National Association of Criminal Defense Lawyers

Norman L. Reimer
Executive Director

April 23, 2012

Dear Member of Congress,

This week, Congress will vote on pending cybersecurity legislation. The National Association of Criminal Defense Lawyers (NACDL) urges you to oppose any legislation that attempts to enhance our security by rendering our Fourth Amendment rights less secure. There are real cybersecurity threats before us, but they do not pose risks so great that we should cross all boundaries of constitutional restraint to seek protection from them.

NACDL supports six principles that cybersecurity legislation should embrace to successfully enhance our security interests and protect the Fourth Amendment, and encourages you to amend or oppose any legislation that does not abide by these principles

1) To preserve our constitutional protections while protecting our cybersecurity, legislation should empower the government to obtain and to share only the most particular information reasonably related to the cyber threat or vulnerability.

The legislation should also require providers to minimize and anonymize what private or proprietary personal identifiable information is revealed, unless there is probable cause to believe disclosure is essential to the identification of the cyber threat source. Providing only what is essential preserves resources, increases investigative efficiencies, and diminishes risks of compromising information not pertinent to cybersecurity. The government should not have broad dominion over the private communications of our citizens and industries.

2) To be an effective tool for defending the nation from cyber threats, cybersecurity legislation must focus only on the national interests in cybersecurity, and not serve as a pretense for obtaining evidence of other types of criminal offenses as an end run around the Fourth Amendment.

It is counterproductive to the national interests in cybersecurity that the information shared to investigate security breaches in cyberspace be used to prosecute criminal offenses other than cyber crimes. Inserting the investigation of all criminal offenses within the mission scope for cyber-criminal investigation is dangerous mission creep because it degrades our defenses against cybercrime.

1660 L Street, NW, 12th Floor, Washington, DC 20036 | Phone 202-872-8600 x223 | Fax 202-872-8690 | E-mail norman@nacdl.org | www.nacdl.org

3) The legislation must not surrender domestic law enforcement investigations to the military. Civilian agencies must maintain control of the cybersecurity regulation and information gathering as well as mediate what access is granted to other federal agencies.

Crime in the digital world is no less diverse in its intentions and consequences than crime in the physical world. As in conventional law enforcement, the apprehension of offenders is not only a federal response. Overall security awareness embraces much more than military and intelligence objectives, and while critical to our overall strategic cyber defenses, a civilian agency is better positioned than military or intelligence agencies to refer security threats and mission tasking to the community of public and private sector resources best prepared to respond to each kind of threat. Private and corporate information ostensibly offered to the government to enhance our cybersecurity should not be parlayed into military domestic intelligence assets.

4) Blanket civil immunity for breaches of all existing laws endangers the public more than it protects the nation.

Parties providing information to the government understandably do not wish to assume liability for civil penalties that could result from its disclosure; however, blanket immunity only encourages overly broad production of information that deters the prompt discovery and interdiction of cyber threats. The larger the scope of immunity, the greater violation of privacy and warrantless surveillance of private communications will result from document and data dumps that serve no legitimate cyber security purpose. A balance must be found that encourages private cooperation and yet does not give cybersecurity information providers a vehicle to escape all civil liabilities.

5) Reliance on the "third-party doctrine" does not vitiate privacy concerns.

All proposed cybersecurity legislation now before Congress ignores the interests of the private citizens whose private communications and personal information is being offered up by private service providers. American citizens, involuntarily and without notice, become subject to possible criminal prosecution for offenses discovered in electronic communications and stored data which they believed was private and confidential and constitutionally protected by due process, existing laws and the Fourth Amendment. Individuals do not lose their privacy interests in their electronic communications and privately stored data simply because they are being stored or transmitted by a third party. Cybersecurity legislation must not be exploited as a means of eviscerating those protections. Recently, in *United States v. Jones*, the Supreme Court GPS case, Justice Sotomayor noted that the notion that individuals have no reasonable expectation of privacy in information disclosed to third parties "is ill suited to the digital age . . ." Congress must not rely on this archaic doctrine as a basis for unlimited information sharing in cybersecurity legislation.

6) Any information that is shared for the purpose of investigating a cyber-threat must not be preserved indefinitely following the investigation and/or prosecution of the cybercrime.

To encourage the broadest private sector commitment to sharing information about cybersecurity threats, the information collected cannot become a data mining adventure to aggregate private and corporate data. Once the security issues for which data was provided have been resolved technically or by prosecution, no legitimate cybersecurity purpose remains for their retention.

NACDL appreciates the difficult task before you, and offers its support to you and your staff in ensuring the protection of our Fourth Amendment rights. Again, NACDL encourages you to oppose or amend any cybersecurity bill that does not limit the type of information shared and the use of such information as discussed above. Please do not hesitate to contact NACDL's National Security Counsel, Mason Clutter, with any additional questions at (202)-465-7658 or mclutter@nacdl.org.

Sincerely,

Norman Reimer
Executive Director