Hearing before the Senate Committee on the Judiciary
"Cyber Crime: Modernizing our Legal Framework for the Information Age"
Questions for the Record Submitted by Senator Al Franken

The Computer Fraud and Abuse Act (CFAA) – with its various penalties – is aimed, in part, at deterring cyber-crime. According to your testimony, the threat of punishment works to deter legitimate security researchers.

Do you think it has the same effect on real cyber-criminals, including those overseas? If not, where do you think the government ought to be focused if our goal is preventing cyber-crime?

Thank you for your question Senator Franken.

In order for penalties to deter crime, criminals need to believe they will be caught[1]. Cybercriminals often don't believe they will get caught, particularly those operating in countries such as China and Russia. So no, I do not believe the threat of punishment deters real cyber-criminals nearly as much as it chills legitimate researchers working to make us safer.

If this is in doubt, we need only look at the booming cybercrime economy and increasing number of attackers. Understanding the elements driving this is a good place to start thinking about prevention:

- Opportunities for cybercriminals abound as our reliance on "connected" technologies increases. The complexity of these technologies provides the opportunity for attacks, while the connectedness enables foreign actors to reach us remotely.
- Attackers are strongly incentivized as it is easy to monetize them through crypto currencies and thriving black markets.
- There are almost no barriers to entry as people share so much information about themselves on the internet, making them easy targets and convenient entry points for attacks on organizations. For more advanced technical requirements, there is a thriving market of hacker-for-hire tools and services.
- These factors provide even stronger incentives in countries with high unemployment/low incomes and wide availability of technical infrastructure (e.g. China and Russia)

To prevent cybercrime in this context, we must address the factors above. The most pragmatic approach is to try to reduce the number of opportunities, and raise the barriers to entry for attackers. To do this requires a combination of measures:

- We must identify and mitigate the bugs in technological systems that create opportunities for attackers. This is where security research plays a critical role, so it is essential that we support research efforts and not chill them legislatively or prosecutorially.
- We must encourage organizations to adopt basic security hygiene and best practices, such as deploying the latest patches; avoiding technologies with a poor security track record; regularly testing for the effectiveness of defenses, optimal configurations of technology, and the likely impact of an attack; using strong encryption standards and not storing non-essential data; etc.
- We must build greater awareness of security threats and best practices for avoiding them amongst consumers and organizations. All internet users should know how to spot phishing attacks, and protect their credentials appropriately.

I would be happy to discuss this in further detail, and again, thank you for the question.

[1] "Deterrence in Criminal Justice," The Sentencing Project, 2010: http://www.sentencingproject.org/doc/Deterrence%20Briefing%20.pdf