

United States Developments in Tackling Online Child Pornography

TJ McIntyre

Lecturer in Law, UCD

GIKII IV, IViR, University of Amsterdam
17-18 September 2009



UCD School of Law

Summary

- International trend towards filtering as a means of blocking online child pornography
- Many jurisdictions moving towards greater state control of this process (Dutch model); but
- US law moving towards greater private sector involvement in take-down, blocking and detection of child pornography
- Coordinated via the (quasi-public) NCMEC and State AGs; facilitated by Federal legislative changes
- Resulting schemes offer potential for more effective enforcement of the law
 - But have little statutory regulation or oversight
 - Presenting issues of transparency and accountability



Background: Center for Democracy & Technology v. Pappert (2004)

- 2002 Pennsylvania statute authorised AG to apply to judge for an order declaring internet content as child pornography
 - No prior notice to site owner or ISP
 - AG in practice bypassed this safeguard, issuing “notices” directly to ISPs
- ISPs serving Pennsylvania then obliged to block that content
 - ISPs generally used IP filtering; some DNS filtering
 - Significant overblocking resulted

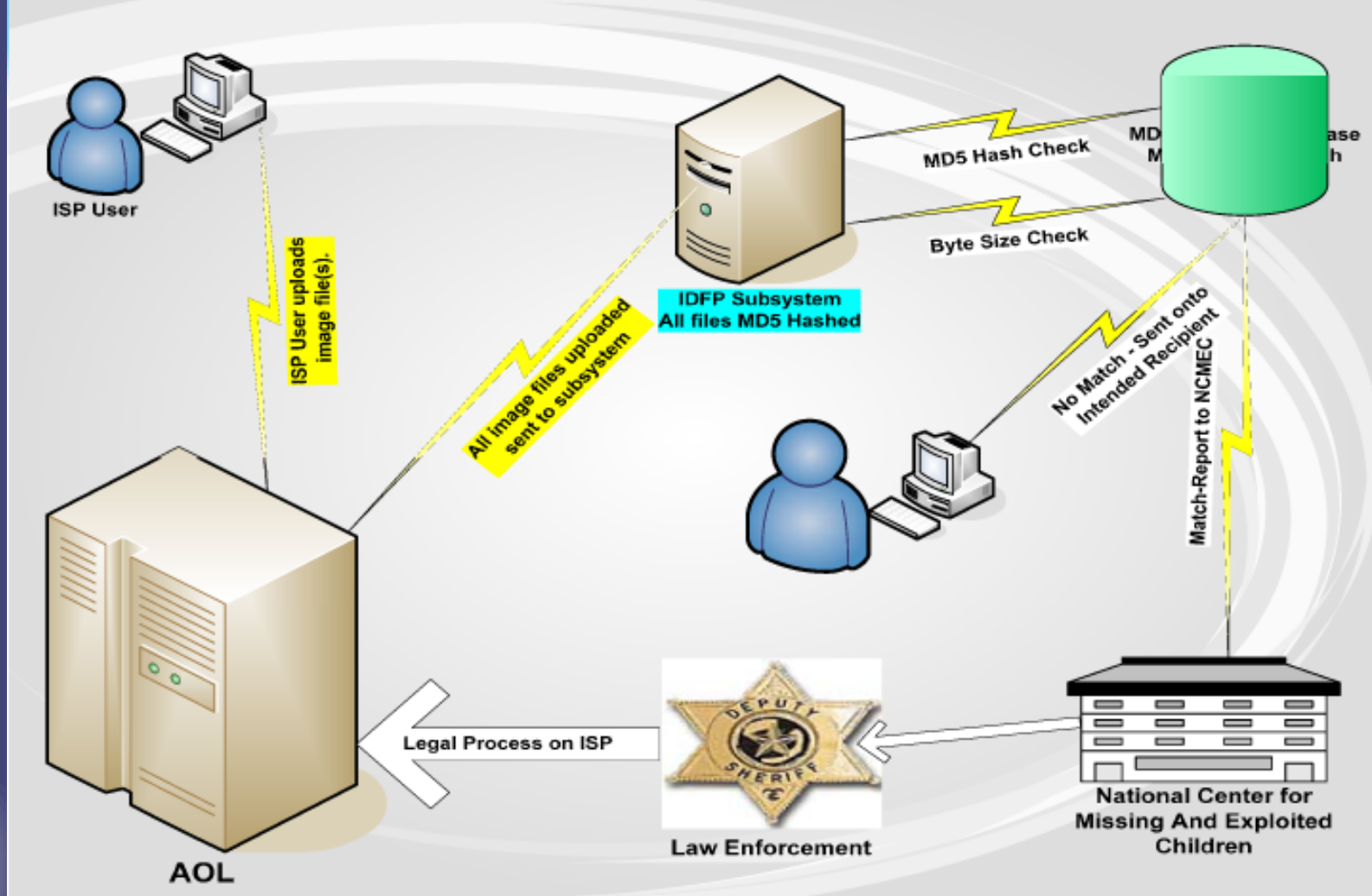


CDT v. Pappert ctd.

- Findings
 - State responsible for ISP overblocking
 - IP/DNS blocking overbroad; URL filtering impractical
 - Blocking orders an unconstitutional prior restraint
 - Informal “notice” system also a prior restraint
 - Coercive in effect; ISPs were not realistically free to ignore them
 - Extraterritorial effect and impact on interstate commerce violated Commerce Clause
- Has this encouraged Congress / NCMEC / State AGs to avoid legislative solutions and rely on “voluntary” blocking?



Image Detection & Filtering Process (IDFP)



Source: Colcolough, "Child Pornography Countermeasures" (presented at the Third World Congress Against Sexual Exploitation of Children and Adolescents, Rio de Janeiro, November 25, 2008)

Example 1: the Image Detection & Filtering Process

- Running since 2004
- Uses hash list developed internally within AOL
 - Based on previous cases of child pornography encountered by AOL
 - Reports only precise (bit by bit) matches with those files
- Inspired by but goes beyond IWF model:
 - Applies to private communications (email), not merely publicly viewable URLs
 - Blocks communications but also provides police reports
- Resulted in numerous convictions
 - E.g. *United States v. Terry* (2008); *Florida v. Woldridge* (2007); *Sisson v. Delaware* (2006) and *US v. Grober* (2008)
 - In some cases, has led to identifying offenders who are engaged in physical abuse also - e.g. *US v. McGarry* (2007)

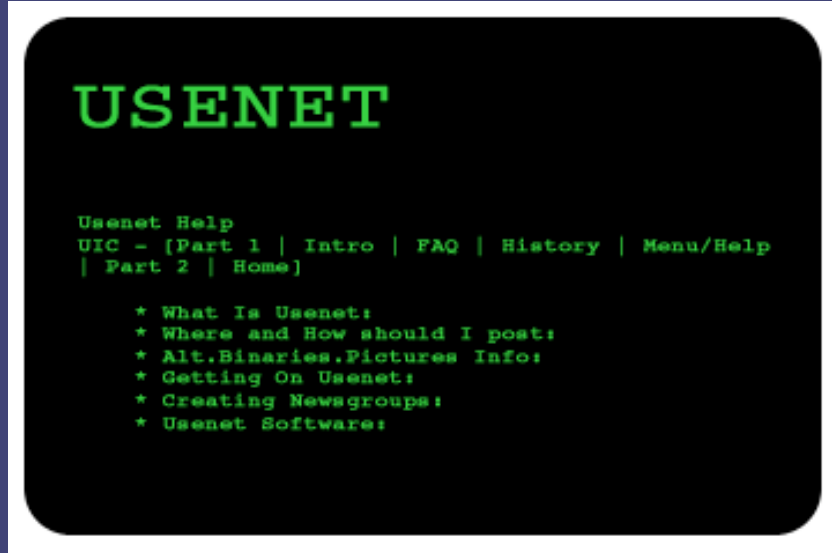


Example 2: The NCMEC URL Project

- Agreed in 2008 between NCMEC, individual ISPs and 45 State AGs
- NCMEC provides list of URLs to ISPs to enable them to takedown or block material
 - Limited to “the worst of the worst” – “sexually explicit images of pre-pubescent children”
 - ISPs covering 87% of market have subscribed
 - Majority of ISPs appear to be doing takedown only
 - Some (e.g. Qwest) appear to be blocking also
- Procedural issues:
 - Site owners not notified
 - No appeal mechanism
 - ISPs agree not to state on block/takedown page that NCMEC was involved in decision



Example 3: NY AG v. Usenet



Prosecution threats

- AG launches "sting" operation against NY ISPs
 - Agents pose as subscribers, complain that child pornography is available on Usenet via their servers
- ISPs fail to enforce terms of use prohibiting this
- AG threatens charges of fraud and deceptive business practices
- Avoiding the protections of s.230 CDA?

Consumer pressure

- AG launches website to "name and shame" and pressure ISPs which don't sign up to voluntary Code of Conduct



Example 3: NY AG v. Usenet ctd.

- Majority of providers operating in NY agree to sign up
 - Verizon, Time Warner Cable, Sprint pay \$1.125 million to AG / NCMEC
- AG's complaints focused on 88 newsgroups
 - Some ISPs cease to host entire alt.* hierarchy
 - Some (Verizon, Time Warner Cable) cease to host Usenet entirely
 - Complaints that legitimate content will be suppressed
- AG subsequently (2008) forwards materials to ISPs suggesting that they deploy deep packet inspection on all connections to detect and report child pornography



Role of NCMEC

- Formally private, non-profit
 - Established by Congress in 1984
 - Approx. 68% of revenue from Federal Funds (2007 Annual Report)
 - Designated by law for mandatory reporting of child pornography by ISPs (18 U.S.C. §2258A)
 - May forward details of child pornography (URLs, hash values) to ISPs for them to stop transmission on their networks (18 U.S.C. §2258C)
 - Central repository for child pornography information and prosecution
 - Numerous officers from FBI & other agencies on secondment to NCMEC
 - Designated Central Authority for US under Hague Convention on Child Abduction
- Should it be treated as a Federal Agency? Brought within FOIA? Have decisions subject to appeal?



Legal status of the IDFP

- Almost entirely unchallenged; no analysis by legal authors. Why?
 - Fourth Amendment exclusionary rule only applies to state agents
 - Vigilante hacker line of cases
 - No suppression remedy for Wiretap Act breaches
- *US v. Richardson* (2008)
 - Defendant claimed AOL should be treated as a state agent
 - Held: failed to meet burden of proof; not entitled to subpoena AOL to find material supporting claim



Broader questions re the IDFP

- Is the use of hash values by state agents a “search” under the Fourth Amendment?
 - *United States v. Place* (1983) – A sniff by a police dog is not a “search”. It reveals only the presence or absence of contraband and is *sui generis*.
 - *United States v. Crist* (2009) (Use of EnCase to compare hash values of files with known child pornography held to be a “search”.)
- Is the use of hash values by private agents an illegal “interception” under the Wiretap Act / Electronic Communications Privacy Act?
 - Notoriously confusing statutory language
 - Is there “an acquisition of the contents of” the communication?
 - Does the provider “protection of rights and property” exception apply?
 - Would the “consent” exception apply?



Some observations and questions

- Common move towards deployment of filtering
- Differences
 - EU jurisdictions move from “voluntary” blocking towards legally mandated blocking (e.g. UK; Germany; Proposed Framework Decision); US moving in the opposite direction
 - US systems moving beyond the “last millennium” model of web-based material? Hash values can easily be used on e.g. email, p2p or IM systems
 - Piggybacking on e.g. “copysense” music filtering software?
 - European systems generally using blocking functionality only; US systems also used / proposed to be used as an intelligence gathering tool
 - Can ISPs resist demands to provide evidence on attempted downloads
- Which model (US or EU) is preferable? On what metric?



Thank you

Questions or comments?

tjmcintyre@ucd.ie

Blog: www.tjmcintyre.com



UCD School of Law