THIRD WAY

MEMO *Published February 23, 2016 • 3 minute read*

Looking Out for U.S. Economic Interests in Intelligence Oversight

Mieke Eoyang
Vice President for the National Security Program
@MiekeEoyang

Todd Rosenblum

Members of Congress on the Intelligence Committees and their staffs perform a critical oversight role. As the only non-executive branch personnel with access to intelligence collection programs, they are often the only people who can raise other policy considerations and expect to have those questions answered. While the primary role of the committees has been to ensure that the programs are effective in securing the nation and that taxpayer dollars are spent wisely, they can also perform an important function in looking at the economic impact of collection programs.

This paper is designed to help Members of Congress consider the impact to American economic interests in the course of their intelligence oversight.

The Problem

In today's telecommunications environment, an ever-increasing share of global communications transit the United States—either through the internet or other channels. U.S. dominance in technology and communications means that the infrastructure is often owned and operated by an

American company. But efforts by U.S. intelligence agencies to collect those communications, sometimes unbeknownst to the companies themselves, have serious negative implications for the reputation of those companies, domestic and international customer trust in American tech products, and the competitiveness of U.S. technology products in the global marketplace. A study by the Information Technology & Innovation Foundation (ITIF) concludes that the U.S. cloud computing industry could lose up to $35 billion over the next three years following Edward Snowden's decision to release information about a wide-range of classified national security programs. [1]

After the leaks by Chelsea Manning and Edward Snowden, and the cyber-security breaches of OPM and other government networks, the U.S. government cannot guarantee the secrecy of its intelligence programs or the data they collect. Thus, it is more important now than ever that intelligence agencies prospectively assess potential harm as a result of a disclosure.

Members of Congress can help ensure that the agencies have considered potential harm as part of their regular budget oversight by asking a series of questions about any intelligence electronic collection program to determine whether the risk has been appropriately evaluated:

1) Does the collection method involve a U.S.-owned company or facility?

a) Is the U.S. company witting?

b) Is the U.S. company compelled?

i) Is the U.S. company allowed to disclose anything about its participation?

ii) Does the company have a right to challenge the compulsion?

iii) Is the U.S. company compensated?

c) Has analysis been done to assess potential damage to the U.S. company from inadvertent disclosure of the program?

d) Have other U.S. agencies been consulted about the potential harm to other U.S. policy interests?

e) Has there been an assessment of the risk of reciprocal requirements being levied on the company or sector by the host nation?

2) Is U.S. person data involved?

a) What is the volume of the data collected?

b) What is the percentage of information in the take that is of national security interest?

c) Is the U.S. person data the target of the investigation?

d) Is the U.S. person data incidentally collected?

3) Does the collection method involve exploiting vulnerabilities in the technology platform, in particular, a cyber vulnerability?

a) Is U.S. information susceptible to the same vulnerability?

b) Has the risk of a potential adversary identifying and exploiting the same vulnerability been assessed?

c) Has the community compared the value of exploiting the vulnerability against the potential harm of not securing the vulnerability?

END NOTES

1. Daniel Castro, "How Much Will PRISM Cost the U.S. Cloud Computing Industry?", (Report), Information Technology & Innovation Foundation, August 5, 2013. Available at: http://www.itif.org/publications/2013/08/05/how-much-will-prism-cost-us-cloud-computing-industry.