

PROTECT-IP (COICA)

Various Authors

(October, 2011)

Legislative Intent

- Intellectual property (content, brands) is easily copied and distributed (thus “stolen”) via the Internet
- Entertainment and premium goods industries spend and work hard to create value and protect works
 - For domestic distributors, law enforcement works
 - For off-shore distributors, something else is needed
- PROTECT-IP (was COICA) targets enablers:
 - Advertising and payment networks
 - DNS resolution by domestic ISP networks
 - Search engine results

Easily Circumvented

- Easily circumvented – any well motivated user can switch to an off-shore DNS provider
 - Which has special perils all its own
 - Off-shore telemetry of US citizen Internet activities
 - ...as well as depriving US ISP's of such telemetry
 - ...with added potential of injected malicious responses
 - Noting, these users are well motivated
 - ...and so are the infringing content providers, who can easily provide free plugins to these “customers”

Makes DNSSEC Undeployable

- Stub validation is coming (IETF DANE, etc)
- Lawful intercept responses will be unsigned
- Some unsigned responses will trigger “defense mode” involving retries, alternate servers, VPN, proxies – because this “looks like” poisoning
- Such a “defense mode” would trivially bypass the intent and effect of this legislation – which would be illegal – so vendors won't want to do it
- DNSSEC deployment is in early fragile days

Status

- Legislation
 - US Congress
 - Senate bill passed out of committee, but there's a “hold”
 - House bill about to be introduced, similar in all respects
 - There is similar work elsewhere (UK etc)
- Position
 - We have to keep these industries from externalizing their risk management costs onto the Internet
 - ICANN SSAC has emitted a short statement about this, which was well received by the ICANN GAC