

---

October 4, 2013

Review Group on Intelligence and Communications Technology  
Mr. Richard Clarke  
Mr. Michael Morell  
Mr. Geoffrey Stone  
Mr. Cass Sunstein  
Mr. Peter Swire  
Office of the Director of National Intelligence  
2100 K Street, NW, Suite 518  
Washington, DC 20427

Dear Members of the Review Group:

**Board of Directors**

**Christian Dawson**

Co-Founder & Board Chair  
COO, ServInt

**David Snead**

Co-Founder  
Attorney, W. David Snead  
P.C.

**David Bryson**

Executive Vice President &  
General Counsel  
Endurance International  
Group

**Richard Feller**

Principal  
Hedgehog Hosting

**Dennis Johnson**

Senior Community Advisor  
iNET

**Andy Mentges**

CEO  
Jumpline, Inc.

**Aaron Phillips**

Vice President of  
Operations  
c-Panel

The continued success of U.S. Internet infrastructure companies, and the valuable role that these companies play in our nation's economy, can only be maintained if the United States reaffirms what can now only be described as a tenuous grasp on its status as the global leader in cloud computing. According to a recent study by The Information Technology & Innovation Foundation, revelations surrounding the PRISM surveillance program could cost U.S. based cloud providers up to \$35 billion in revenue. Additionally, 56% of respondents to a Cloud Security Alliance poll said they are less likely to use US cloud providers.

The first step in establishing this credibility must be to make the policies and collection activities of government agencies open to the public in the most transparent way possible. The Internet Infrastructure Coalition (i2Coalition), a group of over 60 companies that build and maintain the nuts and bolts of the Internet, recommends that the ODNI Review Group take the following steps to ensure that the United States can employ its technical collection capabilities in a manner that optimally protects our national security and advances our foreign policy while respecting our commitment to privacy and civil liberties:

**TRANSPARENCY**

i2Coalition has repeatedly called for greater transparency and appropriate privacy protection when it comes to our nation's intelligence gathering. Equipping the American public with the information they need to have an informed, transparent discussion about the merits of domestic surveillance is essential in striking a balance between National Security issues and concerns about the privacy of American citizens.

Senator Franken, Representative Lofgren and others have submitted legislation to address these issues. The Surveillance Transparency Act of 2013 would improve government reporting and allow voluntary disclosures of certain information related to data collection requests from the government. This legislation would require the government to annually report the number of FISC orders issued under sections 214 and 215 of the PATRIOT Act and section 702 of the FISA, as well as other information related to such queries. In addition, it would allow companies to voluntarily disclose the number of orders they have received and complied with, the general categories this information fell under and the number of users whose information was produced to comply. This will let the American public take part in a robust and informed debate about domestic surveillance while also protecting national security, and the i2Coalition urges this panel to put forth similar common-sense conclusions to increase transparency and protect privacy when it comes to the NSA's intelligence gathering.

---

**Alan Schoenbaum**  
Senior Vice President &  
General Counsel  
Rackspace

**Jeanine Wright**  
General Counsel  
Media Temple

## **MULTISTAKEHOLDER PROCESS**

The Internet infrastructure industry generated an estimated direct and indirect \$46 billion in annual revenue in 2010 with expected 20% growth by 2013, and a trade flow to the United States of \$9.2 billion. While we must continue to respect the need for accurate intelligence to safeguard our nation's security, we also need the opportunity for an open, robust discussion of how to do so while respecting personal privacy and Internet freedom. For our industry to continue to compete in a global economy, we need to ensure that U.S. Internet companies have a seat at the table when discussing issues of electronic surveillance.

## **INTERNATIONAL PRIVACY NORMS**

American cloud companies have for years been at the forefront of the global cloud computing market, but if something is not done to allay concerns over bulk collection of electronic data, non-U.S. companies will surely look elsewhere for their needs. European cloud computing companies eager to break into the international market have been quick to capitalize on the shortcomings of U.S. privacy laws, urging local companies to store their data close by, away from American servers.

Outlawing warrantless surveillance of online communications will alleviate concerns many international entities have about storing data on U.S. servers. Realigning U.S. surveillance policy to comply with established international privacy norms will help restore global confidence in American Internet companies whose competitiveness abroad diminishes with every new report of unjustified U.S. government intrusions on consumer privacy.

Sincerely,



Christian Dawson  
Co-Founder & Chairman  
i2Coalition