

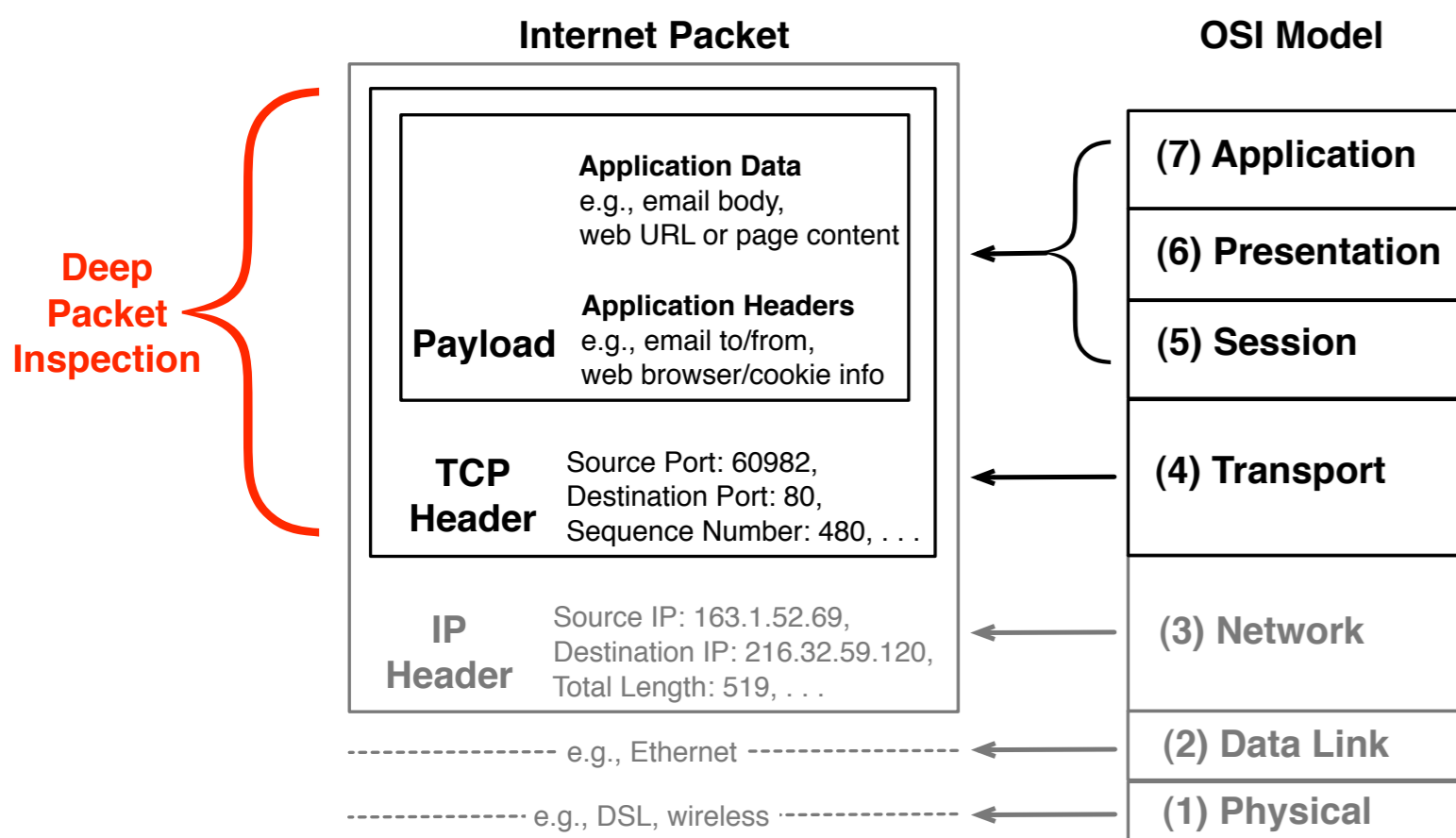
Doing the DPI Dance: Assessing the Privacy Impact of Deep Packet Inspection

In W. Aspray and P. Doty (Eds.), *Privacy in America: Interdisciplinary Perspectives* (139-165). Plymouth, UK: Scarecrow Press.

Alissa Cooper - Oxford Internet Institute

DPI needs a consistent definition for privacy purposes

- DPI defined here as ISP collection, observation, analysis, and/or storage of data relating to an application above OSI layer 3:

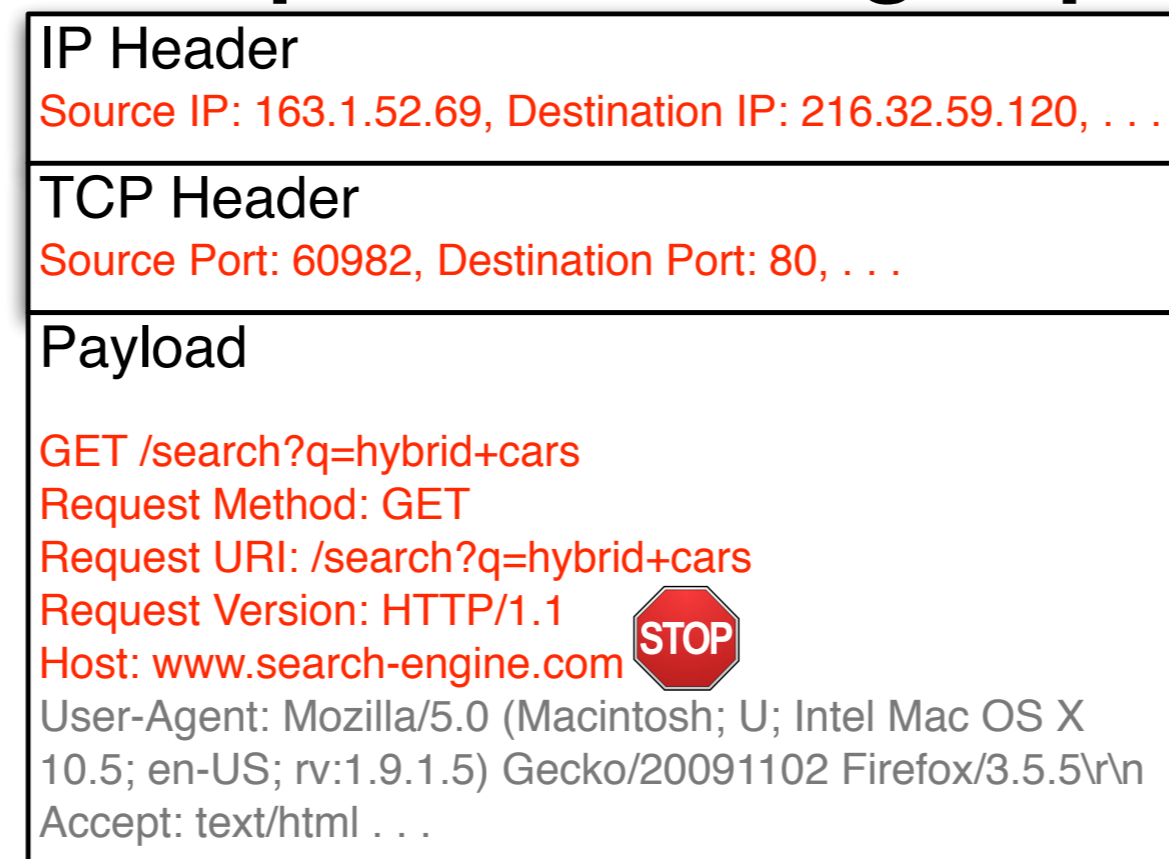


ISPs and their use of DPI pose three unique privacy challenges

- ISPs as Internet gateways:** Absent pervasive encryption, users cannot route around their ISPs.
- High ISP switching costs:** Even with a choice of ISPs, switching to a new one can be difficult/costly.
- DPI prone to mission creep:** As a general-purpose technology, DPI installed for one purpose may easily be used for other purposes.

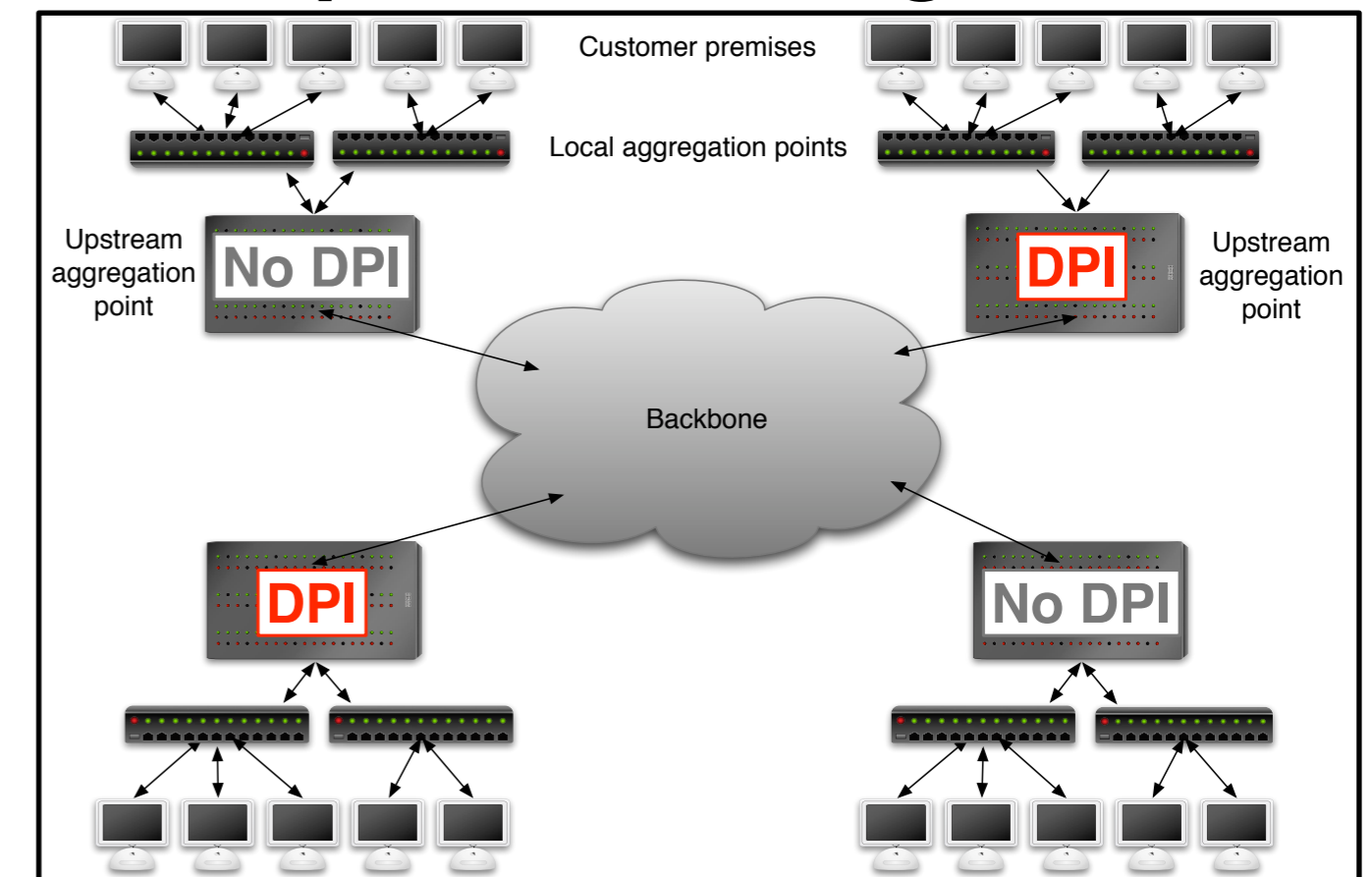
Several privacy risk mitigations exist

Example 1: Limiting depth



- Not all DPI uses require whole-packet inspection; e.g., use for behavioral advertising could limit analysis to host and URL parameters.

Example 2: Limiting breadth



- Not all DPI uses require inspection of every packet; e.g., troubleshooting or gathering usage stats may only need DPI in selective nodes.

Mitigations can reduce some risk, but extent to which they apply depends on DPI use case

✓ = mitigation is very feasible

Ex: Many ISPs provide notice of their use of DPI for troubleshooting or monitoring usage.

✗ = mitigation is **not likely** feasible

Ex: Offering users choice about DPI for congestion management would likely defeat its purpose.

? = mitigation **unclear or deployment-specific**

Ex: Necessity / length of data retention for behavioral advertising highly dependent on design of advertising system.

		Privacy Risk Mitigation				
		Limiting depth	Limiting breadth	Limiting DPI data retention	Notifying users about DPI	Offering users choice about DPI
Use Case	Monitoring usage and generating stats	✓	✓	✓	✓	✓
	Congestion management	✓	✓	✓	✓	✗
	Prioritizing certain apps or services	✓	?	✓	✓	✗
	Troubleshooting network problems	✗	✓	?	✓	✓
	Behavioral advertising	✗	?	?	✓	✓
	Filtering illegal or objectionable content	✗	?	?	✓	?
	Proactive monitoring for security problems	✗	✗	?	?	?