April 2, 2013

The Honorable Bob Goodlatte
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

The Honorable John Conyers, Jr.
Ranking Member
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

The Honorable Jim Sensenbrenner
Chairman
House Subcommittee on Crime, Terrorism, and Homeland Security
U.S. House of Representatives
Washington, DC 20515

The Honorable Bobby Scott
Ranking Member
House Subcommittee on Crime, Terrorism, and Homeland Security
U.S. House of Representatives
Washington, DC 20515

Dear Representatives Goodlatte, Conyers, Sensenbrenner and Scott:

We, the undersigned organizations and individuals, oppose draft legislation reportedly slated for consideration this month to amend the Computer Fraud and Abuse Act by increasing penalties and expanding the scope of conduct punishable under the statute.

Ensuring the security of U.S. computer systems and protecting user privacy require strong federal laws to deter and punish those who maliciously attack U.S. networks. However, the CFAA does far more than this important task: the law endangers ordinary Internet users, academics, researchers and entrepreneurs.

As currently written, the CFAA imposes criminal and civil liability for accessing a protected computer without or "in excess of authorization." "Exceeds authorized access" is vague, and the government and civil litigants have pressed courts to find CFAA violations whenever someone uses computers in a fashion that the system owner doesn't like. This means private companies write federal criminal law when they draft their computer use policies. As a result, CFAA cases have been brought against users who violate websites' terms of service (TOS), employees who violate their employers' policies, and customers who breach software licenses.

A talented and promising young man, Aaron Swartz, recently took his own life while awaiting trial under the CFAA. Aaron's death has prompted an outcry for CFAA reform from legislators, law professors and Internet users across the political spectrum—including many who thought Aaron should have been prosecuted, but not under the CFAA and not under threat of such harsh penalties.

Unfortunately, the draft under discussion is a significant expansion of the CFAA at a time when public opinion is demanding the law be narrowed. This language would, among other things:

- Obliterate the sensible line between criminal attackers and legitimate users who are *authorized* "to obtain or alter the same information" but do so in a manner or with a motive disfavored by the server owner or expressed in unilateral terms of service (TOS) or contractual agreements;

- Substantially increase maximum penalties for many violations to 20 years or more, giving prosecutors a heavy hammer to hang over individuals charged with borderline offenses, and ensuring even minor violations with little or no economic harm (which ought to be misdemeanors at most) will be punished as felonies; and

- Make all CFAA violations a RICO predicate.

On its face, the bill might appear to limit the application of CFAA section (a)(2)'s "exceeds authorized access" crime by specifying categories of information protected from such access. To the contrary, the change expands the statute's reach by criminalizing activities "involving" broad categories of information. As a result, the bill would make it a felony to lie about your age on an online dating profile if you intend to contact someone online and ask them personal questions. It would make it a felony for anyone to violate the TOS on a government website. It would also make it a felony to violate TOS in the course of committing a very minor state misdemeanor.

It is unreasonable to expand CFAA penalties when the statute already makes illegal so much of what Americans do with computers every day. Expanding the scope of the CFAA to cover even more conduct is even more dangerous. This bill would give prosecutors and civil litigants a free hand to go after employees, social networking users, academics, researchers and other computer users for common online activities.

We therefore urge the Committee to reject the proposed draft language, including increased penalties. Instead, this Committee should adopt amendments that would bring the CFAA into the 21st century, with sensible fixes that will protect the ordinary Internet user, while addressing the serious problem of malicious computer attacks.

Sincerely,

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

Jessica McGilvray, Assistant Director
American Library Association

Katie McAuliffe, Executive Director
Americans for Tax Reform's Digital Liberty

Leslie Harris, President and CEO
Center for Democracy & Technology

Fred L. Smith, Founder and Chairman
Competitive Enterprise Institute

Beck Bond, Political Director
CREDO Action

David Segal, Executive Director
Demand Progress

Cindy Cohn, Legal Director
Electronic Frontier Foundation

Holmes Wilson, Co-Director
Fight for the Future

Matt Wood, Policy Director
Free Press Action Fund

Wayne T. Brough, Ph.D., Chief Economist and Vice President, Research
FreedomWorks

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

Paul Rosenzweig, Visiting Fellow
The Heritage Foundation*

Kyle O'Dowd, Associate Executive Director for Policy,
National Association of Criminal Defense Lawyers

Jennifer Granick, Director of Civil Liberties
Stanford Center for Internet and Society*

Berin Szoka, President
TechFreedom

*(Affiliation listed for identification purposes only)

cc: Members of the Judiciary Committee