Legislating the Internet: ACTA and Beyond

Presentation by Jarad Held
Getting Started: ACTA Background

- ACTA stands for the Anti-Counterfeiting Trade Agreement
- Negotiations began in secret in 2006.
- The Treaty was officially revealed in November 2010.
- The Treaty has already been signed.
ACTA Legalese

1) Section 41 of TRIPS constitutes baseline obligations.
   - Measures to “prevent infringements and remedies which constitute a deterrent…”

2) Limited Safe-Harbor Rules for ISPs, Third-Party liability.
   - Three Strikes/Graduated Response

3) DRM and Anti-Circumvention
   - No Fair-Use/Fair-Dealing exceptions
So what does it all mean?

1) - Inspection of all Network Traffic via Deep-Packet Inspection, DNS-block or similar technology, and a DMCA-style notice-and-takedown

2) - 3 Infringements result in an IP Ban and subscriber removal for up to 1 year.

3) - Non-commercial copying for personal use and storage, library DRM circumvention, creation of circumvention software all banned.
Deep-Packet Inspection

- Standard packet inspection only looks at headers
- Deep packet inspection may look at multiple layers – all the way to the application layer data.

Figure 1: Shallow packet inspection – data from packet headers
Application Detection for DPI

- DPI depends on application signatures – analysis by port, analysis by string match, analysis by numerical properties, and analysis by behavior and heuristics.

Figure 2: Deep Packet Inspection – analysis of encapsulated content over many packets
Analysis by Port and/or String

- By Port: Usually a default port is chosen for an application.
- By String Analysis: Many applications display the application name within the protocol.
Analysis by Numerical Properties

- Numerical properties are analyzed such as length of the payload, the number of packets sent in response to a transaction, and the offset of some fixed value within a packet.
Analysis by Behavior and Heuristics

- Typically different protocols can be differentiated statistically and recognized with patterns.
Defeating DPI

- Encryption – Add encryption to the data to confuse DPI systems.

- Obfuscation – Scrambling communications (examples: BitTorrent, eMule, Skype)
Beyond ACTA

- SOPA and PIPA are dead, and the fight to kill ACTA is still continuing.
- Next Challenger: The Trans-Pacific Partnership – “The agreement exports (nearly verbatim) the DMCA's rules on digital locks, ISP liability, and subscriber disconnections, with a few extra goodies on the side.” - Ars-Technica
Sources and Credits


Sources and Credits (Cont'd.)


- “Anti-Counterfeiting Trade Agreement”, [https://www.eff.org/issues/acta](https://www.eff.org/issues/acta), eff.org, n.d., Web, 6 February 2012

Sources and Credits (Cont'd.)


- Michael Geist, “The ACTA Internet Chapter: Putting the Pieces Together”, http://www.michaelgeist.ca/content/view/4510/125/, michaelgeist.ca, 3 November 2009, Web, 6 February 2012