# How to Disclose or Sell an Exploit Without Getting in Trouble

Jim Denaro

@CipherLaw

**This presentation is not legal advice about your specific situation.**

"If I were your lawyer, I'd advise you not to answer that tweet."

# What are we talking about?

# “Techniques”

Information relating to both exploits and vulnerabilities that enable another party to obtain unauthorized access to a computer, deny access by others to a computer, or cause permanent or temporary damage to a computer or a network.

Risks in Publishing or Selling

# Conspiracy

to violate the CFAA

# Risks in Publishing or Selling

- Providing material support to terrorists
- Aiding and abetting
- Cryptography export/arms controls
- Treason
- Espionage Act

# Regulatory Outlook Trends

- In the US
- In Europe
- Globally

# Practical Countermeasures

- Create Dual-Use “Tools”.

# Practical Countermeasures

- Know your reader / buyer.
- Do not direct technique information to someone you suspect is likely to use it illegally.

# Practical Countermeasures

- Be aware of any pre-existing relationships with possible targets of the technique.

# Practical Countermeasures

- Avoid unintentionally creating knowledge and intent.

# Practical Countermeasures

- Be careful in providing “support”.

# Practical Countermeasures

- Use disclaimers

"Compliance with Law. Customer acknowledges that the Software can be configured by the user to obtain access to information using penetration techniques that may cause disruption in systems or services and may cause data corruption. Denial of Service attacks may be run on command that will attempt to render systems and services unavailable to authorized users. Customer specifically agrees that the Software will only be used to target devices under the authorized control of the Customer and in a way in which damage to systems or loss of access or loss of data will create no liability for [company] or any third party. Customer further agrees to strictly comply with all federal, state and local laws and regulations governing the use of network scanners, vulnerability assessment software products, hacking tools, encryption devices, and related software in all jurisdictions in which systems are scanned or scanning is controlled."

"You also agree that you will not use these products for any purposes prohibited by United States law, including, without limitation, the development, design, manufacture or production of nuclear, missiles, or chemical or biological weapons."