



August 7, 2014

Ms. Rebecca Cooper, Hearing Clerk
United States Senate
Committee on the Judiciary, Subcommittee on Crime & Terrorism
Washington DC. 20230

Re: July 23, 2014 – Questions for the record “Taking Down Botnets”

Dear Ms. Cooper,

Thank you for your letter requesting clarification and response to additional questions for the record from Senator Sheldon Whitehouse.

As testified, it is imperative to recognize the vast majority of botnets and cybercrime originates beyond our borders. Building on public-private efforts we need to look beyond U.S. law and Mutual Legal Assistance Treaties (MLATs) to spur collaboration and data sharing. A sustainable effort requires a strategy and legal provisions to address international law, including data sharing and protection of privacy.

1. As we discussed, the Subcommittee is exploring possible legislation to address the botnet threat. What specific proposals would you recommend we include in such legislation?

MLATs have been an effective mechanism to help enable the exchange of evidence and information in criminal and related matters for the past century. Recognizing the global scope of cybercrime, MLATs need to be overhauled. In addition, either supplemental or new MLATs between the United States and other countries which have become a safe-haven for cybercrime need to be explored. Related legislation including the Computer Fraud and Abuse Act (CFAA) need to be updated to include trafficking of access to botnets, perpetuating malvertising, click-fraud spam and related tactics. In the absence of such changes, criminals today can freely sell and trade access to botnets or execute denial-of-service (DDoS) attacks with little fear of legal ramifications.

2. Do you have any comments on the legislative proposals that Assistant Attorney General Caldwell discussed in her testimony?

Faced with the evolving complexity of cybercrime and explosive growth of cloud services, mobile devices and social media, OTA agrees with Assistant Attorney General Caldwell that the Computer Fraud and Abuse Act (CFAA) and the Electronic Communications Privacy Act (ECPA) are in need of updates. As the U.S. is becoming a data driven society and accumulating vast amounts

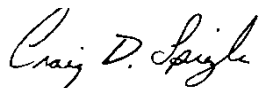
sensitive data including location tracking, user profiling, bio-metrics and facial recognition data, we need to assure that such data should be afforded the same legal protections as documents and photos stored in your home or business. While individual data elements of these may appear benign, when combined they can be open for abuse. Search warrants based on probable cause need to be required before a service provider can be compelled to disclose a user's or businesses private communication or online documents.

3. How do we ensure that our laws give the public and private sectors the tools they need to respond to the botnet threat, while at the same time recognizing that the threat itself – and therefore the most effective responses to it – are constantly evolving?

Updating ECPA and the CFAA and modernizing the MLAT process will help to create a legal environment that will allow the public and private sectors to work cooperatively to respond to botnets and related threats. Congress needs to help create incentives and remove barriers to information sharing while assuring privacy protections. Threat intelligence often contains personally identifiable information (PII), underscoring the importance that privacy be the foundation of all fraud prevention and data sharing practices. These privacy concerns can be easily addressed. When data is collected and used exclusively for threat detection, entities should be afforded "safe-harbor", providing that the data shared is not used or retained for any other purpose. Conversely, industry needs assurances that law enforcement will not use such data for purposes other than fighting cybercrime and to facilitate data sharing back to the private sector.

In summary, the public and private sector have a shared responsibility, including raising public awareness of the threats and promoting the adoption of best practices, standards and self-regulatory programs. With the right balance we can enhance online trust and confidence while promoting innovation. The Online Trust Alliance looks forward to working with the committee to develop balanced legislation, while promoting security and privacy enhancing best practices.

Sincerely,



Craig D. Spiegle
Executive Director and President
Online Trust Alliance
Craigs@otalliance.org
+1 425-455-7400