

# Legal Risks of Vulnerability Disclosure



Jennifer Stisa Granick, Esq.  
Stanford Law School  
Center for Internet & Society  
[jennifer@law.stanford.edu](mailto:jennifer@law.stanford.edu)  
650-724-0014

# Security Publication

Dual Nature:

The same information that allows more widespread exploitation of vulnerabilities is required to correct those vulnerabilities.

# Security Publication: Pros

- Public Awareness of Security Risks
- Enables SysOp Remediation
- Motivation for Vendor to Code for Security, Patch
- White Hats Know What Black Hats Know:  
No Security Through Obscurity

# Security Publication: Cons

- Public Relations Nightmare
- Over/Understates Seriousness of Problem
- Window of Opportunity Before Patch
- Script Kiddies: Greatly Increases Potential Attackers

# Security Publication: Issues

- Security Through Obscurity vs. Script Kiddies
- Timing of Disclosure
- What to Disclose
- Information in what format
- To Whom

# Theories of Legal Liability

- Negligence: Duty Not to Publish
- Conspiracy: Agreement
- Aiding and Abetting: Intent that Breach Occur
- Wire Fraud: Intent to Defraud

# Theories of Legal Liability Part 2

- WIPO Treaty
- U.S.: Digital Millennium Copyright Act 17  
U.S.C. 1201
- E.U.: Intellectual Property Enforcement  
Directive
- Council of Europe Convention on  
CyberCrime

# Art. 11, WIPO Copyright Treaty

- Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.
- 42 Signatories



# Art. 18, WIPO Performances and Phonograms Treaty

- Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by performers or producers of phonograms in connection with the exercise of their rights under this Treaty and that restrict acts, in respect of their performances or phonograms, which are not authorized by the performers or the producers of phonograms concerned or permitted by law.
- 42 Signatories

# U.S.: DMCA

- Prohibits Circumvention of Technological Measure that Effectively Controls Access to a Copyrighted Work
- Prohibits Manufacturing and Distribution of Any Technology (Tools)
  - Primarily Designed for the Purpose of Circumventing Access Controls
  - Limited Commercially Significant Purpose OR
  - Marketed for Use in Circumvention

# DMCA Cases

- Felten v. RIAA
- Hewlett Packard threat to SNOSoft
- Universal Studios v. Reimerdes/Corley
- United States v. Elcom/Sklyarov
- Lexmark v. Static Control
- Chamberlain v. Skylink
- Mod Chips

# DMCA and Disclosure

- Do disclosures promote security/state of knowledge, or facilitate circumvention?
- Limited exceptions for “professionals” only
- Prohibition of circumvention tools may limit devices used for encryption and security research, and also Fair Use.

# DMCA: Relevant Exceptions

- Security Testing
- Encryption Research
- Reverse Engineering

# Security Testing Exception

- information derived used solely to promote the security of the owner or operator of the tested computer system, or
- information obtained shared directly with the developer of the system
- information obtained not distributed in a way that might enable copyright infringement or other legal violations

# Encryption Research Exception

- Professional Cryptographers
- Seek Advance Permission
- Necessary to Advance the State of Knowledge in the Field
- Publishing Results Does Not Promote Infringement

# Reverse Engineering Exception

- Purpose to Achieve Program-to-program Interoperability
- Reverse Engineering Is Necessary
- Information Divulged for the Sole Purposes of Enabling Program-to-Program Interoperability



# EU: IP Enforcement Directive

- Member States shall provide for appropriate legal protection against the manufacture, import, distribution and use of illegal technical devices.
- “illegal technical device”: any technical device which is designed to circumvent a technical device which permits the manufacture of goods infringing industrial property rights

# COE CyberCrime Treaty

- 34 signatories, including US
- Lists activities that each member must criminalize, including unauthorized access, child pornography, and intellectual property violations (Articles 2-11).
- Grant search and seizure powers to law enforcement, including forcing an ISP to preserve internet usage records and real-time monitoring (Articles 16-22).
- Law enforcement must assist police from other participating countries (Articles 23-35).

# COE CyberCrime Treaty

- Article 6: Illegal Devices: Prohibits computer programs designed or adapted primarily for the purpose of gaining unauthorized access to computers, intercepting data or interfering computer systems.
- Signatories may allow devices if not for the purpose of committing an offense.

# First Amendment

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

# Instructions = Speech

Yes, but not if part of criminal act....

- Sale of bookmaking program
- Mailing PCP instructions
- Enabling tax fraud
- Dangerous sex act
- Trade secret misappropriation

# 1st Am. Protects Vulnerability Tools?

- Software is both Communicative and Functional
- Communicative aspect protected by First Amendment
  - Compelling state interest
  - Least restrictive means
- Communication can be regulated if sufficiently important government interest in regulating the non-communicative or functional aspects

# Normative Questions

- More Harm Than Good from Banning Security Publications?
- Incentive to Release Information in a Manner that Maximizes the Pros and Minimizes the Cons?
- Enforcement Mechanism?
- Who Bears the Costs When the System Doesn't Work?

# Risk Management Questions

- How is tool designed?
- How is information marketed?
- How is information used? Purpose of derivation of information?
- With whom is information shared?



# Risk Management Questions con't

- How is information distributed?
- Who are you?
- Obtain Permission?
- What is the place of the publication in the field of knowledge?

# Legal Risks of Vulnerability Disclosure



Jennifer Stisa Granick, Esq.  
Stanford Law School  
Center for Internet & Society  
[jennifer@law.stanford.edu](mailto:jennifer@law.stanford.edu)  
650-724-0014