OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
DIRECTOR OF LEGISLATIVE AFFAIRS
WASHINGTON, DC 20511

MAY 05 2016

The Honorable Ron Wyden
United States Senate
Washington, D.C. 20510

Dear Senator Wyden:

At the 9 February 2016 testimony before the Senate Select Committee on Intelligence, you asked that the Intelligence Community (IC) review and provide our assessment of the then-recently released Berkman Center "Don't Panic" report.

The IC firmly believes that strong encryption is important to protect the privacy and security of our citizens and their information. At the same time, however, and as has been widely reported, the rise of encryption has had a significant negative impact on lawful and authorized law enforcement and foreign intelligence collection activities that are important to our mission of protecting the public. The public debate on how we can best address the challenges associated with the proliferation of certain implementations of encryption is important, and the IC welcomes the contribution of the Berkman Center report to the ongoing discussion, even if the IC does not agree with everything in it.

At the outset, it is important to highlight that, while the contributors to the report did not "unanimously agree upon the scope of the problem or the policy solution that would strike the best balance," they acknowledged that "conducting certain types of survelance has, to some extent, become more difficult in light of technological changes." The contributors believe, however, that law enforcement and IC concerns about intelligence losses due to encryption can be successfully mitigated by other factors. We have not undertaken a line-by-line assessment of the report, but there are a few areas where we believe that the report's conclusions do not fully account for the realities we face. In particular, the report makes three findings that we think are incorrect:

1. The report suggests that the Government need not be concerned about the spread of encryption, since a great deal of information remains, and will continue to remain, unencrypted.
2. The report notes that the fact that the Government will still be able to obtain metadata should lessen the impact of more prevalent encryption.
3. The report asserts that the Internet of Things (IoT) will provide the Government new avenues to obtain important information about surveillance targets that will mitigate the loss of access to encrypted channels.

Notwithstanding the report's suggestion that end-to-end encryption is unlikely to be widely adopted by communications services providers, some of the largest providers of certain types of communications services have already implemented end-to-end encryption, and we are concerned that the trend may be for more and more companies to develop and market easy-to-use, seamless, end-to-end encryption as a standard setting. However, even if many

communications providers do not follow this trend, the spread of transparent and easy-to-use encryption will make it easier for criminals and terrorists to find a safe haven to conceal their illegal activities. This means that law enforcement and national security personnel are losing access to the one area that we care about the most – the content of communications of violent criminals and terrorists. Indeed, we have already seen that our adversaries are choosing to use encrypted communications for the express purpose of avoiding our surveillance. Thus, the availability and spread of certain implementations of encryption is having a real and present negative impact on law enforcement and foreign intelligence collection activities. With the growth of default encryption, this problem becomes magnified, expanding encryption from a limited number of persistent actors choosing to use it, to potentially everyone even without making the choice.

Second, the report suggests that communications metadata, which is generally unencrypted, can mitigate the loss of the content of encrypted communications. With due respect to the authors, this is simply wrong. While metadata is a valuable source of information, it does not replace the definitive value of content, such as when we can intercept two terrorists agreeing on a time, place, and method of attack. Metadata can tell us that a foreign spy is in contact with a government official; it generally cannot tell us whether that contact is innocent or nefarious. Metadata can tell us that two terrorists are in contact, but it generally cannot tell us when, where, and how they intend to strike. In short, metadata cannot replace content.

Finally, the Berkman Center report suggests that some of the gap in collection capabilities can be filled by using the IoT as a surveillance platform. While the IoT is expanding rapidly and data communicated by sensors in consumer products could provide a valuable source of some information about our foreign intelligence targets, data gathered from consumer products will never replace the content of communications now hidden behind encryption. As discussed above with respect to communications metadata, it is difficult to see how information obtained from a refrigerator, a washing machine, or a child's toy could mitigate the impact of the loss of the content of communications between two terrorists describing their plans and intentions to attack the United States. Moreover, the deployment of such products with encryption will also impede efforts to use them for surveillance. The report only cursorily addresses the radically varied capacities of different local law enforcement agencies around the country; many local law enforcement agencies simply do not have the resources to conduct this kind of technologically sophisticated surveillance. Even more troubling, the report fails to acknowledge the different privacy implications of collecting information from these sorts of devices inside one's own home.

The IC will continue to use the lawful tools available to it to acquire its foreign intelligence targets' communications. But the important public debate about the appropriate scope of lawful access to encrypted communications, and whether that access can be provided in a way that preserves the privacy and security benefits of encryption, must be informed by recognition that the increased use of encryption by those targets represents a significant impediment to our efforts to protect the nation, its citizens and our allies – an impediment that cannot be fully mitigated by alternative means.

The Honorable Senator Ron Wyden

We look forward to continuing the conversation with the diverse organizations represented by the report's contributors, as well as working with your committee on these important issues. If you have any questions, please contact the Office of Legislative Affairs at (703) 275-2474.

Sincerely,

Deirdre M. Walsh

Enclosure:
Copy of Article, *Don't Panic. Making Progress on the "Going Dark" Debate,* Published by The Berkman Center for Internet & Society at Harvard University