Die Politik von Deep Packet Inspection

Ralf Bendrath
r.bendrath@tudelft.nl
bendrath.blogspot.com

Vorwort: Das gute alte Internet

"Like a daydreaming postal worker,
the network simply moves the data
and leaves interpretation of the data
to the applications at either end.
This minimalism in design is intentional.
It reflects both
a political decision about disabling control
and a technological decision about
the optimal network design."

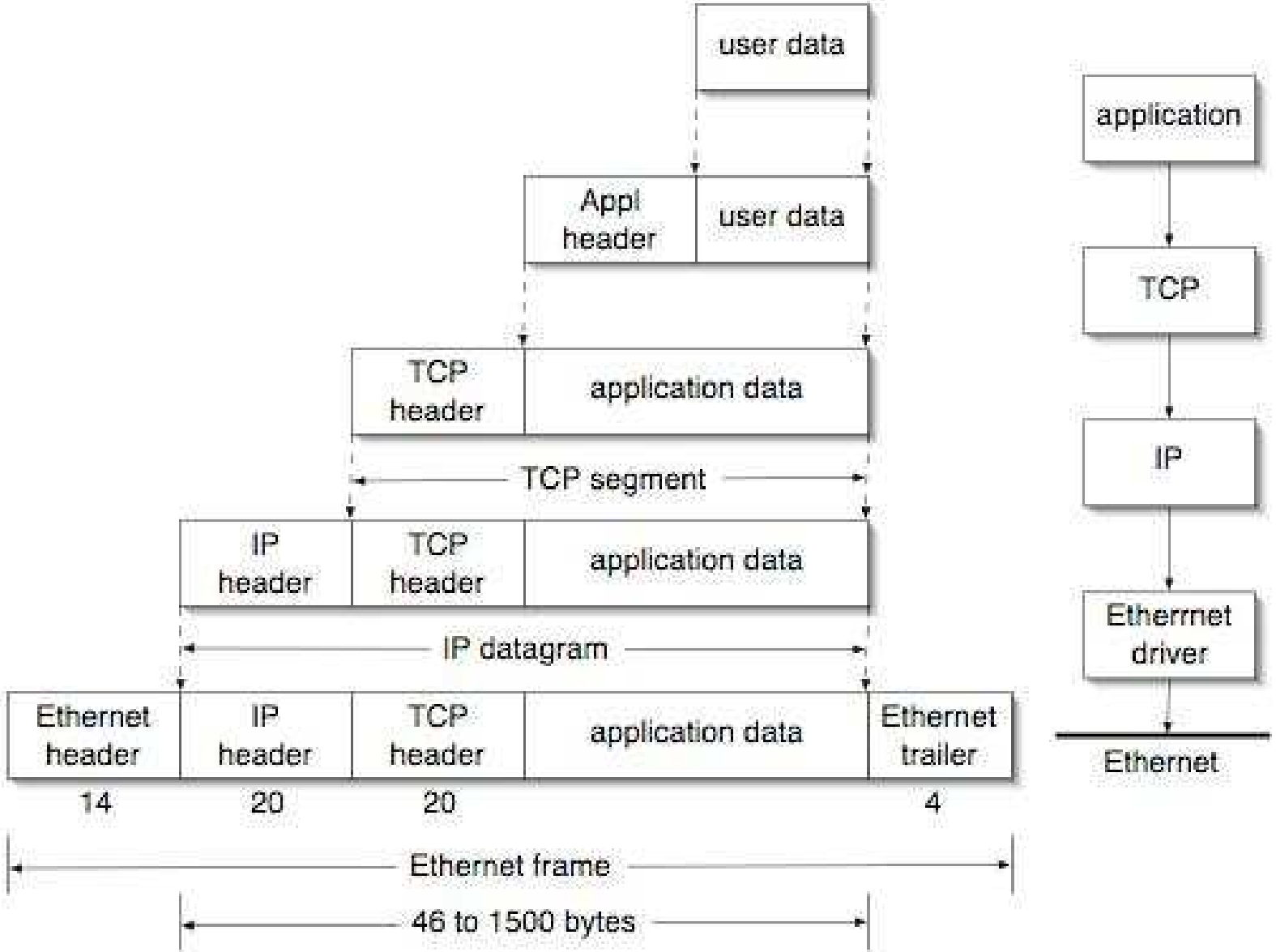
(Lawrence Lessig: Code and other Laws of Cyberspace,
New York: Basic Books 1999, p. 32)

Deep Packet Inspection könnte das ändern

Inhalt

I. Was ist DPI?
II. Was bedeutet das?
III. Probleme mit DPI
IV. Fallstudien-Beispiele
V. Fazit

I. Was ist DPI?


user data
Appl header
user data
TCP header
application data
TCP segment
IP header
TCP header
application data
IP datagram
Ethernet header
IP header
TCP header
application data
Ethernet trailer
14
20
20
4
Ethernet frame
46 to 1500 bytes
application
TCP
IP
Ethernet driver
Ethernet

Spezialisierte Hardware

- inspiziert den Inhalt (application data) von TCP-Paketen
- FPGA und CPLD
- bis zu 80 GBps
- Diskriminierung der Pakete
  - umleiten
  - kopieren
  - verwerfen
  - verlangsamen

Traffic Acquisition and Analysis Overview

Resilient Layer 3 Policy Based Forwarding Engine

- Implements policies that selectively redirect or drop IPv4 packets to specific egress ports through Policy-based Routing (PBR) without impacting performance
- Rich and flexible policies permit any IPv4 traffic to be classified including voice calls, FTP transfers, SMTP transactions, peer-to-peer messages or any type of IP conversation

- Specific bi-directional conversations can be redirected and load balanced to different servers
- Packets are redirected unmodified, the original frame, MAC and IP headers, TTL, payload and checksums are preserved

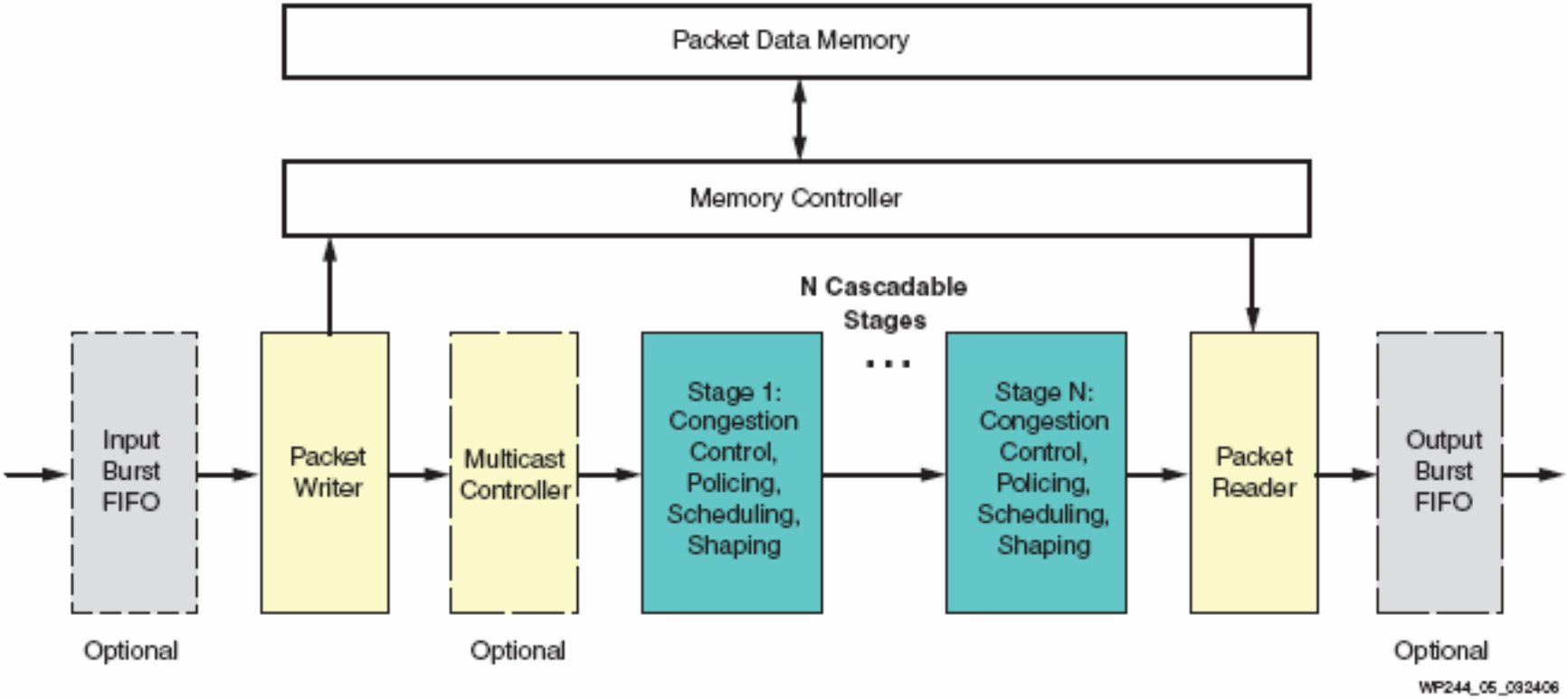


Figure 5: **Xilinx Traffic Manager**

Woher kommt DPI?

- verfügbar seit ca. 10 Jahren Jahren
- ca. 30 Hersteller
  - überwiegend US-Startups
  - teilweise auch aus Israel und Deutschland
- Spezialisierte Geräte
  - IDS, Network Management, Filter, Abhören…
- Konvergiert mit Routern und Switchen
  - „Layer 7 switches“, „policy-based routing“, …
- Konvergiert mit Kunden-Management
  - Abrechnungssysteme, Traffic-Caps, …

II. Was bedeutet das?

Technologie der sozialen Kontrolle?

- Lawrence Lessig nochmal:

  “a political decision about *disabling control* and a technological decision about the *optimal network design*”
- DPI
  - integriert / ersetzt alte Kontroll-Technologien
  - wird (von einigen!) als optimal für neues Netz-Design angesehen
  - verspricht außerdem neue Geschäftsmodelle

Political Control

Zweck	Alt	Neu	Antriebskräfte
Abhören und Überwachen	TCPdump, Snort, etc. (asynchron)	DPI (synchron)	Polizei, Geheimdienste
Filtern / Zensur	Sperren auf Basis der Quelle (DNS / IP-Adresse)	Sperren auf Basis des Inhalts	“Child-Porn”, “Jugendschutz”, “Terrorismus” und ähnliches
Bekämpfung von Raubkopien	DRM, Wasserzeichen (Endpoints)	Filtern auf Basis von Hashes und Signaturen (Traffic)	Content-Industrie

Network Design

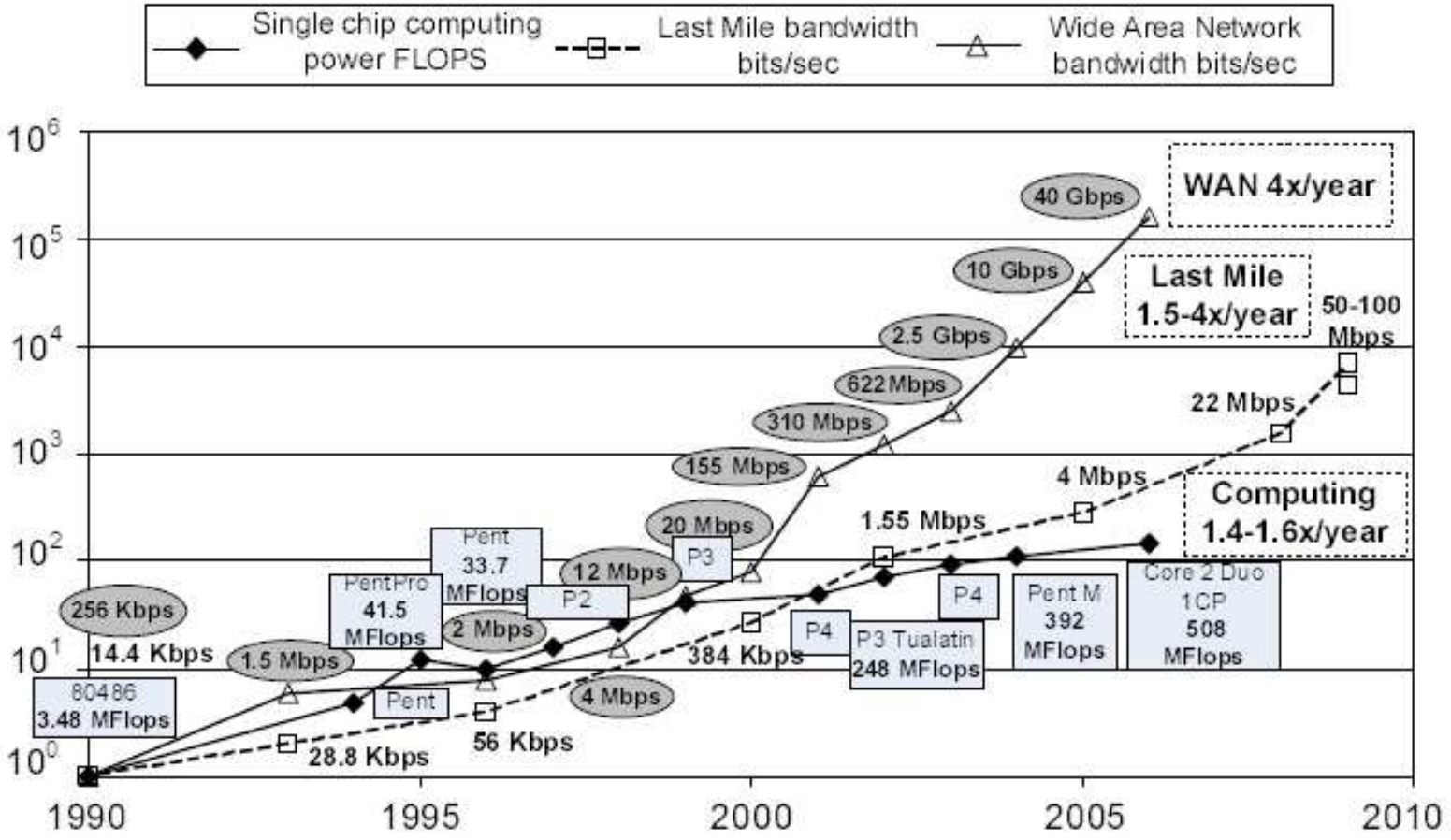
Ziel	**Alt**	**Neu**	**Antriebskräfte**
Bandbreiten-Management	TCP congestion management, QoS	„application-based routing“	Engpass letzte Meile, P2P, …
Subscriber-Management	pay per minute, pay per volume	differenzierte Services und Preise	heterogenes Nutzer-Verhalten
Netzwerk-Sicherheit	stateful Firewalls	stateless Firewalls	Web Services, Cloud Computing

Business Models

Ziel	**Alt**	**Neu**	**Antriebskräfte**
vertikale Integration I (Inhalte)	Koppel-Geschäfte	Abbremsen des Konkurrenz-Traffics	Video on Demand etc.
vertikale Integration II (Telco-Services)	Koppel-Geschäfte	Abbremsen des Konkurrenz-Traffics	Konkurrenz durch Skype etc.
verhaltens-basierte Werbung	Cookies (Websiten-Betreiber)	Ad Injection (ISPs)	geringe Profit-Margen bei ISPs

III. Probleme mit DPI

Technische Grenzen


Single chip computing power FLOPS
Last Mile bandwidth bits/sec
Wide Area Network bandwidth bits/sec
10^6
10^5
10^4
10^3
10^2
10^1
10^0
1990
1995
2000
2005
2010
WAN 4x/year
Last Mile 1.5-4x/year
Computing 1.4-1.6x/year
40 Gbps
10 Gbps
2.5 Gbps
622Mbps
310 Mbps
155 Mbps
20 Mbps
12 Mbps
2 Mbps
1.5 Mbps
256 Kbps
14.4 Kbps
4 Mbps
56 Kbps
28.8 Kbps
384 Kbps
1.55 Mbps
4 Mbps
22 Mbps
50-100 Mbps
80486 3.48 MFlops
Pent
Pent 33.7 MFlops
PentPro 41.5 MFlops
P2
P3
P3 Tualatin 248 MFlops
P4
P4
Pent M 392 MFlops
Core 2 Duo 1CP 508 MFlops

Technische Faktoren

- Bandbreite
- Rechnerleistung
- Anzahl der Regeln

→ DPI (derzeit) nur machbar

  – bei begrenzter Bandbreite

  – mit begrenzter Anzahl von Regeln

Verschlüsselung

- Transportation Layer Security
- Application Layer: end-to-end encryption
- Verbreitung?

→nur Typen von Traffic erkennbar, nicht mehr einzelner Inhalt

Content / Mustererkennung

- Begrenzte Fähigkeiten
- Nur bei festen Bit-Folgen (Viren etc.)
- Re-Codieren verhindert Treffer bei Audio und Video
- Fair Use, legitimer Traffic etc.?
  - rechtliche Beurteilungen sind Layer 8!

Wirtschaftliche Aspekte

Vertikale Diskriminierung

- Inhalte
  - Kontrolle von Video on Demand etc.
  - verzerrt Markt für Inhalteanbieter
- Telco-Services
  - Kontrolle von VoIP etc.
  - verzerrt Markt für Kommunikationsanbieter
- Kontrolle des Transport-Layer

  → lokales Monopol?

Investitionen oder Kostensenkung?

- Investitionsentscheidungen
  - Kundenüberwachung oder mehr Bandbreite?
- Kunden haben sich an Flatrates gewöhnt
- Anwendungs-basierte Tarife nicht angemessen fürs Internet
- Ad Injection = Kunden-Überwachung

Politische und rechtliche Aspekte

Datenschutz

- Telekommunikationsgeheimnis
- Nutzererwartungen
- Vgl. Straßenverkehr!
- DPI mag gegen Malware / Spam ok sein
- ISP-Haftung?
  - „mere conduit“ gilt nicht mehr

Filtern / Zensur

→ siehe Vortrag und Workshop von Scusi

- Rezipientenfreiheit
- Slippery slope?
- Content-Industrie hat ihre eigene Agenda
- Kinder- und Jugendschutz?
- bisher: Filtersysteme auf DNS- oder IP-Basis, DPI noch (?) nicht

Netzneutralität

- Grundlage des Internet bisher
- „Intelligence is at the edges“
- Unabhängigkeit der Protokoll-Schichten
- Ist ein „intelligentes Netz“ weiterhin offen für Innovation oder zu spezialisiert auf heutige Probleme?

IV. Fallstudien

Kontext

- Internet Governance
- Forschungsbedarf
- Internet-Governance-Forschung hat bisher Kernressourcen (ICANN etc.) oder Endgeräte / User-Verhalten erforscht.
- Wenig zur Rolle von ISPs dabei.

Varianz

- Nicht alle Optionen von DPI werden überall genutzt.
- DPI ist ein Fall von technischem Wandel, der derzeit politisch ausgehandelt wird.
- ISPs haben mit DPI neue Hebel in der Hand.
- Wie nutzen sie die in welchem Umfeld?
- Welche Rolle haben dabei politische Regeln und Institutionen?

Fall 1: Bandbreiten-Management

- Varianz der Interessen:
  - Kabel und Mobil: fair share among users
  - DSL: Bandbreite gesamt / over-subscription
- P2P-Blockaden / -Bremsen
  - Transparenz durch User (Azureuswiki etc.)
- Marktmechanismen?
  - nur bei Wettbewerb (EU, nicht US)
  - Comcast (US): RST packet injection
  - Rogers (CA): Bittorrent geblockt

Fall 1: Bandbreiten-Management

- US: Beschwerden bei der FCC
  - EFF, Public Knowledge, Vuze
- FCC broadband principles 2005
  - „*consumers are entitled to run applications and use services of their choice (…)*“
- FCC Entscheidung, August 2008
  - Comcast muss das stoppen, full disclosure
  - hängt noch vor Gericht (9th DC Circuit)
- Trend derzeit: Volumentarife

Fall 1: Bandbreiten-Management

- CA: Beschwerden beim Federal Privacy Commissioner
  - CIPPIC
- Hearing der Telko-Regulierungsbehörde
- Privacy Commissioner macht ganzen Sammelband dazu
- Verfahren noch nicht abgeschlossen
- „Privacy“ statt „Net Neutrality“

Fall 2: Ad Injection

- Genereller Trend: behavioural advertizing
- DPI-basiert:
  - Phorm (UK)
  - NebuAd, AdZilla et al. (US)
- massive Kritik von NGOs
  - FIPR (UK)
  - Free Press / Public Knowledge (US)

Fall 2: Ad Injection

- US: DPI so gut wie tot
  - Charter Communications: AGB-Änderung
  - Abgeordnete, Staatsanwälte: „lasst das“
  - Charter zieht zurück
  - NebuAd stellt Geschäftsbereich ein
- UK: DPI lebt weiterhin
  - Information Commissioner: „ist ok mit opt-in“
  - Polizei weigert sich zunächst, zu ermitteln
  - jetzt ist die EU-Kommission aktiv

Fall 3: Copyright Filtering

- Audible Magic als Filter-“Lösung“
  - bereits von ~ 75 US-Universitäten benutzt
- Belgien: Musikindustrie verklagt ISPs auf Installation, gewinnt (Juni 2007)
- Irland: selbe Klage eingereicht (2008)
- Ooops…
- Belgisches Berufungsgericht (Okt. 2008)
  - „Audible Magic funktioniert nicht“
  - Reaktion in Irland: außergerichtliche Einigung

Weitere Fälle

- Netzwerk-Sicherheit
  - nicht verregelt, nicht umstritten
- NSA-Abhörskandal
  - Illegal, aber post-hoc-Immunität
- „Illegal Content“-Filter
  - KiPo etc. (noch) nicht mit DPI
  - Great Firewall of China etc.???

V. Fazit

Interessen der ISPs entscheidend

- ISPs haben zentrale Stellung
  - Wenn sie etwas wollen, können sie es (erstmal) tun
  - Wenn andere etwas wollen, müssen sie die ISPs zwingen oder überzeugen

→DPI-Use-Cases strukturieren die Interessenlage und Akteurskonstellation

Institutionen & Regeln entscheidend

- ISPs können nicht alles einfach tun
  - DPI-Verhinderung möglich durch Gesetze und andere Akteure
  - Bsp. Ad Injection / Bandwidth-Management
- ISPs können aber viel verhindern
  - DPI-Erzwingung schwierig, wenn sie nicht wollen
  - Bsp. Copyright und NSA

Ausblick

- DPI ist Basis-Technologie
  - Wenn auf einer Schiene eingeführt, dann weitere Anwendungen einfacher.
  - „Censorship is just another policy rule“
- Netz-Neutralität, Privacy herausgefordert
- legitime Use-Cases, aber Regeln nötig
- „DPI Bill“ oder Einzelregelungen?
- Interdisziplinäre Konferenz im Gespräch

Danke für‘s Zuhören!

Feedback, Ideen, Hinweise,
Whistleblowing, …

sehr gerne an r.bendrath@tudelft.nl