

**Questions for the Record**  
**“Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle  
Cybercriminal Networks”**  
**July 15, 2014**  
**Senator Sheldon Whitehouse**

**Cheri McGuire:**

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?

*Streamlining and modernizing the Mutual Legal Assistance Treaties (MLATs) would have an immediate impact on law enforcement’s ability to share information, investigate and prosecute cybercriminals. While the MLAT system today provides an internationally recognized and well understood legal framework, it was first developed in the 1800s – and takes far too long to address the real-time nature of cybercrime. To keep pace with 21st Century threats, the MLAT process should be overhauled, streamlined and properly funded. In addition, the Computer Fraud and Abuse Act (CFAA) should be amended to clarify that trafficking in access to botnets is a criminal offense. Today, a criminal can sell, or even rent, access to a botnet to steal personal or financial information or conduct DDOS attacks and not be in violation of the CFAA. The CFAA should be amended to include trafficking in access to botnets.*

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

*I agree with Assistant Attorney General Caldwell that many of the laws that now govern cybercrime need updating, and that the Computer Fraud and Abuse Act (CFAA) and the Electronic Communications Privacy Act (ECPA) need to be updated to reflect modern technology. Specifically, communications and storage technology such as email, cloud, and social networking, should be afforded the same legal protections as documents stored on a hard drive or letters filed in a drawer and secured in your home. The government should obtain a search warrant based on probable cause before it can compel a service provider to disclose a user’s private communications or documents stored online. With that*

*said, any update must be done with care to ensure that the statutes are flexible enough that they can adapt as new technologies emerge.*

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?

*As I noted above, 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. Information sharing legislation – crafted in a way that both facilitates sharing and that protects privacy – is also essential. Congress can also play an important role in raising public awareness about the continually evolving threat of botnets and cybercrime – as you have done with your hearings. Finally, it is important that Congress continue to engage with the private sector so that together we can all ensure that any new laws do not hamstring innovation and succeed in promoting privacy protections and supporting international cooperation and standards.*