cause mass death" or "major damage to the economy, national security, or daily life,"—in other words applying to most, if not all, major computer networks.

For his part, Lieberman has previously gone on

record to express envy at China's ability to exert strict control over its citizens' online communications. He has proposed the creation of an Internet "kill switch" subject to executive power, similar to the methods used by the Egyptian regime to disrupt communications in the midst of last year's revolution.

In effect, Lieberman's bill would place the Department of Homeland Security in charge of a vast Internet and telecommunications police apparatus. As stalwart free-market defender Fareed Zakariah noted recently on CNN, the Department of Homeland Security already employs 230,000 people, while American intelligence organizations as a whole employ 30,000 people (at the least) whose sole function is to monitor domestic communications.

The current attempts to pass a "cybersecurity" bill come not long after two so-called anti-piracy bills, the Stop Online Piracy Act and the PROTECT IP Act (SOPA/PIPA), supported and drafted in consultation with the entertainment and publishing industry, were met with widespread popular anger and were criticized by prominent members of the tech industry.

Google, Microsoft, and Facebook did not oppose the earlier bills as an infringement of democratic rights, but rather as an impediment to doing business. As such, legislators have worked to make the present cybersecurity bills more amenable to the technology industry. Many of the same corporations who opposed SOPA/PIPA have either openly supported CISPA or remained silent.

In addition to the congressional bills under consideration, the FBI has also been meeting with prominent Internet companies in order to secure support for its own favored legislation, which would require the implementation of surveillance "backdoors" in many kinds of communications software and services, according to a report by tech Web site CNET.

A proposed law, drawn up by the FBI general counsel's office, would compel providers of increasingly popular communications technologies, for example Web based e-mail, such as Gmail or Hotmail; instant messaging on social networking sites such as Facebook; and Voice over IP services, such as Skype or Google Voice, to ensure that their code is "wiretap-friendly." The proposed law would amend the 1994 Communications Assistance for Law Enforcement Act, which currently only covers telecommunications companies and not the aforementioned Web-based services.

The FBI has increasingly complained over recent years that its ability to monitor the population has been impeded by the proliferation of new communications technologies, specifically singling out "Web-based e-mail, social-networking sites, and peer-to-peer communications." In fact, according to British newspaper the *Guardian*, the FBI recently circulated an Orwellian-sounding memo in which it claimed that many popular, ad hoc methods of maintaining online privacy, such as anonymisers and encryption, may be signs of "terrorist activity."

The report from CNET further illustrated the extent to which technology firms conditional opposition to a surveillance apparatus over the Internet is rooted solely in financial considerations: "Industry would like to see any new legislation include some protections against disclosure of any trade secrets or other confidential information that might be shared with law enforcement, so that they are not released, for example, during open court proceedings," said Roszel Thomsen, a partner at Thomsen and Burke who represents technology companies and is a member of an FBI study group. He suggests that such language would make it "somewhat easier" for both industry and the police to respond to new technologies."

The rapidity with which the US has renewed its attempts to exert greater control over the Internet reveals the urgency with which the ruling class views the necessity of monitoring and restricting both communication and the distribution of information. No faith should be placed in the willingness of any section of the political establishment or the technology industry to defend a free and open Internet.