

July 30, 2012

The Honorable Harry Reid
Majority Leader
United States Senate
Washington, D.C. 20510

The Honorable Mitch McConnell
Minority Leader
United States Senate
Washington, D.C. 20510

Re: Leahy CFAA Amendment to the Cybersecurity Act

Dear Majority Leader Reid and Minority Leader McConnell:

The undersigned individuals and organizations from across the philosophical spectrum share a commitment to ensuring our nation's cybersecurity in a manner consistent with the Bill of Rights and the rule of law. We write today regarding the Computer Fraud and Abuse Act, the subject of an amendment Senator Leahy has offered to the Cybersecurity Act, S. 3414. The Leahy amendment (SA 2579) would, among other things, increase penalties for CFAA violations. It is based on the Personal Data Privacy and Security Act, a bill that the Senate Judiciary Committee marked up in September. We write to urge that should the Leahy CFAA amendment come to a vote, it include the Grassley/Franken/Lee amendment adopted last year to ensure that mere violation of website terms of service are not treated as a CFAA crime.

While the CFAA is an important tool in the fight against cybercrime, its language is also both overbroad and vague. The law can be read to encompass not only the malicious hackers and identity thieves the law was intended to cover, but also users who have not engaged in any activity that can or should be considered a "computer crime." Any attempt to update this increasingly outdated 1986 law should start with revisions addressing this structural problem before considering any increase in the penalties for violations.

The CFAA imposes civil and criminal liability for accessing a protected computer "without" or "in excess of" authorization, but fails to define "authorization." This makes the definition of the precise activities that are punishable unavoidably vague. As a result of this lack of clarity, several courts have used companies' network terms of use, which lay out *contractual* constraints on users' use of those networks, to also define what constitutes *criminal* behavior on those networks. The consequence is that private corporations can in effect establish what conduct violates federal criminal law when they draft such policies – without even realizing it.

Our primary concern – that this will lead to overbroad application of the law – is far from hypothetical. At least two federal circuit courts have agreed that an employee who exceeds an employer's network acceptable use policies can be prosecuted under the CFAA. At least one federal prosecutor has brought criminal charges against a user of a social network who signed up under a pseudonym in violation of terms of service.

These activities should not be “computer crimes,” any more than they are crimes in the physical world. If, for example, an employee photocopies an employer’s document to give to a friend without that employer’s permission, there is no federal crime (though there may be, for example, a contractual violation). However, if an employee emails that document, there may be a CFAA violation. If a person assumes a fictitious identity at a party, there is no federal crime. Yet if they assume that same identity on a social network that prohibits pseudonyms, there may again be a CFAA violation. This is a gross misuse of criminal law. The CFAA should focus on malicious hacking and identity theft and not on criminalizing any behavior that happens to take place online in violation of terms of service or an acceptable use policy.

We believe that the Grassley/Franken/Lee amendment was an important step forward for security and civil liberties. It is designed to ensure that mere violations of consumer terms of service are not treated as criminal offenses under the CFAA except in very limited circumstances. It would strengthen the law and focus the justice system on the malicious hackers and online criminals who invade others’ computers and networks to steal sensitive information and undermine the privacy of those whose information is stolen. Should the Leahy amendment be brought up for a vote, it should include this important – and long overdue – fix to the CFAA.

Sincerely,

*Laura W. Murphy, Director, Washington Legislative Office
American Civil Liberties Union*

*Leslie Harris, President and CEO
Center for Democracy & Technology*

*Fred L. Smith, President
Competitive Enterprise Institute*

*Orin S. Kerr, Professor of Law
George Washington University**

*Norman L. Reimer, Executive Director
National Association of Criminal Defense Lawyers*

*Paul Rosenzweig
Visiting Fellow, The Heritage Foundation**

*Berin Szoka, President
TechFreedom*

**(Affiliation listed for identification purposes only)*

cc: Members of the U.S. Senate