THE PERMANENT REPRESENTATIVE
OF THE
UNITED STATES OF AMERICA
TO THE
UNITED NATIONS AND OTHER INTERNATIONAL ORGANIZATIONS
IN GENEVA

February 26, 2015

David Kaye
Special Rapporteur on the Promotion of the Right to Freedom of Opinion and Expression
Office of the United Nations High Commissioner for Human Rights
Geneva, Switzerland

Dear Mr. Kaye:

The United States is pleased to respond to this first call for information from the new Special Rapporteur for the promotion and protection of the freedom of expression and opinion and looks forward to working with the Special Rapporteur during his occupancy of the mandate.

The United States has a long and proud tradition of defending freedom of expression, which is enshrined in our Constitution and robustly protected under our laws. Consistent with Article 19 of the International Covenant on Civil and Political Rights, these protections apply regardless of how the speech is articulated or the medium that is used.

In the United States, there are no laws that prohibit the development or use of encryption or anonymity online. Moreover, the United States Government strongly supports an open, interoperable, secure, and reliable Internet, and has long worked to promote accessibility, security, privacy, and freedom of expression online. Together with other States, the United States has worked to establish an international consensus around the principle that the same rights that people have offline must also be protected online, in particular freedom of expression.

As President Obama recently made clear, the United States firmly supports the development and robust adoption of strong encryption, which is a key tool to secure commerce and trade, safeguard private information, promote freedoms of expression and association, and strengthen cybersecurity. Encryption, as well as tools that assist with anonymity, are especially important in sensitive contexts where attribution could have negative political, social or personal consequences or when the privacy interests in the information are strong. In general, the free flow of information, opinions, and data helps foster transparency, creativity, innovation, and learning, and tools and methods that support this flow generate positive economic, social, and political consequences.

At the same time, terrorists and other criminals use encryption and anonymity tools to conceal and enable their crimes. This poses serious challenges for public safety. Society has an undeniable interest in law enforcement being able to investigate and prosecute terrorists and other criminals, and as President Obama recently made clear it is important to have a public

debate about how to address this issue. Misuse by a few, however, does not change the fact that responsibly deployed encryption helps secure many aspects of our daily lives, including our private communications and commerce. The United States will work to ensure that malicious actors can be held to account without weakening our commitment to strong encryption.

As a matter of policy, and consistent with our international commitments as a Participating State of the Wassenaar Arrangement, we continue to regulate the exports of certain forms of encryption. These items are controlled due to U.S. national security, foreign policy and law enforcement interests. The U.S. implementation of these controls can be found in the Export Administration Regulations, mainly in Sections 774 (the control list), and Sections 742.15 and 740.17 (licensing policy and license exceptions).

Consistent with this legal framework, as a matter of policy, the United States has long supported the development and use of strong encryption and anonymity-enabling tools online. The United States has a proud history of working with the international cryptographic community to develop and vet the strongest possible encryption algorithms for public and private sector stakeholders. This work dates back to the 1970s with international competitions that resulted in the Data Encryption Standard and, more recently, with the Advanced Encryption Standard, both of which became widely used international encryption standards. Currently, the Secure Hash Encryption (SHA-3), which was developed through another international competition we held, is in the process of becoming an international standard.

In addition, as part of the United States' commitment to defend and promote human rights online, the United States Government has provided funding to support the development and dissemination of anti-censorship and secure communications technologies to ensure that human rights defenders and vulnerable civil society communities, such as journalists, LGBT activists, and religious minorities, operating in repressive contexts are able communicate securely, associate safely, and express themselves freely online.

Sincerely,

Pamela K. Hamamoto
Ambassador