Deep Packet Inspection, Public Pressure and Regulatory Actions

Comparative Cases on Online Copyright Enforcement and Behavioral Targeted Advertising

Andreas Kuehn, Milton Mueller
School of Information Studies, Syracuse University
www.deeppacket.info

Talk @ HIIG, Berlin, Oct 24, 2012

DPI – a current issue in Germany

DIGITALE GESELLSCHAFT

DPI

oder

Warum wir in unseren Paketen nicht gerne herumschnüffeln lassen.

Flyer der Digitale Gesellschaft e.V. zum Thema DPI, Oktober 2012.
Source: https://digitalegesellschaft.de/wp-content/uploads/2012/10/dg_dpi_FINAL1.pdf

DPI – a current issue in Germany

Stellen Sie sich vor, die Post öffnet alle Ihre Briefe und liest den Inhalt. Manche schreibt sie um – und andere schmeißt sie einfach weg. Das klingt absurd?

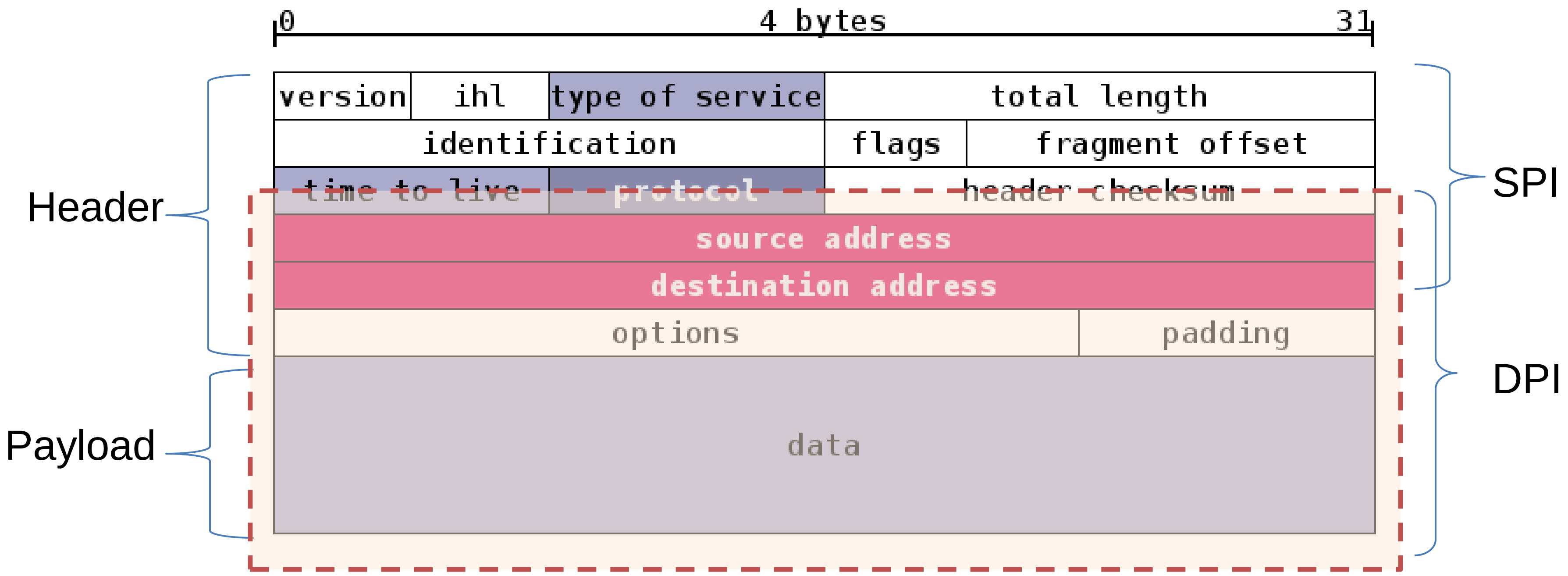
Genau das passiert mit Ihren Daten im Internet

Flyer der Digitale Gesellschaft e.V. zum Thema DPI, Oktober 2012.

Overview

- Introduction
  - What is DPI?
  - DPI Capabilities and Applications
- Cases: Online Copyright Enforcement
- Cases: Online Behavioral Advertising
  - Proposed 4-Stage Disclosure Pattern
- Conclusion
- Q&A

Deep Packet Inspection



Deep Packet Inspection

Key Features

- DPI pertains to *information in motion*, not information at rest.

Technical Capabilities

- Recognition
- Manipulation
- Notification

Applications and Deployments

- Using these three basic capabilities, vendors and network operators build DPI applications.
- The list of DPI use cases is long and the lines between them are blurry.

DPI as “Disruptive Technology”

- **Tension or conflict with three fundamental principles of Internet governance:**
  - The end to end argument (a.k.a. net neutrality)
  - Intermediary immunity
  - Expectations of privacy

General Research Question

- **Is the disruptive potential of DPI being realized?**
    - Will DPI transform Internet governance, or will Internet regulation “tame” or control DPI capabilities to keep them consistent with prior norms?

Six Generic DPI Applications

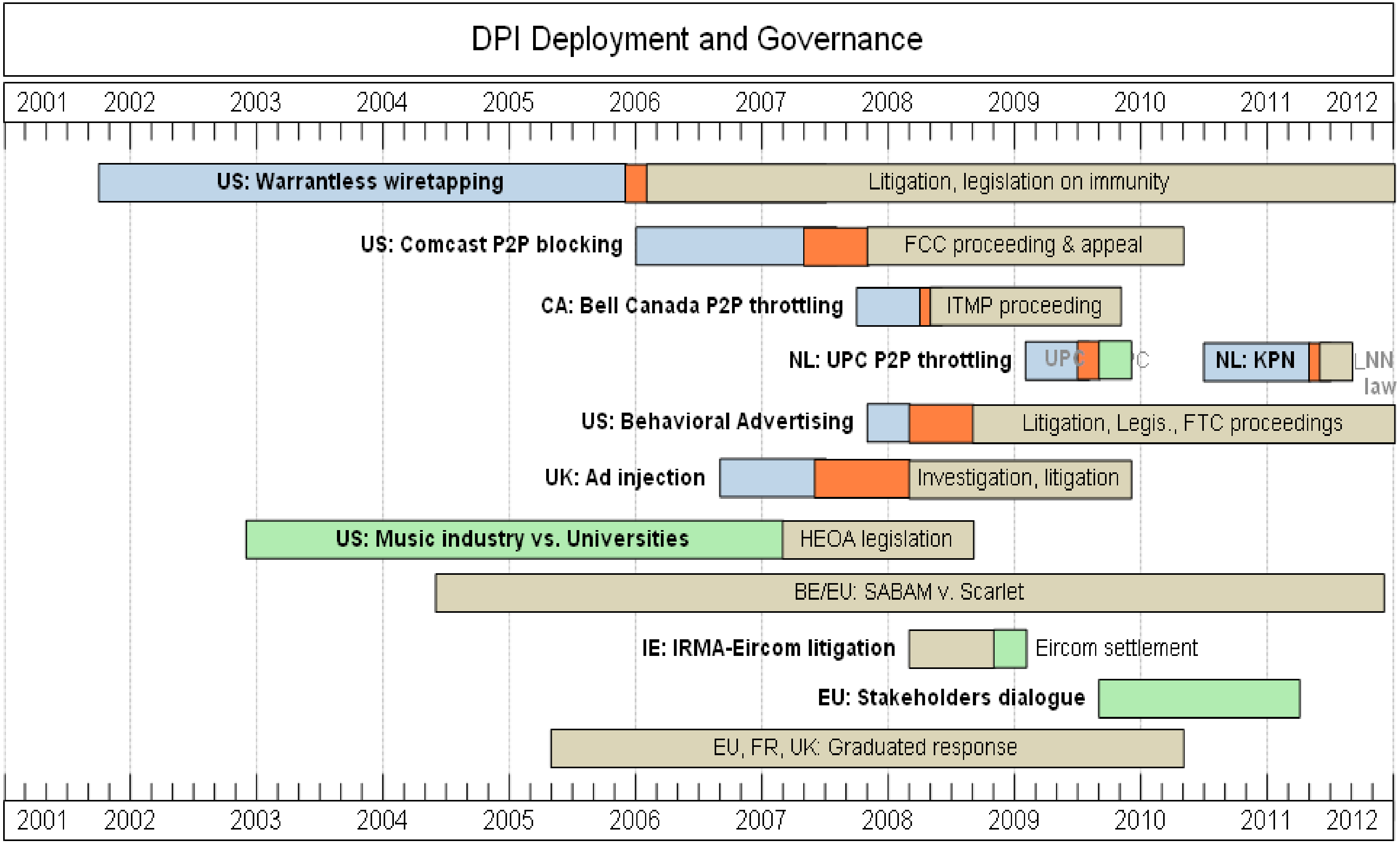
- Network security
  - Intrusion detection and prevention
- Bandwidth management
  - “Throttling,” traffic shaping
  - Enforcement of bandwidth caps
- Customer profiling
  - Ad injection and targeted ads
- Copyright protection
  - Detection and blocking of file sharing
- Censorship
  - Prohibited content recognition and blocking
- National security surveillance

Case Studies: Variation Across Cases and Institutional Settings

	Bandwidth management	Behavioral targeting, ad injection	Filtering illegal content	Filtering copyrighted content
US	Comcast BitTorrent FCC ruling	NebuAd		Universities, negotiated ISP deals
CA	CRTC proceeding on “ITMPs”			
EU		Phorm	Germany (?)	EU-level debate on “technical measures”
CN	China Telecom		Chinese MII	China Telecom, Licensed ISPs
IR			DPI to block, surveillance	

Public Pressure and Regulatory Actions in DPI Deployments

- Observed public pressure across different DPI deployments; DPI in conflict with established norms.
- Consequently, DPI emerges as a hot topic in the policy arena - it becomes *political* (…but what about other techniques?)
- Role of ISPs as a decisive element?
  - ISPs’ role in online copyright enforcement
  - ISPs’ role in online behavioral advertising
- Observable, recurring patterns?



🟧 Public exposure 🟦 Secret deployment ▨ Public ordering 🟩 Private negotiation

Mueller & Kuehn, 2012
www.deeppacket.info

Comparative Cases: Europe and U.S.

ONLINE COPYRIGHT ENFORCEMENT

Online Copyright Enforcement

- Network monitoring and surveillance
- Prevalence of online piracy ask rights holders to take action
  - Legal actions: civil law suits against individual users as well as service providers
  - Technical actions: content filtering based on technical measures
  - Educational actions: graduated response
- Technical measures (DPI) as a prerequisite for effective graduated response (…)

Copyright Enforcement Cases

Europe / European Union

- *Graduated Response*
- Several public consultations and reviews of existing directives with focus on IPR. Multiple Member States implement graduated response.

U.S.

- *Higher Education Institutions*
- Must comply with HEOA requirements to prevent P2P file-sharing, DPI implementation as an option.

Europe: Outcomes so far

- "Three strikes will not become part of European law."
  - Commissioner Reding
- IP addresses cannot be stored by ISPs for online copyright enforcement purposes
  - EC report on data protection and copyright enforcement
- Action devolves to individual nations
  - UK – has passed graduated response
  - Belgium – court has rejected ISPs' requirement to report
  - France – has implemented graduated response
  - Ireland – private, negotiated agreement
- Debate is not over yet

Empirical Conclusions

- DPI in relation to digital piracy discussed within the context of graduated response in Europe and increasingly in the U.S., *but clearly not the only technical option to this end*.

- ISPs continue to resist urging by rights holders to implement DPI in Europe and U.S.

- Copyright enforcement issues intertwined with issues of censorship, national security and government control of public discourse

- Public interest groups and citizen activists actively voiced opinions against the use of technical measures such as DPI by ISPs in U.S. and Europe

- ***So far*, DPI is deployed more as a tool of network operators' policy than as a direct tool of public policy.**

Comparative Cases: UK and U.S

ONLINE BEHAVIORAL ADVERTISING

Online Behavioral Advertising

Behavioral Advertising

- Internet users' online activities are meticulously collected on the fly while surfing the Internet, categorized and then aggregated in allegedly anonymous but unique user profiles that are later used to display targeted advertising to Internet users.

ISPs' Role with regards to DPI

- Strategically placed at the Internet access point of their customers
- Economic pressure on smaller ISPs to increase margins
- DPI applications allow them to exploit behavioral data in order to compete with cookie-based ad networks

Main Actors UK/US

- **DPI Behavioral Ad Application Vendors**
  - NebuAd, Adzilla, Front Porch, Kindsight (U.S.), 2006 to 2008
  - Phorm (UK, later Brazil, Korea, etc.), 2007 to present
- **ISP Partners**
  - BT (Phorm)
  - 30+ smaller US ISPs
- **Internet Activist Groups**
- **Politicians, Regulators, Courts**

Proposed 4-Stage Disclosure Pattern

Evidence across several use cases suggest a common 4-stage pattern of disruption:

- Stage 1: unilateral, secret deployment
- Stage 2: uncontrolled public disclosure
- Stage 3: civil activism
- Stage 4: political, regulatory, legal proceedings

DIGITALE GESELLSCHAFT
DPI
oder
Warum wir in unseren Paketen nicht gerne herumschnüffeln lassen.

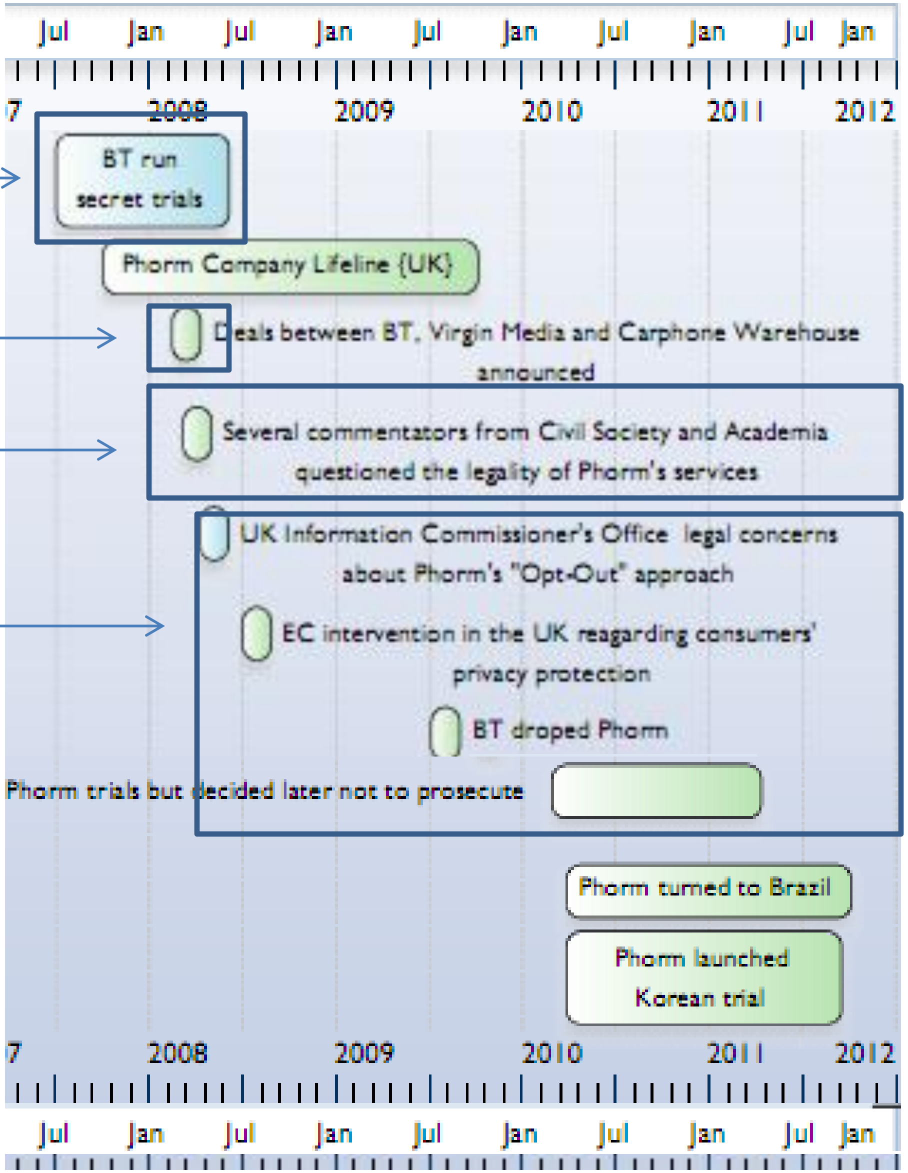
Example Timeline: Phorm (Europe)

Stage 1 - Secret Deployment

Stage 2 - Public Disclosure

Stage 3 - Civil Activism

Stage 4 - Political, Regulatory, Legal Proceedings



Stage 1: Unilateral Deployment

New technology perceived to confer an economic advantage

US ISPs

- In late 2007, several ISPs planned/implemented DPI-based customer profiling in trials of NebuAd: Cable One, CenturyTel, WOW! , Charter Communications, …

British ISPs

- BT trials Phorm secretly in 2006 + 2007, openly in 2008
- Virgin Media and TalkTalk consider Phorm in 2008

Stage 2: Public Disclosure

NebuAd (U.S.)

- *User Discovery* – In April 2008 two WOW customers notice unexpected cookies on their machine, re-direction of traffic.
- *Company Disclosure* – In May 2008, Charter Communications informs its customer via a letter that it is going to monitor its costumers' Internet traffic for targeted advertising.

Phorm (UK)

- *User Discovery* - In June 2007, BT customers noticed that their Internet traffic was redirected
- *Company Disclosure*
  - 80/20 consulting report
  - February 2008 Phorm announcement of agreements with 3 major UK ISPs ~ 70% of households with broadband access in the UK)

Disclosure linked to net neutrality and privacy activism

Stage 3: Civil Activism

NebuAd (U.S.): Discovery feeds net neutrality and privacy activism

- Reports and posts on www.dslreports.com, NYT, The Register.
- June 6, 2008 leading Internet advocacy groups urge Senate/Congress to hold hearings
- June 18, 2008, Topolsky report (Free Press, Public Knowledge)
- July 8, 2008, Center for Democracy and Technology published a legal analysis

Phorm (UK): Discovery fuels privacy activism

- March 6, 2008, Cambridge University Professor R. Anderson “If you care about your privacy, do not use BT, Virgin or TalkTalk as your ISP”
- March 12, 2008, Open Rights Group raised questions about Phorm’s compliance with the law
- March 17, 2008, Sir Tim Berners-Lee rejected customer profiling practices on the Internet
- March 4, 2009, online petition “Stop ISP's from breaching customers privacy via advertising technologies” on the Prime Minister’s web site closed with 21,403 signatures.
- From April to July 2009, Internet platforms requested an opt-out: Amazon.com, Wikimedia Foundation, etc.
- Endless FOIA requests

Stage 4: Political Proceedings

NebuAd (U.S.)

- July 2008, Senate and House Committee hearing on DPI and privacy Implications of online advertising
- August 2008, House Committee sends letters of inquiry to 34 ISPs/telcos using DPI
- *September* 2008, NebuAd closes its California offices; 10/2008, Adzilla closes US offices
- September 2008 additional Senate hearings
- Ongoing FTC regulatory activities
- Proposed Do not track and privacy legislation, 2011

Phorm (UK, EU)

- Numerous questions between 2008 and 2009 in the UK Parliament
- March 2009 House of Lords event "Online Privacy and the Interception of Internet Communications"
- Several administrative activities and interactions: Information Commissioner's Office, City of London Police, Crown Prosecution Service.
- September 2009, Phorm left the UK market, refocusing on Korea and Brazil.
- EU got involved due to UK's implementation of EU law

Stage 4: Legal/Judicial Proceedings

NebuAd (U.S.)

- NebudAd-related cases in the U.S. – *Mortensen v. Bresnan Communications*, *Deering v. CenturyTel*, and *Kirch v. Embarq* – turned on issues related to consent, notice and disclosure, respectively. Generally, they upheld the ISPs.
- Lawsuits related to Adzilla: Simon v. Adzilla
- Some settlements, but no ISP or DPI platform convicted of breaking the law

Phorm (UK, EU)

- September, 2010, EC finally referred the UK to the European Court of Justice for not complying with the ePrivacy Directive 2002/58/EC and the Data Protection Directive 95/46/EC
- April, 2011, the UK Parliament approved an amendment of the "Regulation of Investigatory Powers Regulations 2011“. EU infringement proceeding suspended.
- No British legal action against BT for the secret trials

Outcomes and Empirical Conclusion

- Disruption
  - It was DPI’s clash with pre-established norms and expectations, not its legality, which drove societal outcomes
- Market Exit
  - In both cases DPI advertising platforms were literally driven out of the market by political pressure.
- Institutionalization
  - Abrupt market exits mooted some of the more significant issues regarding law, regulation and public policy
  - FTC Report and “do not track”
  - Minor change in UK law forced by EC pressure
- Notification and Consent Paradigm
  - Ambiguities on what constitutes notification and consent

Other Interesting Conclusions

- Europe’s supposedly stronger privacy protections did not lead to tighter protection of communications confidentiality.
  - In UK no sanction by the data protection authority and no civil or criminal prosecution, much less a conviction, against Phorm or BT.
- Has the controversy killed a technology and set of market actors who might compete with the cookie-based actors?
  - Google & Facebook
  - Post-2008 convergence between capabilities of DPI and cookies

CONCLUSION AND REFERENCES

General Conclusions

- Disruption through public pressure
  - Major, ongoing changes in law, regulation, industry operations are provoked – for DPI but also similar, adjacent technologies
- The importance of technical configuration
  - Actual vs. potential exposure
- Debate and policy focus on DPI as a technology, rather than monitoring capabilities in general
  - “same ends, different means” – other technologies and approaches with comparable capabilities

- ***Will there evolve a “general” politics of DPI?***

Pointers to Key Resources

Project Resources “The Network is Aware,” www.deeppacket.info. See also work on NN, bandwidth throttling and soon IDS/IPS. See also https://twitter.com/DPIdroid. Supported by the US National Science Foundation.

Mueller, Kuehn, Santoso (2012). Policing the Network: Using DPI for Copyright Enforcement. Surveillance & Society, 9 (4): 348–364.

Kuehn, Mueller (2012). Profiling the Profilers: Deep Packet Inspection and Behavioral Advertising in Europe and the United States. SSRN: http://ssrn.com/abstract=2014181 .

Mueller (2011). DPI Technology from the Standpoint of Internet Governance Studies.

Andreas Kuehn
ankuhn@syr.edu
www.deeppacket.info

THANK YOU