HOUSE JUDICIARY COMMITTEE
SUBCOMMITTEE ON CRIME, TERRORISM AND HOMELAND SECURITY

HEARING ON HR 4175
THE PRIVACY AND CYBERCRIME ENFORCEMENT ACT OF 2007

WRITTEN TESTIMONY FOR THE RECORD

ROBERT HOLLEYMAN
PRESIDENT AND CEO,
BUSINESS SOFTWARE ALLIANCE

DECEMBER 18, 2007

Thank you very much for the opportunity to testify today on the urgent need for legislation to update our criminal laws and provide law enforcement with much-needed tools to find and prosecute cyber criminals.

Mr. Chairman, Ranking Member Forbes, we greatly appreciate the interest and leadership you have shown on this issue with your recent introduction, with Chairman Conyers, Ranking Member Smith, Chairman Scott, Ranking Member Forbes, and Representatives Davis, Jackson-Lee and Sanchez, of H.R. 4175, the Privacy and Cybercrime Enforcement Act of 2007. We also want to commend Congressmen Schiff and Chabot for their leadership on HR 2290, The Cyber Security Enhancement Act of 2207, which they introduced with Committee Members Delahunt, Lungren, Davis, Goodlatte, Wexler, Issa, and Sanchez. We appreciate their continued commitment to promoting consumer trust in the internet and online transactions.

BSA is the foremost organization dedicated to promoting a safe and legal digital world. We are the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Our members represent one of the fastest growing industries in the world. BSA

programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce.[1]

This holiday season, Americans will spend as much as 30 billion dollars for their online holiday shopping. They will be able to shop at thousands of stores, compare products, services and prices, without regard to time or geography in order to find just the right gift at the right price. But while they are doing so, many will worry that criminals are lurking in cyberspace waiting to steal their money or even their identity. Unfortunately, their concerns are justified.

We urge you to act swiftly to enact cybercrime legislation. Under today's law, the ability of law enforcement officers to act against cyber-criminals is limited by gaps and ambiguities in the law. Legislation is needed to correct these deficiencies.

The nature of the threat has changed. Today's cyber criminals are more potent than ever before:

1. Cyber crime today is overwhelmingly fueled by profit. Cyber criminals used to write malicious code for bragging rights. Not anymore. Now they are drawn to cyber space for the same reason that Willie Sutton robbed banks – because that's where the money is. Cyber criminals

[1] BSA members include Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, CA, Cadence Design Systems, Cisco Systems, CNC Software/Mastercam, Dell, EMC, Entrust, HP, IBM, Intel, McAfee, Microsoft, Monotype Imaging, PTC, SAP, Siemens PLM Software, SolidWorks, Sybase, Symantec, Synopsys, and The MathWorks.

attack business and financial institutions. But they also go after individuals' Social Security, credit card or bank account numbers. That information leads to identity theft and fraud and is often illegally traded online, for great profit.

2. Cyber crime is increasingly technologically sophisticated. Because cyber crime has become a profession, and because it is financially motivated, criminals have a tremendous incentive to innovate. In particular, the rise of vast, surreptitiously controlled computer networks, called "botnets," has led to an explosion in the number and types of cyber crimes committed.

For too long, cyber criminals have taken advantage of legal blind spots to brazenly threaten online confidence and security. For that reason, BSA has strongly advocated updating our cyber crime laws to meet the changing nature of the threat.

Importantly, this is an issue that Members of Congress on <u>both</u> sides of the aisle and on both sides of the Hill agree they <u>can</u> do something about and have shown that they <u>want</u> to take action.

There is broad congressional, law enforcement and industry support for legislation that will:

- Target botnets by criminalizing cyber attacks on 10 or more computers even if they don't suffer $5,000 worth of damages.
- Address new forms of cyber extortion where a criminal threatens to obtain information from a computer or to publicize information already obtained from a computer.
- Broaden coverage of the cyber crime laws to include computers "affecting" interstate or foreign commerce.
- Attack organized cyber crime by creating an explicit conspiracy to commit cyber crime charge
- Strengthen penalties by calling for the forfeiture of computers and other equipment used to commit cyber crime and by adopting tougher sentencing guidelines.

Earlier this year, Congressmen Schiff and Chabot introduced H.R. 2290, the Cyber Security Enhancement Act of 2007. BSA welcomed this legislation which addressed all the key issues I outlined. We would be delighted if this bill were to become law.

More recently, however, the action shifted to the Senate. On November 1st, the Judiciary Committee reported legislation introduced by Chairman Leahy and Ranking Member Specter, S. 2168, the Identity Theft Enforcement and Restitution Act of 2007. This bill also incorporated many of the provisions of a bill introduced

by Senators Hatch and Biden, S. 2213. The Senate passed this legislation **unanimously** on November 15th.

BSA applauded Senate passage of S. 2168, which covered the major areas needed for improvement that I highlighted earlier. We also would be pleased if this bill was enacted.

Most recently Mr. Chairman, you and Ranking Member Forbes and others on the Committee introduced H.R. 4175. This bill also covers the same major areas as the earlier bills, with the exception of a crucial provision to target botnets.

The legislation also has other provisions including data breach notification. BSA understands the seriousness of the problem that data breaches represent, and we are working with this Committee, and the seven other Congressional committees involved, to develop legislation. We are committed to comprehensive legislative action that increases online security, including data breach reform, but we are very concerned that inclusion of this or other provisions in a cyber crime bill will delay enactment of cyber crime legislation, on which there is substantial bicameral consensus.

In conclusion, our message is simple. Cyber criminals are not waiting to attack and we can't afford to delay. There is broad bipartisan support in the House and Senate for legislation to update our criminal laws in the areas I have summarized. We think it is vital to make these changes to our criminal laws as soon as possible. Such legislation deserves to be enacted, can be enacted and should be enacted as soon as possible.

Thank you.