Oct. 19, 2015

Dear Senator,

We, the undersigned civil liberties and privacy groups, and security experts, write in opposition to the proposed amendment (No. 2626) from Senator Whitehouse to the Cybersecurity Information Sharing Act ("CISA") that would expand the Computer Fraud and Abuse Act ("CFAA").

Amendment No. 2626 would alter the CFAA in dangerous and unpredictable ways.

First, the amendment would expand the existing prohibition in the CFAA against selling passwords to any "means of access" without clarifying how the law applies to legitimate computer security research, such as paid researchers who identify and disclose software vulnerabilities. Second, the amendment includes a requirement that empowers government to obtain injunctions that can force companies to hack computer users for a wide range of activity unrelated to botnets, though the provision is ostensibly directed at stopping botnets. Third, the amendment would create a broad new criminal violation for damaging critical infrastructure, which is already illegal under the CFAA.

The Whitehouse amendment fails to address ambiguity in current law that has led to the use of the CFAA to prosecute valuable security research, levy disproportionate penalties, and criminalize ordinary Internet activity. We are united in our view that, at the very least, any amendment to the CFAA be subject to full and open debate and must not be tacked on to CISA, itself a highly controversial and complex piece of legislation.

The amendment would exacerbate existing problems with the CFAA and enable prosecution of behaviors that are not malicious computer trespasses or hacking, which was the original and appropriate target of the CFAA. Worse, these changes are being rushed through Congress without adequate debate over the far-reaching effects of its provisions.

Accordingly, we urge you to oppose Amendment No. 2626 to CISA. Please do not hesitate to contact Gabe Rottman, legislative counsel with the American Civil Liberties Union, at 202-675-2325 or grottman@aclu.org, with any questions or comments.

Sincerely,

Organizations

Advocacy for Principled Action in Government
American-Arab Anti-Discrimination Committee
American Civil Liberties Union
American Library Association
Bill of Rights Defense Committee
Center for Democracy and Technology
Constitutional Alliance
Copia Institute
Cyber Privacy Project
Defending Dissent Foundation
Demand Progress

Electronic Frontier Foundation
Fight for the Future
Free Press Action Fund
Government Accountability Project
National Association of Criminal Defense Lawyers
New America's Open Technology Institute
Niskanen Center
R Street
Restore the Fourth

Security Experts

Sergey Bratus, Research Associate Professor
Eric Brunner-Williams
Antonios A. Chariton - Security Engineer, IDAspis
Stephen Checkoway, Assistant Professor, University of Illinois at Chicago*
David L. Dill, Professor, Stanford University*
Aiden Riley Eller
Robert G. Ferrell, Security Expert
Joe Grand, Product Designer, Security Researcher, Teacher, Grand Idea Studio, Inc.
Carl Hewitt, Board Chair Standard IoT
Frederic Jacobs, Security Researcher, Swiss Institute of Technology (EPFL), Open Whisper Systems
Ryan Lackey, Security Researcher
Robert J. Lupo, Security Architect, IBM Inc.
Brian Martin, Risk Based Security, Director of Vulnerability Intelligence
Morgan Marquis-Boire, Senior Researcher, Citizen Lab, Munk School of Global Affairs, University of Toronto
Andrew McConachie, Internet Infrastructure Engineer
Katie Moussouris, Chief Policy Officer, HackerOne
David Wagner, Professor, University of California, Berkeley*
Stephen Wilson, Managing Director, Lockstep Consulting & Lockstep Technologies
Stefano Zanero, Chair, IEEE Computer Society, STC on Cybersecurity

*Affiliation provided for identification purposes only