

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,

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