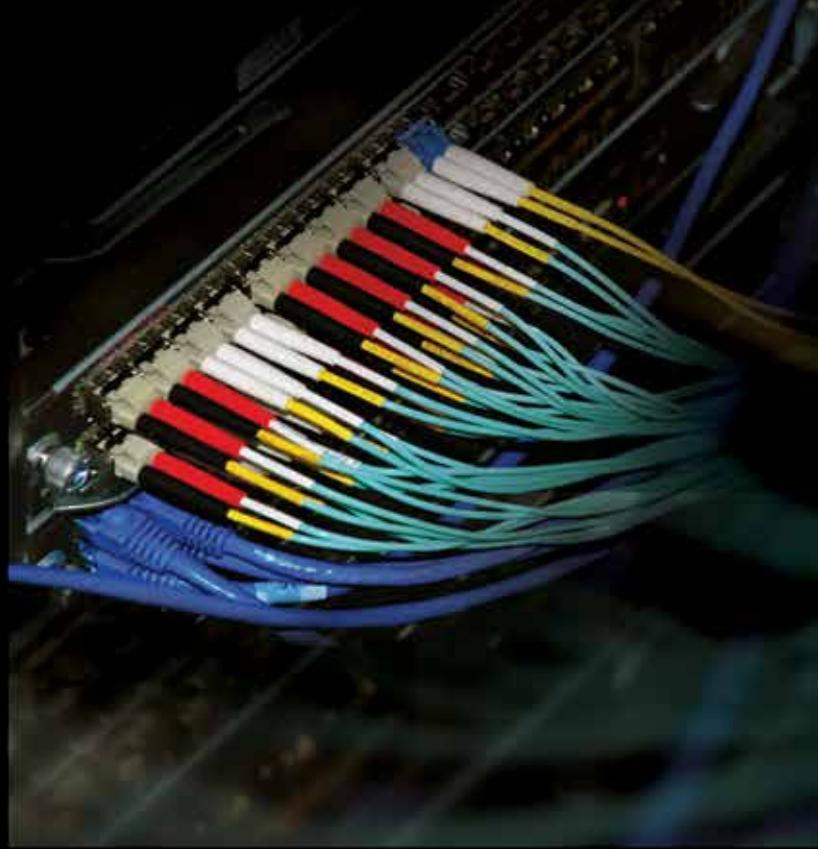


# Surveying internet surveillance

PROFESSOR MILTON MUELLER



The application of Deep Packet Inspection technologies which allow evaluation of the data being communicated online has always been a controversial subject. Here, **Professor Milton Mueller** explains how his team has looked into the role of such tools in governing the Internet



**Who is involved in this project? What range of disciplines and expertise do they represent?**

The research team has expertise in social science and technology, but the emphasis is on social science. The main disciplines involved are political science, historical political economy, science, technology and society (STS) studies, computer science and network engineering. Lengthy interviews with cooperating Deep Packet Inspection (DPI) vendors and a special relationship with technologists at the Dutch Internet Service Provider (ISP) XS4All gave us additional insights into the operational aspects of the technology.

**For those who are unfamiliar, could you explain what Measurement Lab (M-Lab) is and how it is used in your research?**

M-Lab is a globally distributed server platform that enables researchers to publish measurement tools that allow internet users to test their connections. M-Lab supports the creation of 'crowd-sourced' data. Users around the world run tests of their internet connection and the results are stored and made available to researchers. One of the tools supported by M-Lab is especially relevant to this project; a test known as 'Glasnost' detects whether ISPs are reducing the speed of peer-to-peer file sharing protocols such as BitTorrent, or blocking them outright. Careful analysis of Glasnost results can tell us whether DPI is being used to recognise the BitTorrent application. The M-Lab platform is supported by Google, the New America Foundation's Open Technology Institute and the PlanetLab Consortium. There are about 50 servers in about 20 international locations.

**What are the main methods used to answer your research questions?**

We combined quantitative data with qualitative, comparative case studies. Network performance tests from M-Lab enabled the creation of datasets showing which ISPs use DPI and when they started or stopped. Using this statistical data, as well as interviews, regulatory proceedings and other documentary information, we develop detailed analyses of DPI deployments that generated political, legal and regulatory conflicts in indifferent countries.

**Can a compromise between users' privacy and monitoring internet usage for purposes**

**of control, policy enforcement and regulation ever be achieved?**

Wherever there are network managers with a policy they want to enforce upon their users, compromises between user autonomy and organisational control must be made. They may be unbalanced and dysfunctional or reasonably satisfactory, but they happen. In a networked society these trade-offs occur at any and every level of organisation – the department, the enterprise, the campus, the ISP.

The stakes of such trade-offs increase when they affect large-scale commercial ISPs and the global Internet as a whole. Today, the trend seems to be toward evermore comprehensive surveillance, data retention and automated policy enforcement. But politically there is resistance from privacy and network neutrality advocates, the copyright resistance, advocates of internet liberty, and sometimes from the ISPs themselves. The outcome is not pre-determined.

**Are there questions you still seek to answer?**

We are still studying the use of DPI by authoritarian countries, as well as the use of Intrusion Detection and Prevention systems by national security agencies in Western countries. While gathering data about classified, sensitive practices is difficult, especially in closed societies, it will be interesting to learn how differently – or similarly – the two types of political systems handle the same technological capability.

# Profiling the profilers

With a programme that seeks to raise awareness, a research body at the **Syracuse University School of Information Studies** is making use of network performance data and detailed case studies to turn the tables on the providers that use internet surveillance technology

**WITHIN A MATTER** of decades, the Internet has gone from being a specialist technological concept to an essential part of modern culture and everyday life. Such a swift rise to significance has disrupted existing institutions governing communication and information, leaving great unanswered questions regarding internet public policy, the responsibility of those who use it and the common values upon which this important resource should be built.

Thankfully, a group led by Principal Investigator Milton Mueller at the Syracuse University School of Information Studies is shedding some light on these discussions. The team's work focuses on the emergence of Deep Packet Inspection (DPI) technologies, which arm Internet Service Providers (ISPs) or government authorities with the ability to scan and identify the data being communicated by members of their network. Recognising the potential of DPI to challenge the current principles of internet governance by disrupting the balance of power, the group seeks to investigate whether these technologies will bring into question the foundational principles behind internet usage.

## ONLINE CULTURE

While the team acknowledges that DPI technologies have beneficial applications, it has focused on how DPI has been employed by ISPs to inspect, manage and control the transfer of data using peer-to-peer protocols such as BitTorrent. While ISPs have traditionally occupied a relatively passive stance when it comes to monitoring user activity, the introduction of DPI technology could give them a more involved role in online governance. Such methods are seen by critics as unsettling the confidentiality of online behaviour and privacy of data. The widespread incorporation of DPI technologies, then, is a highly controversial move that has the ability to alter the governance of the Internet.

## USAGE PATTERNS

To stress how the implementation of DPI services has changed, Mueller looks back on the first packet-scanning tools, which were devised around 1999. The earliest DPI applications were centred on detecting network intrusions and protecting computers from malicious attacks. The focus was more about protecting network

security rather than intellectual property or content regulation.

But as the uses of the Internet multiplied, so too did the applications of DPI. The technology was adapted in order to identify and quantify the different applications, or specific items of content such as copyrighted files. Such methods of implementation gave network managers a more detailed and intrusive portrait of the activity of their users, changing the political economy of communication and information industries. In persuasive arguments posed by Mueller's team, the researchers suggest that by embracing this function of DPI systems we are at risk of threatening the open, competitive nature of the Internet and of privileging the behaviours of some users over others. These developments also raise important questions about censorship, freedom of speech and online behaviour, and should encourage us to question whether it is good practice to 'throttle' the bandwidth of certain users because of their participation on peer-to-peer platforms.

## AN ENABLING TECHNOLOGY

Yet while the researchers have expressed their concerns regarding how DPI might challenge network neutrality, undermine online confidentiality and transform the existing structures of internet governance, the US National Science Foundation-funded project set out to provide a full, dispassionate evaluation of this innovation. It is, then, important to note that the multiplicity of functions attributable to DPI has been an important factor in leading Mueller to describe it as 'an enabling technology'. Indeed, the ways in which DPI can be utilised are numerous and varied. From optimising the network itself through bandwidth management and traffic analysis, to the safeguarding of people and intellectual property through applications relating to lawful interception and copyright protection, this particular technology has the potential to contribute significantly towards managing the problems associated with the rapid rise of the Internet, problems that have not yet been adequately addressed.

## DEVELOPMENT

Indeed, what is fascinating about Mueller's work is that it forces us to consider the values

After the project began, an international debate emerged about the export of DPI capabilities from Western vendors to authoritarian countries. This raises important questions about whether control of multiple-use information technologies can be effective, and whether such restrictions do more harm than good. There is very little scientific literature about this.

Perhaps the toughest question we face is how to isolate the technology and uses of DPI from other technologies that perform similar functions.

### What do you hope the ultimate impact of this research will be?

The increasing scope and power of surveillance and information management technologies is one of the defining features of contemporary society. We want our research to broaden public awareness of this fact and contribute dispassionate empirically-grounded analysis to a passionately-debated problem.

We expect our research to provide policy makers with an insight into the actual scope of DPI deployment, the way it is being used and contested by various actors, and the ways different legal and regulatory systems are responding.

For researchers in the fields of STS, we hope our work will set a new standard for analysis of the co-production of technology and society. We hope to see our methods replicated by other researchers.

## INTELLIGENCE

### DEEP PACKET INSPECTION AND THE GOVERNANCE OF THE INTERNET

#### OBJECTIVES

Is new network technology changing the way we govern the Internet? Deep packet inspection (DPI) scans internet traffic in real time and makes automated decisions about what to do with it. This new capability has important implications for privacy, network neutrality, and service provider responsibility.

The project analysed five DPI applications to understand whether new technologies disrupt law, policy and regulation.

#### KEY COLLABORATORS

**Hadi Asghari**, Doctoral candidate, Technology University of Delft, The Netherlands

**Andreas Kuehn**, Doctoral candidate, Syracuse University School of Information Studies, USA

**Stephanie Santoso**, Doctoral candidate, Cornell University, USA

**Xiang Wang**, MS-TNM, Syracuse University School of Information Studies, USA

#### FUNDING

The project is funded by the US National Science Foundation, SBER Division, Program on Science, Technology and Society, Award SES-1026916

Work at TU Delft is funded by the Next Generation Infrastructure Foundation, project no. 04.11.TPM.

#### CONTACT

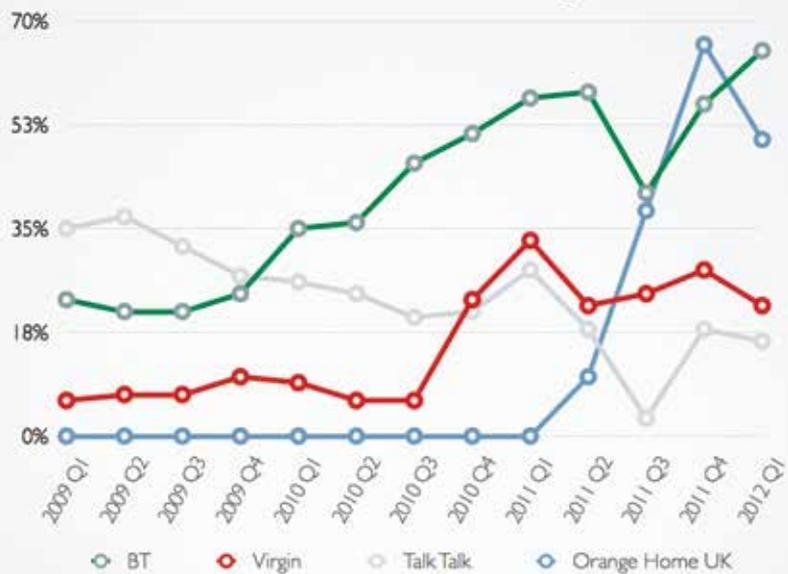
**Professor Milton Mueller**  
Principal Investigator

Syracuse University  
School of Information Studies  
307 Hinds Hall  
Syracuse, NY  
13244  
USA

T +1 315 443 5616  
E mueller@syr.edu

**MILTON MUELLER** is Professor at Syracuse University School of Information Studies, USA. Using the new institutional economics, he investigates the political economy of communication and information industries and the way institutions and governance adapt to technological change. He received a PhD from the University of Pennsylvania in 1989.

### British ISPs: DPI use as indicated by Glasnost test



we place on the Internet, and urges us to evaluate how new technology can threaten or protect our interactions within this giant and important resource. At the heart of this thorough, unbiased project is a refreshing new take on the relationship between policy, regulations, law and technology, which criticises old understandings for being misled. Crucially, Mueller challenges the image of technology and regulation as two separate entities working in competition with each other. Instead, he has a vision of interdependence, where our values and our technologies are in a constant dialogue: "Technology and regulation can disrupt and divert each other or facilitate and reinforce each other – but they always inhabit the same world". Mueller's image of a co-productive system of innovation is one of great importance when we consider how policy can govern the ways in which we operate the Internet.

#### TECHNICAL AND LEGAL IMPLICATIONS

Part of the results of the study exposed how DPI can be its own worst enemy: the technical limitations of DPI have curbed its use. For example, DPI technology can only detect patterns that it has been programmed to recognise. Thus, this tool needs to be constantly updated. Moreover, problems arise when DPI applications have to recognise a large number of items.

More revealing than the technical limitations of DPI technology are the political, social and legal consequences of its use. Mueller and his colleagues found that DPI implementation initially had disruptive effects on internet governance; but in democratic countries

public exposure of DPI usage triggered strong reassertions of privacy and net neutrality norms, leading to limitations on its use. Political influence also led to restrictions on the use of DPI by ISPs to cater advertising to internet users' preferences based on their online behaviour. Furthermore, questions surrounding who is responsible for enforcing copyright laws have also limited the uptake of DPI: "Neither the EU nor the US, for example, required DPI for copyright policing due to the disjunction between the interests of network operators and the interests of copyright holders," Mueller adds.

As a result of the technical inconveniences of DPI use, alongside press and public outrage and concern, Mueller observes a global decline in the use of DPI to detect and manipulate peer-to-peer protocols such as BitTorrent. However, its use may be increasing in other areas.

#### THE IMPACT OF AWARENESS

Looking at Mueller's study, with its use of dynamic and clever slogans such as 'The Network is Aware' and 'Profiling the Profilers' and use of data collected from internet users worldwide through open-access Glasnost data made available through the Google-supported MLab initiative, it comes as little surprise to see that the decline in DPI usage has come as a result of user awareness and observation. Such factors have turned the tables on internet surveillance and suggest that if ISPs are to become accountable for the transparent interactions of their users, they must first be in a position to justify their own behaviour.

The widespread incorporation of DPI technologies is a highly controversial move that has the ability to alter the very culture of the Internet