June 1, 2016

Dear Senator,

We, the undersigned civil liberties and privacy groups, oppose the Botnet Prevention Act of 2016 (S. 2931), both as a standalone bill and an amendment to S. 356. The proposal would expand the activities covered by the Computer Fraud and Abuse Act ("CFAA") and create new authority for the government to hack computers that could result in severe collateral damage, and would give users no recourse if their systems are harmed. Without major changes, the legislation could stifle much needed security research.

The proposal would expand the existing prohibition in the CFAA against selling passwords to any "means of access." The provision could make criminals of paid researchers who test access in order to identify, disclose, and fix vulnerabilities. In addition, the proposal would create a broad new criminal violation and harsh penalties for damaging "critical infrastructure" computers. The scope of critical infrastructure has been broadly interpreted by the Department of Homeland Security,[1] and because hacking associated computers is already illegal under the CFAA, such an addition is unnecessary.

Further, the proposal may empower the government to obtain injunctions to force companies to hack user devices, or allow the government itself to do the hacking.[2] It also fails to require notice of any potential targeting of non-suspect or innocent consumers, such as botnet victims. Though the provision is ostensibly directed at stopping botnets, it could apply to a wide range of unrelated activities. For example, activist organizations frequently target for outreach hundreds of devices as part of campaign activities, but without intent to cause damage. The proposed changes, in conjunction with pending changes to Rule 41 of the Federal Rules of Criminal Procedure currently before Congress, represent a vast expansion of the scope of both government hacking and government mandated hacking in response to the threat of botnets. Given the potential impact on botnet victims, security and privacy experts have questioned the broader impact of such tactics.[3]

Finally, the proposal fails to address ambiguity in current law that has led to the use of the CFAA to prosecute security researchers, levy disproportionate penalties, and criminalize ordinary Internet activity.[4] The proposal will exacerbate the CFAA's existing problems and enable prosecution of behaviors well beyond malicious computer trespasses or hacking, which were the original and appropriate targets of the CFAA.

---

[1] https://www.dhs.gov/critical-infrastructure-sectors (The Department of Homeland Security's plan for the Information Technology Sector includes industries that depend upon security research, such as software companies and ISPs.)

[2] https://www.justice.gov/opa/blog/assuring-authority-courts-shut-down-botnets (The Department of Justice has used the civil injunction authority to interfere with the operation of botnets.)

[3] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=7433349

[4] https://www.theguardian.com/technology/2014/may/29/us-cybercrime-laws-security-researchers

Accordingly, we urge you to oppose the Botnet Prevention Act of 2016 in any form. If you have any questions, please contact Drew Mitnick, Policy Counsel at Access Now, who will communicate with the other signers.

Sincerely,

Access Now
Advocacy for Principled Action in Government
American Civil Liberties Union
American Library Association
Center for Democracy and Technology
Demand Progress
Electronic Frontier Foundation
Free Press Action Fund
Liberty Coalition
OpenMedia.org
R Street
Restore the Fourth
RootsAction.org
New America's Open Technology Institute