Christian Fuchs

SOCIETAL AND IDEOLOGICAL IMPACTS OF DEEP PACKET INSPECTION INTERNET SURVEILLANCE

This paper analyses societal and ideological impacts of Deep Packet Inspection (DPI) technologies. DPI surveillance technologies are communications surveillance tools that are able to monitor the traffic of Internet data, including content data. The analysis presented in this paper is based on product sheets, self-descriptions, and product presentations by 20 European security technology companies that produce and sell DPI technologies, as well as on whitepapers, research papers, news articles, and opinions of privacy advocates, civil society groups, and consumer protection groups. The results show the complexity of societal dimensions of DPI and the importance of the analysis of power and political economy in assessing these implications. They are interpreted in the light of the emergence of a new mode of governmentality, in which the economic interests of the security industry and state interests interact. The analysis also shows that there is a variety of ideological explanations employed by the security industry for justifying its sales of communications surveillance technologies.

Keywords political economy; Internet surveillance; Deep Packet Inspection; security industry; surveillance-industrial complex; security-industrial complex

(Received 22 August 2012; final version received 18 January 2013)

1. Introduction

The German TV programme Fakt interviewed a Syrian activist who fled to Germany. He said: 'I provided YouTube videos of demonstrations. When I was arrested, my exact behaviour was read to me from the files. Every single

step I've taken on the Internet was held against to me while I was beaten'[1] (FAKT, Syrien überwacht mit Siemens-Technik, 10 April 2012, http://www.mdr.de/fakt/siemens106.html).

> On the ground floor of a six-story building here, agents working for Moammar Gadhafi sat in an open room, spying on emails and chat messages with the help of technology Libya acquired from the West. [. . .] The Tripoli Internet monitoring center was a major part of a broad surveillance apparatus built by Col. Gadhafi to keep tabs on his enemies. Amesys in 2009 equipped the center with 'deep packet inspection' technology, one of the most intrusive techniques for snooping on people's online activities, according to people familiar with the matter. (Wall Street Journal Online, Firms Aided Libyan Spies, First Look inside Security Unit Shows how Citizens Were Tracked, 30 August 2011)

These two examples concern the Finnish–German company Nokia Siemens that according to news sources sold its Monitoring Centre (a communications surveillance technology) to Syria and Iran and the French company Amesys that according to news sources sold such technologies to Libya. According to sources, these technologies were used for monitoring political opponents of the governments. The obtained data were used for repression and in torturing activists. DPI is one of the technologies that have become infamous in this context.

These examples show that surveillance does not only have a state dimension (police and secret services monitoring citizens in order to catch criminals, terrorists, and repressing political opponents), but also has a corporate dimension: surveillance technology is a very lucrative business. State surveillance is fuelled by private businesses that produce and sell monitoring technologies that allow the surveillance of mobile phone communication, fixed line phones, email, and Internet communication and thereby achieve profit.

The security industry has especially been growing since 9/11 (Lyon 2003b, 2007) that resulted in an increased interest in the application of surveillance technologies that is guided by the technological-deterministic belief that crime and terrorism can best be stopped by creating a surveillance society. Lyon (2007, p. 184) suggests that the welfare state is being superseded by 'the safety state'. There is an increased focus on law and order politics. 9/11 has resulted legally in the definition of 'states of exception', 'most notably for preemptive war, domestic surveillance, and the torture of terrorist suspects; and practically' in 'the establishment of elaborate surveillance rituals for citizens (e.g. airport screening) and the outsourcing of lucrative security contracts to private industries' (Monahan 2010, p. 6). 'Capturing terrorists before they strike became an obsessive goal of many governments after 9/11' (Lyon 2003a, p. 52). Since

9/11, European security politics also have 'been mainly oriented towards the right for governments to strengthen coercive and surveillance security measures' (Bigo 2010, p. 265f).

Hall et al. (1978) describe how a moral panic about street robbery ('mugging') developed in the UK in the 1970s. They argue that this panic must be seen in the context of the crisis of the mid-1970s. Hall et al. (1978) stress that the moral panics of the 1970s were used for creating and enforcing law and order politics that not only tackled criminals, but especially the working class, the black working class, and social movements. The result was the rise of what Hall calls a 'law and order society'. In the political constellation characterizing the first decade of the twenty-first century, something comparable happened: 9/11 was indicative for a crisis of the hegemony of Western thought that was questioned by people and groups in Arab countries that put religious ideology against Western liberal and capitalist ideology. The 'war against terror', the security discourse and the intensification of surveillance resulted in a political crisis, in which war and terrorism tend to reinforce each other mutually, which results in a vicious cycle that intensifies hatred and conflict. Financialization and neoliberalism made capitalism more unjust (which constitutes a social crisis) and also crisis-prone, which resulted in a new world economic crisis that started in 2008. Western societies have faced a multidimensional crisis in the first decade of the twenty-first century. One of the ideological responses was to erect a surveillance society that is based on law and order politics and omnipresent surveillance. This new surveillance not only tackles criminals and terrorists, but erects a visibility of everyone and everything that also allows (actually or potentially) the control of political protests (that are on the rise in situations of crisis), which not only undercuts the liberal values of freedom of speech and assembly and thereby shows how modern society contradicts and limits its own values on which it is built.

The task of this paper is to analyse the societal, ethical, and ideological implications of one specific communications surveillance technology – DPI. DPI is a surveillance technology that allows monitoring of not only the meta-data of Internet communication (sender, recipient, type of data, etc.), but also the sent content. It is therefore, of particular interest for state and commercial actors that want to monitor citizens' and customers' behaviour and attitudes. It is therefore, no surprise that DPI, a relatively young technology, has become in recent years subject of public controversies.

This paper deals with two specific subtasks:

(1) It identifies the multitude of societal implications of DPI.
(2) It analyses which DPI technologies European security companies produce and sell, how they ideologically justify their engagement in the surveillance business, and how the companies react to negative societal implications criticized by civil society and the public.

The analysis of the societal dimensions gives a general overview of the various issues that relate to DPI in a societal context. They are political and economic in character and relate to the circumstance that DPI is produced by private companies and used by both companies and the state. Given this political and economic dimensions of DPI, a political economy of communication framework is suited. Such an analysis focuses on the 'study of the social relations, particularly the power relations, that mutually constitute the production, distribution, and consumption of resources, including communication resources' (Mosco 2009, p. 2). Applied to the analysis of DPI, this means that in order to work out this technologies' societal implications, it is important to analyse how the power relations of industry, the state and the connection of both shape the production and use of DPI. But besides the focus on economic and state power, a political-economic analysis also focuses on the role of ideology in society and a political economy of communications approach situates communication also in the context of ideology (Murdock & Golding 1974; Golding & Murdock 1978). It is therefore, not only important to study the societal implications of DPI for industry and the state, but also what are the ideological self-definitions, justifications and explanations that the security industry gives for its engagement in the production and selling of DPI. The ideological analysis is situated in a European context because this paper was conducted as part of a European-wide research project that requires such a focus. The data used for the ideological analysis stem mainly from the WikiLeaks SpyFiles that also contain data about security companies from Africa, Asia, North America, Oceania South America, which would allow to conduct the same analysis for other regions. This task, however goes beyond the scope of this paper.

In Section 2, the societal context of DPI surveillance is outlined. In Section 3, the paper's method is explained. Section 4 identifies societal implications of DPI. Section 5 presents the main results of the analysis of the ideologies of European security companies that sell DPI. Finally, some conclusions are drawn.

First, we want to define what DPI is. Data transmission on the Internet is based on the Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP is an application of the so-called Open-Systems Interconnection (OSI) Model of network data transmission to the realm of the Internet. Whereas the OSI Model consists of seven dimensions of transmission, TCP/IP maps these seven dimensions to five (Stallings 1995; Comer 2004). Table 1 shows the layers in the OSI and the TCP/IP model.

Each device (such as a computer or a printer) in a network connected to the Internet has a specific IP address. In the IP version 4 (IPv4), each IP address is a unique 32 bit long identifier (such as 170.12.252.3). For enlarging the available IP address space, the identifier length has been increased to 128 bit in version 6 of the IP (Ipv6). In order for data to be transmitted over the Internet, a source and destination IP address are needed. If a user, for example, searches for data on

TABLE 1 The layers of the OSI Reference Model and the TCP/IP.

7	Application layer	This layer provides access of applications to the network. The software applications reside at this level, such as browsers, email programmes, FTP clients, chat software, voice over IP software, file sharing software, etc.	Application
6	Presentation layer	Here, the format of the exchanged data is defined. Data are transformed, for example, compressed or encrypted. It ensures that the format of transmitted files as understood across different systems	
5	Session layer	This layer organizes the communication between two applications on different machines in the form of sessions that define, e.g. when one side transmits and avoids communication problems of the applications	
4	Transport layer	This layer receives data from the application layer, segments and reassembles the data flow into smaller units. This is necessary because files are often too large to be transmitted at once over a network. The transmission is organized in several sequential steps	Host-to-host/ transport (TCP)
3	Network layer	This layer is responsible for finding and directing the way that data packets take across various networks in order to correctly arrive at the destination network and computer (routing). It sends the data packets from network to network by finding a way so that the data are transported from the source network to the destination network	Internet (IP)
2	Data link layer	This layer secures the reliable transfer of data across networks. It breaks the data stream into blocks of data (so-called frames), calculates and adds check sums to the blocks that are checked in the destination and routing networks in order to guarantee error-free transmission	Network access
1	Physical layer	This layer takes care of the transmission of data bits over network cables, wireless connections, etc. One finds cables, plug connectors, electronic impulses, etc. on this level	Physical

Source: Stallings (1995, 2006) and Comer (2004).

Google, he enters search keyword into the Google search box. This is at the application level.

At the TCP level, the TCP takes the data, adds a communication port number (an address, by which the application is addressed) and breaks the data into packets. TCP identifies ports, the sequence number of a packet and a checksum and provides a reliable transport service (Comer 2004, p. 386). At the IP level, the IP address of the destination is determined, as well as the routing over the Internet are determined. The IP 'specifies addressing: IP divides each Internet address into a two-level hierarchy: the prefix of an address identifies the network to which the computer attaches, and the suffix identifies a specific computer on the network' (Comer 2004, p. 301). At the lower levels, the data are transmitted. The data are routed over the various routers of the Internet until it finally arrives in our example in Google's network, where it is treated in the opposite sequence (from the lowest level to the highest layer) so that data that answers to the search query is generated, which is then in the same way sent back to the user, who requested the information.

Table 2 shows the structure of a TCP/IP packet that is transmitted over the Internet. A packet is a 'small, self-contained parcel of data sent across a computer network. Each packet contains a header that identifies the sender and recipient, and a payload area that contains the data being sent' (Comer 2004, p. 666). The payload is 'the data being carried in a packet' (Comer 2004, p. 667), the header contains data such as the network address of source and destination. In the TCP/IP that the Internet uses, the packet is called an IP datagram. It consists of 'a header that identifies both the sender and receiver and a payload area that contains the data being carried' (Comer 2004, p. 658).

'Deep packet inspection is the collection, observation, analysis, and/or storage of data related to an application that is found in Internet packets above OSI layer 3' (Cooper 2011, p. 145). DPI technologies 'are capable of analysing the actual content of the traffic that is flowing' (Jason 2011, p. 118). 'DPI allows network operators to scan the payload of IP packets, as well as the header. [. . .] It enables the network operator to analyse the datagrams passing through the network in real-time and discriminate among them according to their payload' (Bendrath & Mueller 2011, p. 1144). Parsons (2008, p. 8) defines DPI technologies as surveillance methods that can 'identify the origin and content of each packet of data'. DPI surveillance technologies are communications surveillance tools that are able to monitor the traffic of network data that is sent over the Internet at all seven layers of the OSI Reference Model of Internet communication, which corresponds to the five layers of the TCP/IP. This means that DPI surveillance includes the surveillance of Internet content data. Important features of DPI are the recognition of objects on the network that may trigger notification and manipulation (Mueller 2011; Mueller et al. 2012).

TABLE 2 A TCP/IP packet.

Payload	TCP Header	IP Header
Application data: email text, URL, website content, chat message, video content, image content, etc. Application header: application programme version, email address sender/receiver, etc.	Source port Destination port Sequence number	Source IP Destination IP Total length
Defined at TCP/IP layer 5 (OSI layers 5, 6, 7)	Defined at TCP/IP layer 4	Defined at TCP/IP layer 3

2. The societal context of surveillance

The global politics and economy of the 2000s have been shaped by various phenomena, including the global hegemony of neoliberal capitalism, the emergence of a new world economic crisis, new protests and revolutions, a political crisis that is based on a vicious cycle of war and terrorism and expresses, which some have termed as the new imperialism (Harvey 2003; Wood 2003; Fuchs 2010a), a moral panic about terrorism, the expansion of state surveillance of citizens, the growth of investment in and sales of the surveillance industry, the diffusion of a conservative ideology that believes in a law and order state and a technological fix to crime and terrorism, the focus on preemptive surveillance, and the use of surveillance technologies originating in the 9/11 context against political activists. Surveillance has in the 2000s stood in the context of the neoliberal commodification of everything and the new imperialism that is based on the interaction of global capitalism, financialization and global wars.

Harvey, therefore, characterizes contemporary society as neoliberal imperialism (Harvey 2005, p. 184, 188, 190), or 'imperialism as accumulation by dispossession' (pp. 137–182). Accumulation by dispossession employs four strategies for turning assets into profitable use, that is, the commodification of everything (Harvey 2005, p. 165ff): the privatization and commodification of public assets and institutions, social welfare, knowledge, nature, cultural forms, histories, and intellectual creativity (the enclosure of the commons); financialization that allows the overtaking of assets by speculation, fraud, predation, and thievery; the creation, management, and manipulation of crises (e.g. the creation of debt crises that allow the intervention of the IMF with structural adjustment programmes so that new investment opportunities, deregulations, liberalizations, and privatizations emerge); and state redistributions which favour capital at the expense of labour (Harvey 2005, pp. 160–165, 2006, pp. 44–50).

Based on Foucault, one can argue that what Harvey terms neoliberal accumulation by dispossession forms a contemporary mode of governance: In

his lectures at the Collège de France in 1978, Foucault introduced the notion governmentality. Governmentality means that there is 'a plurality of forms of government' (Foucault 2007, p. 93). It is 'the way in which one conducts the conduct of men' (Foucault 2008, p. 186),

> the ensemble formed by institutions, procedures, analyses and reflections, calculations, and tactics that allow the exercise of this very specific, albeit very complex, power that has the population as its target, political economy as its major form of knowledge, and apparatuses of security as its essential technical instrument. (Foucault 2007, p. 108)

The state has been governmentalized, governmentality is 'both external and internal to the state' (Foucault 2007, p. 109).

Governmentality has traditionally existed in the interplay of apparatuses like the police, the military, and the church, prisons, hospitals, family, schools and education, and the truth claims that they create (knowledges). In his Collège de France lectures conducted in 1978 and 1979, Foucault described the emergence of a new form of governmentality in the twentieth century: neoliberalism. He engaged thoroughly with political economy in these lectures, which is an area that was somewhat neglected in many of his other works.

Neoliberalism aims at a society that is oriented on the 'multiplicity and differentiation of enterprises' at all levels of society (Foucault 2008, p. 149). It is in favour of the 'formalization of society on the model of the enterprise' (Foucault 2008, p. 160). It advocates the idea that the human is a homo oeconomicus – an 'entrepreneur of himself' (p. 226). This model stands for the 'economization of the entire social field' (p. 242) and the creation of an 'enterprise society' (p. 242).

Foucault gave a thorough characterization of neoliberalism in his 1978 Collège de France lectures, although he did not provide a criticism of it, which shows that his lectures were political-economic, but did not provide a critique of the political economy. Writing before the rise of Reaganomics and Thatcherism, he correctly predicted that neoliberalism was 'the birth, maybe for a short period or maybe for a longer period, of a new art of government, or at any rate, of a renewal of the liberal art of government' (Foucault 2008, p. 176). In the decades that followed, neoliberalism has become ever more extended to societies and realms of society and ever more intensified.

So Harvey (2005) argues that neoliberalism is a project that redistributes wealth and income from the poor to the rich, a project of continuous primitive accumulation that he terms accumulation by dispossession. Foucault has characterized a new model of governance that is based on the principles identified by Harvey and that step by step became the new model of how to organize capitalist states, economies, and societies. Economically, neoliberalism results in the phenomenon that capital accumulation and capitalist interests permeate large

realms of society. Therefore, security has been increasingly privatized and there has been a rise of the role of private companies in security (security industry and security services). Ideologically and politically this development has been accompanied by global wars that on the one hand try to globalize the neoliberal ideas of free enterprise and the management of society as a capitalist company and on the other hand tries to secure Western hegemony by military means. In this political-ideology context, the vicious cycle of war and terrorism has led to the rise of state security policies that advance the ubiquitous use of surveillance technologies and of a surveillance ideology that believes in being able to fight crime and terrorism by a surveillance fix to societal problems.

Given this societal context, the next section introduces the research methodology of this paper.

3. Research method

In October 2011, WikiLeaks published the so-called 'SpyFiles', a collection of files that document surveillance technologies produced by Western companies (http://wikileaks.org/the-spyfiles.html). On 23 January 2012, there were 287 documents in this archive. The archive consists of digital versions of brochures, catalogues, contracts, manuals, newsletters, papers, presentations, pricelists, and videos. WikiLeaks categorized the documented surveillance technologies documented into six types: Internet monitoring, phone monitoring, Trojan, speech analysis, SMS monitoring, and GPS tracking.

We downloaded all documents that were available on 22 February 2012, for the category of Internet surveillance for companies located in 27 countries in the European Union (EU). These were a total of 17 companies from 9 European countries (Czech Republic, Denmark, France, Germany, Hungary, Italy, Netherlands, Poland, and UK). We added three companies (Trovicor, Area Spa, and Gamma Group) because a search for news articles about privacy aspects of European Internet surveillance technology producers in the database LexisNexis showed that these three companies have been mentioned in respect to discussions about the actual or planned export of communication surveillance technology to countries where political opposition is repressed. The total number of analysed companies was therefore, set at 20. The number of files about Internet surveillance of these 20 companies that we found in the WikiLeaks SpyFiles was 64. We searched on the websites of all 20 companies for documents (white papers, product specifications, corporate responsibility reports that mention privacy aspects, etc.) about Internet surveillance technologies and found 23 additional documents that we included in the analysis. For two companies, two important documents were taken from additional sources (a product offer from the company Digitask, a Gamma Group product specification that could not be found on the company's website). There were a total of 89 documents as

input for the analysis. Table 3 shows a list of the analysed companies and the number of documents for each.

The SpyFiles are not covering all European surveillance technology producers. They however, provide comprehensive access to a sample that is large enough for conducting a document analysis that can give a picture of the type of Internet surveillance technologies that are produced in Europe and the self-understandings of the companies that create these technologies. Data about Internet surveillance technologies are not easy to obtain. On many company websites, no detailed information about the produced technologies is supplied. The sampling process must therefore, in the case of an analysis of Internet surveillance technologies be based on convenience sampling that is 'relying on available subjects' (Babbie 2010, p. 192). So, the 89 analysed files were gathered based on convenience sampling and constitute a corpus that is large enough for obtaining an impression of how the European Internet surveillance technology industry looks like.

For each company, we have conducted a document analysis of the available files. It focused on the following four aspects:

(1) Description and use of Internet surveillance technologies that are produced and sold.
(2) The self-description of the company.
(3) The explanation of the relevance of Internet surveillance, i.e. why the company thinks it is important that it produces and sells such technologies.
(4) A documentation of what the company says about problems and privacy violations arising in the context of Internet surveillance.

In order to identify societal and ethical dimensions of DPI, we conducted an Internet search for documents, whitepapers, research articles, research reports, and news reports, opinions of privacy advocates, civil society groups, and consumer protection groups. DPI is a relatively new technology, therefore, not much has been published on this topic. A title search for DPI OR 'deep packet' in the Social Sciences Citation Index (conducted on 17 February 2011) produced nine results, of which only two were really about DPI. A similar search in the database Communications and Mass Media Complete (conducted on 17 February 2011) brought 10 results, of which three focused on DPI. The appendix provides an overview of the documents that were used for identifying societal implications of DPI. We conducted a document analysis that allowed identifying six topics that relate to societal implications and contradictions of DPI.

Societal impact assessment is concerned with power relations in society that concern how relations between humans and human groups impact democracy, politics, the economy, social care, communities, families, nature, culture, everyday life, and gender (International Association for Impact Assessment 2003;

TABLE 3 A list of the companies included in the analysis.

ID	Country	Company name	Number of files
1	Czech Republic	Inveatech	1
2	France	Qosmos	6
3	France	Thales	5
4	France	Aqsacom	6
5	France	Alcatel-Lucent	3
6	France	Amesys (Bull)	18
7	Germany	Elaman	12
8	Germany	Datakom	3
9	Germany	Trovicor	1
10	Germany	Digitask	5
11	Germany	Ipoque	6
12	Germany	Utimaco Safeware	4
13	Hungary	NETI	1
14	Italy	Area Spa	0
15	Italy	Innova	1
16	Italy	IPS	3
17	Netherlands	Group 2000	8
18	Netherlands	Pine Digital Security	1
19	UK	Gamma Group	1
20	UK	Telesoft Technologies	4

Schooten et al. 2003). It wants to show if the analysed phenomena can bring about harm and negative aspects for humans in any of these realms of society. In this paper, we use an assessment method that studies existing documents that have been published about DPI in order to identify topics that relate to the societal dimensions of DPI. The exact impacts that DPI could have in the future cannot be fully assessed at the moment because it is a relatively novel technology whose wide-scale use is heavily debated in a controversial manner. So the task of this analysis is to point out areas, in which DPI could have impacts.

4. Societal implications of DPI

Internet Service Providers (ISPs) have for a long time been using DPI for network and bandwidth management, packet destination routing, and filtering (spam, viruses) (Cooper 2011). Also industry representatives stress these advantages (e.g. ipoque, #11_5). For achieving these tasks, DPI does not have to be conducted at the content level (Cooper 2011). There is the danger that the use of

DPI for various controversial purposes (see the discussion that follows) is justified by the argument that DPI is needed for network management and that surveillance is thereby extended and becomes ubiquitous at the level of ISPs. Several possible negative implications that have been identified based on available literature will now be discussed. Mueller (2011) argues that there are various DPI families for different purposes, such as network visibility/bandwidth management, user profiling/monetization, governmental surveillance, network security, copyright policing, and content control. Although some convergence of these usage cases would have developed, integration would be technologically difficult.

4.1 Net neutrality

The media reform group Free Press defines net neutrality as the principle 'that Internet service providers may not discriminate between different kinds of content and applications online. It guarantees a level playing field for all websites and Internet technologies' (http://www.savetheinternet.com/faq). If DPI is used by ISPs, then they can filter all content accessed by single users. This allows introducing business models, in which users, who pay more, get a faster access to certain services than others, which violates the principle of net neutrality. Controversial examples of the violation of net neutrality are Comcast's and Bell Canada's use of DPI for detecting and slowing down file sharing (Mueller & Asghari 2012).

One argument advanced by Free Press, the Consumer Federation of America and the Consumers Union (2006) is that giving up net neutrality would give Internet service providers a lot of power and would discriminate certain services so that their own favoured content and applications (that they either provide themselves or offer in co-operation with specific media content providers) would be advantaged and others disadvantaged. This can especially become a problem if the network provider is also a content provider or has collaboration with a content provider. A second warning by Free Press, the Consumer Federation of America and the Consumers Union (2006) is that a tiered Internet is a stratified system, in which rich players (such as big companies) use a fast Internet and everyday people, who do not have so much money, a slow Internet. Mueller and Asghari (2012) argue that ISPs' DPI use for surveillance of users' activities redistributes agency and control in a way that benefits the network operators.

4.2 The power of ISPs for undermining users' trust

Heavy use of DPI by ISPs may undermine the trust that users have in the network and ISPs and this can result in self-censorship and inhibition of users (Cooper 2011, p. 147). Internet users have to trust their ISP more than Google or

Facebook or another web platform because their whole traffic passes through the ISP's servers.

ISPs have with the help of DPI, the power to monitor the entire Internet usage of subscribers. Discussions and assessments of DPI frequently stress the crucial role of ISPs, which shows that they are crucial actors in Internet surveillance and that they hold tremendous power in implementing or preventing Internet surveillance. They hold the power to potentially build a total Internet surveillance system. Encryption can make this more difficult, but the question is if users can be expected to use encryption for all of or large parts of their Internet use and if privacy protection should be a default option guaranteed by the ISP or a non-default option that can only be achieved by special actions on behalf of the users.

4.3 Potential function creep of DPI surveillance

The notion of the surveillance creep was introduced by Marx (1988, p. 2): 'As powerful new surveillance tactics are developed, the range of their legitimate and illegitimate use is likely to spread. Where there is a way, there is often a will. There is the danger of an almost imperceptible surveillance creep'.

DPI usage for one purpose (such as network management or spam filtering) may creep to other, more privacy-sensitive activities (such as targeted advertising or content monitoring for political purposes or law enforcement, violation of net neutrality, the surveillance of file sharers, etc.). An important aspect here is that DPI can be employed 'mostly invisibly on the network' (Cooper 2011, p. 149), thereby enabling invisible surveillance creep.

4.4 Targeted advertising

Targeted advertising (also called targeted tracking, personalized advertising or behavioural advertising) means that 'marketing or media firms follow actual or potential customers' marketing and/or media activities to learn the consumers' interests and to decide what materials to offer them' (Turow 2008, p. 180).

On Facebook, targeted advertising is the standard option and there is no opt-in to this type of advertising. Facebook has the means for conducting surveillance of parts of users' online activities. Given that ISPs' employment of DPI for targeted advertising has the potential to use all user data (headers/connection and content data), one can imagine that DPI-based targeted advertising can intensify the potential problems and discussions about online data protection violations.

In 2008, there were reports that the US company Phorm had deals signed by BT, Virgin Media and Carphone Warehouse to 'report your browsing habits to Phorm' and to implement a behavioural ad targeting system (The Register, The Phorm Files,All Yer Data Pimping News in One Place, 29 February 2008).

Because of the Phorm case, the European Commission opened an infringement proceeding against the UK in order to see if the UK had correctly implemented the EU's ePrivacy and data protection rules.

Whereas targeted advertising on Facebook, Google, or DoubleClick can only be based on parts of the web usage of a user, the profiling used in deep packet targeted advertising has the potential to be based on a total Internet surveillance system that scans, filters, and analyses the entire Internet data traffic and content of a user. Deep packet inspection targeted advertising, therefore, has the potential to be a total Internet surveillance system. The main criticisms of DPI-based targeted advertising is that users' consensus needs to be obtained to such wide-reaching data processing (opt-in instead of opt-out), that sensitive data might be analysed and misused, and that there may be a surveillance function creep with unintended consequences.

According to Smythe (1977), commercial media sell the audience as a commodity. In targeted online advertising, commercial platforms like Facebook and Google gather data about portions of the time that users spend online and sell it as commodity to ad clients that provide targeted ads, they commodify Internet prosumers (Fuchs 2010b). DPI-based targeted advertising goes one step further, it has the power to monitor and commodify all the time that users spend online. It makes audience commodification totally encompassing all online time, and is a form of total commodification of online activity.

4.5 The surveillance of file sharers

DPI can be used for detecting or blocking illegal file sharing. The Belgian music industry association SABAM (Société d'Auteurs Belge – Belgische Auteurs Maatschappij) sued the ISP Scarlet and requested that it installed Audible Magic for copyright surveillance (Bendrath & Mueller 2011). In Ireland, EMI, Sony, Warner, and Universal wanted to require Eircome to implement a similar system (Bendrath & Mueller 2011). SABAM also wanted to require the Belgian social networking site Netlog to install filtering systems that prevent copyright violations. The European Court of Justice ruled that DPI-based surveillance of file sharers violates Internet users' rights to privacy, information freedom, and information protection.

Mueller et al. (2012) have shown that both in Europe and the United States, discussions about copyright policing with the help of DPI have featured an intense conflict between copyright holders on the one side and advocacy groups and ISPs on the other. These policy debates would have revolved around the 'immunity principle': Discussed policy changes 'would make the Internet access network itself responsible for surveillance, detection, notification and enforcement' of copyright infringements (Mueller et al. 2012, p. 361). Thus far, such legislation has not been successfully introduced and there are large privacy concerns about it.

Since 2007, Australia, Canada, the EU, Japan, Jordan, Mexico, Morocco, New Zealand, South Korea, Singapore, Switzerland, the United Arab Emirates, and the United States have engaged in negotiation about an Anti-Counterfeiting Trade Agreement (ACTA). If ACTA became a reality, then DPI could be used for determining, who infringes copyrights on the Internet by sharing. To use the analogy of a letter, such provisions would mean that the post office opens all letters to determine their content, keeps a record of them and in the cases where individuals or organizations send undesirable content three times, bans them from further use of the postal service, and therefore, from a fundamental means of human communication. In July 2012, the European Parliament has rejected the ratification of ACTA with a large majority. The vote was preceded by large protests in several European countries and three Europe-wide protest days.

4.6 Political repression, social discrimination and the export of Internet surveillance technologies

DPI can be used for the monitoring of specific users or a large number of users in order to find out with whom they communicate about what, including the content of communication and the filtering of content for keywords.

Algorithmic analysis and collection cannot semantically and perfectly distinguish between sensitive and non-sensitive data. The use of DPI, for targeted advertising, and by governments and companies faces the risk that sensitive data (ethnicity, political opinions, philosophical or religious beliefs, trade-union membership, data concerning health or sex life, criminal convictions) of users are being monitored. The examples about the alleged surveillance of political opposition documented in this report show that there is the risk that the processing and analysis of sensitive content, results in political repression or social discrimination of certain groups. Roger Clarke warns in this context that in many countries, including the United States, UK, and Australia, 'a considerable amount of message interception is being conducted in the absence of demonstrated and reasonable grounds for suspicion of criminal behaviour', which would represent 'concrete steps' towards an 'authoritarian future'. DPI surveillance can bring about privacy violations and the processing of sensitive data and thereby, result in repression against and discrimination of certain groups in society. The danger is that due to racial profiling Arabs and Muslims in general are considered to be terrorists until they prove not to be, that businesses exclude or provide unfair disadvantages to certain groups (¼ rational discrimination that is frequently especially based on racist assumptions, see Gandy 2009), and that arbitrary disadvantages an individual has suffered cumulate and result in further disadvantages that are enforced by predictive algorithms (¼ cumulative disadvantage, see Gandy 2009).

There have been cases, where news media reported that European security technologies exported communications surveillance technologies to countries, where they were used for the monitoring of and repression against political opponents. The examples concern the following European security companies: Area Spa (Italy), Qosmos (France), Utimaco (Germany), Amesys (France), trovicor (Germany), Nokia Siemens Networks (Finland), and Gamma Group (UK).

In April 2009, the Washington Times reported that Nokia Siemens sold a Monitoring Centre to Iran that was used for monitoring the phone calls, emails, and Internet communication of political opponents (Washington Times, Fed Contractor, Cell Phone Maker Sold Spy System to Iran, 13 April 2009). Nokia Siemens Networks' Intelligence Solutions, which was Nokia Siemens' surveillance business branch, was sold to Persua GmbH, which now operates it under the name Trovicor GmbH (Spiegel Online International, Western Surveillance Technology in the Hands of Despots, 8 December 2011). In August 2011, Bloomberg reported that the imprisoned human rights activists Abdul Ghani Al Khanjar was tortured in a Bahraini prison and that the officials possessed transcripts of his communications. According to two people associated with Trovicor, the company provided surveillance technology to Bahrain (Bloomberg, Torture in Bahrain Becomes Routine With Help From Nokia Siemens, 23 August 2011). In April 2012, German media published allegations that Nokia Siemens also sold its Monitoring Centre to Syria (Spiegel Online International, Monitoring the Opposition: Siemens Allegedly Sold Surveillance Gear to Syria, 11 April 2012).

The Wall Street Journal wrote in August 2011 that the French company Amesys, a unit of the firm Bull SA, sold DPI technologies to Libya, where Gadhafi's regime used them in an Internet spying centre in Tripoli to monitor the Internet usage of Libyan citizens and political opponents (Wall Street Journal Online, Firms aided Libyan spies. First look inside security unit shows how citizens were tracked, 30 August 2011). The British firm Gamma International sold its FinSpy software to Egyptian security authorities and the Italian firm Hacking-Team surveillance software to security agencies in North Africa and the Middle East (EUobserver.com, EU Companies Banned From Selling Spyware to Repressive Regimes, 11 October 2011).

In November 2011, there were news reports that the Italian firm Area Spa equipped the Syrian intelligence with surveillance technologies (project 'Asfador') that can be used for monitoring the political opponents of Bashar al-Assad's government. In this project, according to news reports, technologies by Qosmos (France) and Utimaco (Germany), also seem to have been used (Bloomberg, Syria Crackdown Gets Italy Firm's Aid With US-Europe Spy Gear, 4 November 2011). In Syria, hundreds of members of the political opposition have been killed by the government that tries to repress protests that started in January 2011.

We found public charges published in the mass media that European security companies exported or planned to export Internet surveillance technologies to undemocratic regimes. Such claims could be found in respect to the following countries:

- Bahrain: trovicor.
- Egypt: Gamma Group.
- Iran: Nokia Siemens Networks (cell phone networks).
- Libya: i2e Technologies (that after a fusion with Artware later became Amesys).
- Syria: Asfador project (Area Spa, Qosmos, Utimaco), Nokia Siemens Networks.

The discussion of DPI Internet surveillance brings up broader societal issues relating to power structures. The danger of large-scale and in-depth Internet surveillance points towards potential violations of the collection limitation and data minimization principles (data collection should be limited to that which is necessary for the specified purpose and should not be excessive). The danger of surveillance creep in the context of DPI is an expression of potential violations of the purposeful data procession principle (the purpose of data processing should be specified and data collection should be limited to this purpose). These principles are so-called fair information principles that are part of data protection legislation and discussions about privacy rights (Bennett & Raab 2006, p. 12; Information and Privacy Commissioner of Ontario 2009).

Violations of net neutrality that can arise from DPI could create a tiered Internet that is controlled by large media companies and slower for certain groups of users (e.g. those who pay less for Internet access). This is an issue that goes beyond concerns for privacy rights. It has to do with information inequality and is a matter of justice, inclusion/exclusion, and the centralization of power. Therefore, a societal impact could be the increase of inequality, exclusion and the asymmetrical distribution of power.

The topic of implementing targeted advertising at the Internet Service Provider level with the help of DPI relates on the one hand to privacy issues (consensus to such data processing, surveillance of sensitive data), on the other hand also to the more political-economic question if an Internet that is heavily based on advertising culture is desirable. This means that another societal impact of DPI could be the intensification of the commodification of almost everything, including culture, and therefore, the unequal access to culture.

The issue of conducting surveillance and policing of file sharers with the help of DPI has to do with questions of freedom and democracy, namely if there should be free access to cultural goods and if policing and surveillance of the Internet, results in a culture of suspicion and police power that negatively impacts democracy. A potential negative impact can be that on the one hand,

the commodification of culture is intensified and that on the other hand, culture is strongly policed, which can result in a culture of policing that limits freedom and democracy.

Last, but not least, we have seen that DPI Internet surveillance and communications surveillance in general have been used for monitoring and repressing members of the political opposition in various countries. This question is not simply a privacy issue, it rather relates to the violation of political freedoms (the freedom of assembly, association, opinion, expression), the violation of human dignity, the violation of the right to life, and the violation of the prohibition of torture and inhuman or degrading treatment. DPI here relates to issues of democracy and human rights. The violation of these rights by monitoring and repressing political opponents with the help of communications surveillance is not only a democratic and political issue – it is also a political- economic issue.

We have seen that Western companies exported communications surveillance technologies to countries, where they were used for political repression. The violation of civil rights is in these contexts, therefore connected to the profits of what Hayes (2009, 2010) terms the European security-industrial complex. He argues that there is a 'close bond between corporate and political elites in the homeland-security sector' and that on an ideological level one finds 'the inherently neoconservative appeal to the defence of the homeland' (Hayes 2010, p. 148).

> Neocon ideology is centred upon the 'right to limitless profit-making', which is at the very heart of the EU's desire to create a lucrative homeland-security industry. The EU's security policies are premised on the neocon philosophy of global policing and intervention in failed states to both pre-empt 'threats' to security and further the spread of the free market and western-style democracy around the world. (Hayes 2009, p. 7)

The security-industrial complex on the one hand wants to make a business out of developing military and surveillance technologies and on the other hand advances the large-scale application of surveillance technologies and the belief in managing crime, terrorism and crises by technological means. DPI Internet surveillance is part of this political-economic complex that combines profit interests, a culture of fear and security concerns, and surveillance technologies.

Actual and potential societal implications of DPI include negative implications, such as the violation of privacy rights, information inequality, the centralization of power, the commodification and commercialization of culture, the limitation of access to cultural goods and therefore, the increase of cultural inequality, the creation of a culture that is based on suspicion, fear and policing and therefore, the limitation of freedom and democracy, the violation of human rights and negative implications on democracy. All of these are negative societal impacts (Barrow 2000; Schooten et al. 2003). This means that DPI is a technology that can have profound implications for human well-being, material and

economic well-being, culture, the quality of everyday life, equity, and democracy. The analysis shows that DPI poses a variety of economic and political threats. Given such an analysis, the question should be posed as to how those who produce DPI technologies see the role of these tools in society. This task requires an ideology analysis. In the next section, the attitudes of the European security industry towards DPI that were identified in an ideology analysis will be presented.

5. DPI and the European security industry's ideologies

There is a variety of Internet surveillance technologies available on the European security technology market that uses DPI. Some of them are the following:

- Alcatel Lucent 1357 ULIS – Unified Lawful Interception Sites (Alcatel-Lucent).
- ALIS - Aqsacom Lawful Interception System (Aqsacom).
- BONGO Monitoring Centre (NETI).
- CS-2000, POSEIDON, Munin POTS (Elaman).
- DigiBase, DigiNet (Digitask).
- EAGLE (Amesys).
- EVE Lawful Interception Solution (Pine Digital Security).
- GENESI Monitoring Centre, GENESI Network Interception Platform (IPS).
- Target Profiling (IPS).
- iXEngine, ixMachine (Qosmos).
- Lawful Interception Mediation Architecture (LIMA), LIMA DPI Monitor, LIMA Management System (Group 2000).
- LI System (Inveatech).
- MCR System Monitoring Centre (Area Spa).
- Net Spyder, IP Tr@pper (Thales).
- PRX Traffic Manager, Net Reporter, DPX Network Probe, PACE (ipoque).
- SIP & GTP Probe (Telesoft Technologies).
- Trovicor Monitoring Centre (trovicor), formerly: Nokia Siemens Monitoring Centre (Nokia Siemens Networks).
- Utimaco Lawful Interception Management System (LIMS) (Utimaco).

An analysis of the available product sheets shows that there are two main target groups, to which the analysed DPI technologies should be sold:

(a) Telecommunications operators and Internet service providers, who can use them for network management and for enabling law enforcement agencies to intercept traffic.
(b) The state, law enforcement agencies, intelligence organizations that monitor activities on the Internet.

The following list shows the customers to whom specific firms address their technologies in the analysed brochures and documents:

(a) Telecommunications operators and Internet service providers: Alcatel-Lucent, Qosmos, Group 2000, ipoque, Utimaco.
(b) State, law enforcement agencies, intelligence organizations: Aqsacomm, NETI, Elaman, DigiTask, Amesys, Pine Digital Security, IPS, Qosmos, Group 2000, Inveatech, Area Spa, Thales, ipoque, Telesoft Technologies, trovicor, Utimaco.

Such systems are typically coupled to monitoring centres that are able to scan different types of communication networks (e.g. the Internet, fixed line telephony, and mobile telephony). Deep Packet Internet surveillance is facing the challenge, as IPs are changing and that filtering, decoding and analysis of different protocols (such as email, webmail, VoIP, chat, http, FTP, etc.) are needed in order to thoroughly monitor Internet traffic.

van Dijk (1998, 2011) has proposed a scheme called the Ideological Square for the analysis of ideologies. He argues that there are four common ideological argumentation strategies:

- To emphasize positive things about Us (¼ the in-group).
- To emphasize negative things about Them (¼ the out-group).
- To de-emphasize negative things about Us.
- To de-emphasize positive things about Them.

'The complex meta-strategy of the ideological square tells us that group members will tend to speak or write positively about their own group, and negatively about those out-groups they define as opponents, competitors or enemies' (van Dijk 2011, p. 397). Reisigl and Wodak (2009) call the discourse strategy of setting up a Us/Them difference 'predication'. Predication is the 'discursive qualification of social actors, objects, phenomena, events/processes and actions' as 'more or less positively or negatively' (Reisigl & Wodak 2009, p. 94).

We have used van Dijk's scheme for identifying how the documents of the analysed security problems relate to potential problems in society caused by the use of their technologies. A range of how European companies position themselves towards questions regarding privacy violations and other problems of DPI technologies exists. Six positions could be identified in the conducted analysis.

(a) No discussion

A first identified rhetoric strategy was that the discourse is rejected at all: no problems are seen, the role of security technologies in society is not an issue. In this type of discourse, there was either (1) no commenting on potential problems of DPI use in the analysed documents or (2) if there was criticism of a specific company, it declined to comment. Aspects relating to privacy and other potential

problems associated with DPI often were not mentioned in the analysed documents and on the analysed websites (e.g. Inveatech, Aqsacom, Datakom, and NETI). Some companies responded to charges by refusing to comment and with the reference to trade secrets and customer protection. For example, being asked if trovicor exported communications surveillance technology to Bahrain, trovicor officials 'were only willing to state that they could not publicly discuss customers and the details of agreements' (Spiegel Online International, Western Surveillance Technology in the Hands of Despots, 8 December 2011).

(b) Emphasis on positive company aspects

The ideological strategy of emphasizing positive aspects about oneself took on two forms.

(b1) Addressing of security technology exports

Thales, a company against which no charges were made in the mass media, in its 2010 Corporate Responsibility Report (#3_5) addressed the issue of the export of security technologies. It writes that it respects export controls because profitability can otherwise be harmed by negative news reporting. Thales says that it respects 'obtaining export licences from various national authorities' because 'breaching export controls can have serious consequences for a company. Depending on the nature of the violation, sanctions can include heavy fines, imprisonment of company officials and prohibition of future exports or imports by the company' (#3_5, p. 18).

The interesting aspect of this argument is that Thales argues entirely self-focused in terms of its profits. It does not talk about negative implications that the use of DPI or other surveillance technologies can have for citizens or consumers, but is rather only concerned with its own profit interests.

(b2) Presentation of advantages of DPI

Some companies stressed in discussion of advantages and disadvantages of DPI that there are big advantages. For example, ipoque mentioned that DPI is used in network and bandwidth management and the filtering of spam emails and computer viruses. Telesoft Technologies says that DPI is needed for network management and that it can create new personalized content services with payment.

The ideological strategy is to only talk about potential positive aspects that the use of technologies produced by security technologies has and to avoid engagement with potential negative aspects.

(c) Emphasis on negative aspects about Them

The most frequently found ideological strategy in how security companies address societal aspects of DPI was that they constructed a Us/Them difference between governments and their institutions on one side, and with whom the

companies identify, and criminals and terrorists on the other side. They painted the picture that society is full of crime and terrorism that needs to be controlled and can be controlled with the help of the surveillance technologies that are produced and sold by the companies themselves. So, a typical explanation why European companies sell Internet surveillance technologies is that criminals and terrorists use the Internet and that Internet surveillance can prevent and police crime and terrorism.

Inveatech says that Internet surveillance is necessary to 'be able to guarantee public safety' (document #1). Thales argues that 'terrorism and cybercrime are on the rise' (#3_4, 3). Aqsacom says that there is a 'dark side to the Internet's power – namely the Internet's exploitation by criminals and terrorists' (#4_5, 3). Amesys argues that Internet surveillance is needed in order 'reduce crime levels, protect from terrorism threats, and identify new incoming security danger[s]' (#6_1). Elaman points out that Internet surveillance is needed 'for investigating and prosecuting criminal activities and terrorism' (#7_10, 11). trovicor says: 'When it comes to fighting crime and thwarting terrorist attacks, law enforcement and government security agencies need the right communication tools to get results' (http://www.trovicor.com/en/business-sections/lawful-interception.html). Utimaco writes that there is a 'broad availability of communication options and the relative ease with which criminal networks and terrorist groups can exchange information' (#12_4, 5). IPS states: 'Criminal organizations exploit these applications taking advantage of the anonymity granted by the Internet. Social Networks monitoring or Web Mails interception can gather the intelligence helping to identify people involved in criminal activities' (http://www.resi-group.eu/ips/?page_id=210&lang=en). The Gamma Group holds: 'The increase of cyber crime both through terrorism, intimidation and industrial espionage are constantly on the rise, and illegal activities are aided by available technologies' (#19).

These opinions can be considered as being expressions of a specific worldview on the role of crime in society that has by some scholars been characterized as conservative ideology of crime (Hall et al. 1978; Jewkes 2011). It is based on law and order politics and the assumption that surveillance technologies should be heavily used and can prevent crime and terrorism. It 'emphasizes deterrence and repression and voices support for more police, more prisons and a tougher criminal justice system' (Jewkes 2011, p. 62). Policing crime and terror can in such a situation easily turn over into policing the poor, the unemployed, minorities, people of colour, and civil society. The practice of using new surveillance technologies not only tackles criminals and terrorists, but erects a visibility of everyone and everything that also allows (actually or potentially) the control of political protests (that are on the rise in situations of crisis), which undercuts the liberal values of freedom of speech and assembly and thereby shows how modern society today is running the risk of contradicting its own values, on which it was built.

The identified technology fetishism of the security industry is grounded in a strong belief in the power of technology that is conceived as being independent of society. Societal phenomena (crime, terror, crises, and political transformations) are mistaken to be caused and controllable by technology. But societal phenomena merely express themselves in communicative and technological spaces, they are not caused by them. Technological determinism inscribes power into technology, it reduces power to a technologically manageable phenomenon and thereby neglects the interaction of technology and society. Technological determinism sees technology as developing independently from society, but as inducing certain societal effects with necessity

(d) De-emphasis on negative aspects of DPI

This ideological strategy took on the form of statements that came about as the result of public pressure (media and civil society). Such statements typically tried to reassure the public that the consequences of DPI use that were criticized were not so severe and that the company in question had already taken remedial measures (such as leaving a certain project or selling parts of its business).

So in some analysed cases, public pressure (media and civil society) created company reactions to claims that there were plans of selling surveillance technologies to regimes that repress political opposition.

One analysed company (Qosmos) said that a mistake was made and that they would pull out of the project that engaged in the export of surveillance technologies. The export of surveillance technology seems in this circumstance to have been prevented because critical journalists and civil society stepped in. Civil society tends to have limited resources and one can ask what will happen in those cases that remain unknown.

News reports have argued that Monitoring Centres produced by Nokia Siemens and trovicor were used to repress the Iranian and Bahrainian opposition, people like the journalist Isa Saharkhiz and the political activists Poojan Mahmudian and Kianoosh Sanjari in Iran or the Bahraini human rights activist Abdul Ghani Al Khanjar. After media reports and heavy public criticism, Nokia Siemens Networks admitted that a surveillance system for local phone networks was implemented in Iran, but said that it had already sold its intelligence business in March 2009.

In autumn 2011, charges emerged that claimed that the follow-up company trovicor sold a monitoring centre to Bahrain, where according to media reports it was used for surveilling political opponents. Investigative journalist Erich Möchel pointed out that public pressure (by the media and civil society) on one company does not automatically stop unethical business practices, but can result in the selling of business units to other companies that engage in comparable practices:

> Meanwhile predominates the insight that the collateral damage for company policy probably will be much smaller if these Monitoring Centers [. . .] are

companies identify, and criminals and terrorists on the other side. They painted

> cally so that this foreign equipment supplied by third parties can without problem be docked to one's own telephone networks. [. . .] It is pure market politics, nothing else. It has nothing to do with human rights, but only with the fact that one does not want to dirty one's own hands. (NDR, ZAPP: Interview mit Erich Möchel, 7 December, 2011, http://www.ndr.de/fernsehen/sendungen/zapp/media/moechel103.html)

(e) De-emphasis on positive things about Them

In one document (by Elaman from Germany), we found an approval of the surveillance of the communication of the political opposition. The rhetoric strategy used set up an Us/Them Difference between the government and the opposition. Political opposition was not seen as important for a dynamic democracy, but as disruptive factor that needs to be controlled and monitored. So the used formulation justified the surveillance of the communication of political opponents. Elaman wrote that with communications surveillance 'governments can identify an individual's location, their associates and members of a group, such as political opponents' (#7_12, 17). The question that arises here is whether this formulation questions the 'right to freedom of peaceful assembly and to freedom of association' that is defined in article 11 of the European Convention of Human Rights and in article 12 of the Charter of Fundamental Rights of the European Union. Elaman's formulation may however imply that it wants to enable governments in general to monitor the membership of political groups, which may limit the right to freedom of political assembly.

6. Conclusion

Hall et al. (1978) argue that the law and order worldview has been connected to the rise of neoliberal economies. So whereas this worldview sees the need for a strong state in the area of policing, it advocates liberalization, privatization, and deregulation in the economy. The involvement of the security industry in the production of communications surveillance technology that is used by state actors is characteristic for the neoliberal mode of governance – policing is turned into a profitable business; companies make profit from surveillance technologies that are sold to state actors.

Policing looks for security by algorithms in a world of high insecurity (Gandy 2009; Mattelart 2010). It advances a fetishism of technology – the belief that crime and terrorism can be controlled by technology. Technology promises an easy fix to complex societal problems. This explains the results that the security industry tends to justify the selling of surveillance technologies, such as DPI, with reference to the ideological assumption that more surveillance is needed for fighting crime and terror.

The post-9/11 situation has resulted, not only in the intensification of surveillance (Lyon 2003a), but at the same time in the growth of the security industry. DPI Internet surveillance, as well as communication surveillance must be placed in the context of the post-9/11 moral panic about terrorism, the rise of a security-industrial complex, the new imperialistic vicious cycle of war and terrorism and the neoliberal politics of privatization and commodification of everything.

The interconnection of state surveillance and corporate surveillance that is expressed in examples, such as DPI surveillance must be seen in the context of the rise of neoliberal governmentality that has generalized the principles of markets, competition, the enterprise, commodification, individual responsibility, and the ideology of the homo oeconomicus to large realms of society. The capitalist economy has thereby become an important principle that governs the life and conducts of populations and interacts with other apparatuses of government such as the state. Surveillance in the climate of neoliberalism has taken on commercial forms and become a central principle of consumer culture. After 9/11, Western states have tried to erect panoptic surveillance mechanisms in order to control and gain insights into the world population's communication based on the naïve belief that technological methods of surveillance can prevent the societal problem of terrorism. The context of these surveillance state endeavours is the situation of neoliberal governmentality, which requires that states gain access to privately gathered data in order to build a panopticon that makes citizens' communicative activities visible for the state. The visibility erected by companies is coupled to state activities. The result have been policies like the EU's Data Retention Directive that requires EU Internet service providers and telecommunications companies to store identification and connection data of all users of phones and the Internet so that the police can gain access to data about suspected terrorist or criminal activities. Surveillance after 9/11 has acquired its own specific form of political economy that connects economic surveillance and state surveillance.

Foucault uses the notion of governmentality for non-state forms of governing. In policing, governing the population has taken on a new governmentality regime that is based on the access of the state to surveillance data gathered by private actors and the state use of surveillance technologies produced by the capitalist security industry. The state–capital nexus is a central feature of the contemporary political economy of surveillance. A security-industrial context has emerged (Hayes 2009, 2010). The security-industrial complex on the one hand wants to make a business out of developing military and surveillance technologies and on the other hand advances the large-scale application of surveillance technologies and the belief in managing crime, terrorism and crises by technological means. DPI Internet surveillance is part of this political-economic complex that combines profit interests, a culture of fear and security concerns, and surveillance technologies.

Moral panics are ideological reactions to situations of crisis. They create a public discourse that distracts the attention from the political-economic and societal causes of societal problems, constructs certain groups as scapegoats, and promises easy solutions (policing, surveillance technologies, law and order politics that include harsh sentences) to complex problems (Cohen 1972/2002; Hall et al. 1978; Jewkes 2011)

Contemporary discourses about terrorism and security constitute a moral panic: Western governments, the police, intelligence agencies, the military, the media, and businesses tend to present a Muslim terrorist threat. The terrorism discourse is ever-present in Western political discussions since 9/11. Although there were actual attacks in Western countries (New York, London, Madrid), the discourse seems to imply that the threat is so present that every Muslim is a potential terrorist and that we require a law and order state that uses harsh sentences, long-term imprisonment, the death penalty, preventive policing, a three strikes rule, mandatory sentencing, and that limits probation possibilities. The intensification of surveillance is the ideological reaction to the terrorist panic. The very discourse about Muslim terrorism and increased warfare can result in a spiral that amplifies terrorism itself because Arab people feel unfairly and in a racist manner signified by Western discourses to which they can react with radicalization.

Moral panics often make use of signification spirals (Hall et al. 1978, p. 223). After 9/11, the terrorism threat discourse emerged. The focus was on terrorists and potential terrorists, hardly on the causes of terrorism. The complex phenomenon was much simplified and reduced to its immediate dimension – the act of violence – by abstracting from the structures that produce terrorist potentials. A signification spiral set in, in which politics, law enforcement, military, intelligence and the media painted the picture of omnipresent terrorism and called for war and surveillance, which were presented as means that bring 'security'.

The Internet as a relatively new medium of information, communication and collaboration (Fuchs 2008) is inserted into contemporary moral panics in a different way than the mainstream media that simply tend to act as ideological control institutions. The Internet acts as arena of ideological projections of fears and hopes that are associated with moral panics – some argue that it is a dangerous space that is used by terrorists and criminals, and therefore, needs to be policed with the help of Internet surveillance, whereas others argue that the Internet is a new space of political hope that is at the heart of demonstrations, rebellions, protests and revolutions that struggle for more democracy. What both discourses share is a strong belief in the power of technology independently of society, they mistake societal phenomena (crime, terror, crises, political transformations) to be caused and controllable by technology. But societal phenomena merely express themselves in communicative and technological spaces, they are not caused by them. Technological determinism inscribes power into technology, it reduces power to a technologically manageable phenomenon and thereby neglects the interaction of technology

and society. The Internet is not like the mainstream mass media, an ideological actor, but rather an object of ideological signification in moral panics and moral euphoria.

The analysis of security companies' ideologies presented in Section 5 shows that a variety of ideological strategies tends to be employed: Discussing negative dimensions of DPI was either avoided or circumvented by only stressing positive aspects of DPI or the companies' business behaviour. The need for DPI was emphasized with the help of a combination of a conservative ideology that stresses threats of crime and terrorism and a techno-fetishistic ideology that claimed that there was the power of technology to prevent crime and terror. The major problem is that security companies that sell surveillance technologies make profits with technologies that can harm democracy, freedom and human rights and can foster the advancement of totalitarianism and a fascist surveillance society. There are no easy solutions to this problem, except for the recommendation that stakeholders see that societal problems do not have easy technological fixes and that crime and terrorism can only be overcome by tackling their root causes, such as inequality, poverty, discrimination, and power asymmetries. The combination of a capitalist surveillance industry and law and order politics by the state has created a dangerous political economy that puts society at high risks. A paradigm shift is needed from the conservative ideology of crime and terror and the fetishism of crime fighting by technology towards a realist view of crime that focuses on causes that are grounded in society and the lived realities of humans and power structures and that overcoming problems in society requires changes that address the causes of societal problems (Young 1992/2002; Matthews & Young 1992/2009; Young 2002; DeKeseredy et al. 2006; Friedrichs 2009; Matthews 2009; Friedrichs 2010; DeKeseredy 2011).

Acknowledgements

The research presented in this paper was conducted in the project 'PACT – Public Perception of Security and Privacy: Assessing Knowledge, Collecting Evidence, Translating Research into Action', funded by EU FP7 SECURITY, grant agreement no. 285635

Note

1 Translation from German. 'Ich stellte YouTube Videos von Demonstrationen bereit. Als ich danach verhaftet wurde, wurde mir meine genaue Vorgehensweise aus den Akten vorgelesen. Jeder einzelne Schritt, den ich im Internet unternommen habe, wurde mir vorgehalten, während ich geschlagen wurde'.

References

Babbie, E. (2010) The Practice of Social Research, Wadsworth, Belmont, CA.

Barrow, C. J. (2000) Social Impact Assessment. An Introduction, Arnold, London.

Bendrath, R. & Mueller, M. (2011) 'The end of the net as we know it? Deep packet inspection and Internet governance', New Media & Society, vol. 13, no. 7, pp. 1142–1160.

Bennett, C. & Raab, C. (2006) The Governance of Privacy, MIT Press, Cambridge, MA.

Bigo, D. (2010) 'Delivering liberty and security? The reframing of freedom when associated with security', in Europe's 21st Century Challenge. Delivering Liberty, eds D. Bigo, S. Carrera, E. Guild & R. B. J. Walker, Ashgate, Farnham, pp. 263–287.

Cooper, A. (2011) 'Doing the DPI dance. Assessing the privacy impact of deep packet inspection', in Privacy in America. Interdisciplinary perspectives, eds W. Aspray & P. Doty, Scarecrow Press, Plymouth, pp. 139–165.

Cohen, S. (1972/2002) Folk Devils and Moral Panics, Routledge, London.

Comer, D. E. (2004) Computer Networks and Internets, Pearson, Upper Saddle River, NJ.

DeKeseredy, W. S. (2011) Contemporary Critical Criminology, Routledge, London.

DeKeseredy, W. S., Alvi, S. & Schwartz, M. D. (2006) 'Left realism revisited', in Advancing Critical Criminology, eds W. S. DeKeseredy & B. Perry, Lexington, Lanham, MD, pp. 19–41.

van Dijk, T. (1998) Ideology. A Multidisciplinary Approach, Sage, London.

van Dijk, T. (2011) 'Discourse and ideology', in Discourse Studies. A Multidisciplinary Introduction, ed. Teun van Dijk, Sage, London, pp. 379–407.

Foucault, M. (2007) Security, Territory, Population. Lectures at the Collège de France 1977–1978, Palgrave Macmillan, Basingstoke.

Foucault, M. (2008) The Birth of Biopolitics. Lectures at the Collège de France 1978–1979, Palgrave Macmillan, Basingstoke.

Free Press, Consumer Federation of American & Consumers Union (2006) 'Why consumers demand Internet freedom. Network neutrality: fact vs. fiction', [Online] Available at: http://www.freepress.net/files/nn_fact_v_fiction_final.pdf (7 February 2013).

Friedrichs, D. O. (2009) 'Critical criminology', in 21st Century Criminology. A Reference Handbook, vol. 1, ed. J. M. Miller, Sage, Thousand Oaks, CA, pp. 210–218.

Friedrichs, D. O. (2010) Trusted Criminals. White Collar Crime in Contemporary Society, 4th edn, Wadsworth, Belmont, CA.

Fuchs, C. (2008) Internet and Society. Social Theory in the Information Age, Routledge, New York.

Fuchs, C. (2010a) 'Critical globalization studies: an empirical and theoretical analysis of the new imperialism', Science & Society, vol. 74, no. 2, pp. 215–247.

Fuchs, C. (2010b) 'Labor in informational capitalism and on the Internet', The Information Society, vol. 26, no. 3, pp. 179–196.

Gandy, O. H. (2009) Coming to Terms with Chance. Engaging Rational Discrimination and Cumulative Disadvantage, Ashgate, Farnham.
Golding, P. & Murdock, G. (1978) 'Theories of communication and theories of society', Communication Research, vol. 5, no. 3, pp. 339–356.
Hall, S., Critcher, C., Jefferson, T., Clarke, J. & Roberts, B. (1978) Policing the Crisis, Palgrave Macmillan, Basingstoke.
Harvey, D. (2003) The New Imperialism, Oxford University Press, Oxford.
Harvey, D. (2005) A Brief History of Neoliberalism, Oxford University Press, Oxford.
Harvey, D. (2006) Spaces of Global Capitalism. Towards a Theory of Uneven Geographical Development, Verso, London.
Hayes, B. (2009) NeoConOpticon. The EU Security-Industrial Complex, Transnational Institute/Statewatch, Amsterdam.
Hayes, B. (2010) '"Full spectrum dominance" as European Union security policy. On the trail of the "NeoConOpticon"', in Surveillance and Democracy, eds K. D. Haggerty & M. Samatas, Routledge, Oxon, pp. 148–169.
Information and Privacy Commissioner of Ontario (2009) 'Creation of a global privacy standard'. [Online] Available at http://www.ipc.on.ca/images/Resources/gps.pdf (7 February 2013).
International Association for Impact Assessment (2003) Social Impact Assessment. International Principles. Special Publication Series No. 2, IAIA, Fargo, ND.
Jason, A. (2011) The Basics of Information Security, Syngress, Waltham, MA.
Jewkes, Y. (2011) Media & Crime, 2nd edn, Sage, London.
Lyon, D. (2003a) Surveillance after September 11, Polity, Cambridge.
Lyon, D. (2003b) 'Surveillance after September 11, 2011', in The Intensification of Surveillance. Crime, Terrorism and Warfare in the Information Age, eds K. Ball & F. Webster, Pluto Press, London, pp. 16–25.
Lyon, D. (2007) Surveillance Studies. An Overview, Polity, Cambridge.
Marx, G. T. (1988) Undercover. Police Surveillance in America, University of California Press, Berkeley, CA.
Mattelart, A. (2010) The Globalization of Surveillance, Polity, Cambridge.
Matthews, R. (2009) 'Beyond "so what?" criminology. Rediscovering realism', Theoretical Criminology, vol. 13, no. 3, pp. 341–362.
Matthews, R. & Young, J. (1992/2009) 'Reflections on realism', in Key Readings in Criminology, ed. T. Newburn, Willan, Oxfordshire, pp. 278–282.
Monahan, T. (2010) Surveillance in the Time of Insecurity, Rutgers University Press, New Brunswick, NJ.
Mosco, V. (2009) Political Economy of Communication, 2nd edn, Sage, London.
Mueller, M. L. (2011) 'DPI technology from the standpoint of Internet governance studies', [Online] Available at: http://dpi.ischool.syr.edu/Papers_files/WhatisDPI-2.pdf (7 February 2013).
Mueller, M. L. & Asghari, H. (2012) 'Deep packet inspection and bandwidth management. Battles over BitTorrent in Canada and the United States', Telecommunications Policy, vol. 36, no. 6, pp. 462–475.

Mueller, M. L., Kuehn, A. & Santoso, S. M. (2012) 'Policing the network. Using DPI for copyright enforcement', Surveillance & Society, vol. 9, no. 4, pp. 348–364.
Murdock, G. & Golding, P. (1974) 'For a political economy of mass communications', in The Political Economy of the Media I, eds P. Golding & G. Murdock, Edward Elgar, Cheltenham, pp. 3–32.
Parsons, C. (2008) 'Deep packet inspection in perspective: tracing its lineage and surveillance potentials. Version 1.2', [Online] Available at: http://www.sscqueens.org/sites/default/files/WP_Deep_Packet_Inspection_Parsons_Jan_2008.pdf (7 February 2013).
Reisigl, M. & Wodak, R. (2009) 'The discourse-historical approach', in Methods of Critical Discourse Analysis, 2nd edn, eds R. Wodak & M. Meyer, Sage, London, pp. 87–121.
van Schooten, M., Vanclay, F. & Slootweg, R. (2003) 'Conceptualising social change processes and social impacts', in The International Handbook of Social Impact Assessment. Conceptual and Methodological Advances, eds H. A. Becker & F. Vanclay, Edward Elgar, Cheltenham, pp. 74–91.
Smythe, D. (1977) 'Communications: Blindspot of Western Marxism', Canadian Journal of Political and Social Theory, vol. 1, no. 3, pp. 1–28.
Stallings, W. (1995) Operating Systems, 2nd edn, Prentice-Hall, Eaglewood Cliffs, NJ.
Stallings, W. (2006) Data and Computer Communications, Prentice-Hall, Eaglewood Cliffs, NJ.
Turow, J. (2008) Niche Envy. Marketing Discrimination in the Digital Age, MIT Press, Cambridge, MA.
Wood, E. M. (2003) Empire of Capital, Verso, London.
Young, J. (1992/2002) 'Ten points of realism', in Criminology. A Reader, eds Y. Jewkes & G. Letherby, Sage, London, pp. 42–55.
Young, J. (2002) 'Critical criminology in the twenty-first century. Critique, irony and the always unfinished', in Critical Criminology, eds K. Carrington & R. Hogg, Willan, Cullompton, pp. 251–271.

Appendix. References for the analysis of societal implications of DPI

80/20 Thinking, 'Privacy impact assessment for phorm', [Online] Available at: http://www.phorm.com/assets/reports/Phorm_PIA_Final.pdf (7 February 2013).
Bendrath, R. & Mueller, M. (2011) 'The end of the net as we know it? Deep packet inspection and Internet governance', New Media & Society, vol. 13, no. 7, pp. 1142–1160.
Berners-Lee, Tim (2009) 'No snooping', [Online] Available at: http://www.w3.org/DesignIssues/NoSnooping.html (7 February 2013).

Brand Republic News Releases (2010) 'EU to take UK to court over Internet privacy rules', 4 October.

Clarke, R. (2009) 'Deep packet inspection. Its nature and implications', [Online] Available at: http://www.rogerclarke.com/II/DPI08.html (7 February 2013).

CNET UK (2009) 'Virgin media and CView to rifle through your packets', 27 November.

Cooper, A. (2011) 'Doing the DPI dance. Assessing the privacy impact of deep packet inspection', in Privacy in America. Interdisciplinary perspectives, eds. W. Aspray & P. Doty, Scarecrow Press, Plymouth, pp. 139–165.

Daly, A. (2010) 'The legality of deep packet inspection', [Online] Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1628024 (7 February 2013).

Electronic Privacy Information Center (EPIC), 'Deep packet inspection and privacy', [Online] Available at: http://epic.org/privacy/dpi/ (7 February 2013).

Free Press, Consumer Federation of American & Consumers Union (2006) 'Why consumers demand Internet freedom. Network neutrality: fact vs. fiction', [Online] Available at: http://www.freepress.net/files/nn_fact_v_fiction_final.pdf (7 February 2013).

Landau, S. (2010) Surveillance or Security? The Risks Posed by New Wiretapping Technologies, MIT Press, Cambridge, MA.

Lessig, L. & McChesney, R.W. (2006) 'No tolls on the Internet', The Washington Post, 8 June.

McStay, A. (2011) 'Profiling phorm. An autopoietic approach to the audience-as-commodity', Surveillance & Society, vol. 8, no. 3, pp. 310–322.

Morozov, E. (2011) 'Political repression 2.0', New York Times, 1 September.

Mueller, M. L. (2011) 'DPI technology from the standpoint of Internet governance studies', [Online] Available at: http://dpi.ischool.syr.edu/Papers_files/WhatisDPI-2.pdf (7 February 2013).

Mueller, M. L. & Asghari, H. (2012) 'Deep packet inspection and bandwidth management. Battles over BitTorrent in Canada and the United States', Telecommunications Policy, vol. 36, no. 6, pp. 462–475.

Mueller, M. L., Kuehn, A. & Santoso, S. M. (2012) 'Policing the network. Using DPI for copyright enforcement', Surveillance & Society, vol. 9, no. 4, pp. 348–364.

Office of the Privacy Commissioner of Canada (2009) 'Review of the Internet traffic management practices of Internet service providers', 18 February, [Online] Available at: http://www.priv.gc.ca/information/pub/sub_crtc_090728_e.cfm (7 February 2013).

Parsons, C. (2008) 'Deep packet inspection in perspective: tracing its lineage and surveillance potentials. Version 1.2', [Online] Available at: http://www.sscqueens.org/sites/default/files/WP_Deep_Packet_Inspection_Parsons_Jan_2008.pdf (7 February 2013).

Privacy International (2009) 'PI warns that new ISP interception plans will be illegal', 26 November

Riley, Chris M. & Scott, B. (2009) Deep Packet Inspection. The End of the Internet as We Know It?, Free Press, Florence, MA, [Online] Available at: http://www.freepress.net/files/Deep_Packet_Inspection_The_End_of_the_Internet_As_We_Know_It.pdf (7 February 2013).

The Register (2008) 'The phorm files. All year data pimping news in one place', 29 February.

Wired Magazine Online (2011) 'EU court rules that content owners can't force web filters on ISPs', 24 November.

Wired Magazine Online (2012) 'Social networks don't have to police copyright, rules E', 16 February.

ZDNet UK (2010) 'Virgin media puts CView packet sniffing trial on hold', 30 September.

Christian Fuchs is Professor of Social Media Research at the University of Westminster's Communication and Media Research Institute. He is editor of the journal tripleC – Journal for a Global Sustainable Information Society, co-founder of the ICTs and Society Network, and chair of the European Sociological Association's Research Network 18 – Sociology of Communications and Media Research. His fields of research are Critical Media and Communication Studies, Information Society Studies, Internet & Society, and Media & Society. Website: http://fuchs.uti.at. Address: Communication and Media Research Institute, University of Westminster, Wat ford Road, Northwick Park, Harrow, London HA1 3TP, UK. [email: christian.fuchs@uti.at]
