The Privacy & Security Research Paper Series

Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society

issue #1

The Privacy & Security - Research Paper Series

Edited by Centre for Science, Society & Citizenship
Co-edited by Uppsala University - Department of Informatics and Media
ISSN 2279-7467

Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society

Authors:
Christian Fuchs

Research Paper Number #1
Date of Publication: July 2012

Acknowledgement: 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

All rights reserved.
No part of this publication may be reproduced, distributed or utilized in any form or by any means, electronic, mechanical, or otherwise, without the prior permission in writing from the Centre for Science, Society and Citizenship.
Download and print of the electronic edition for non commercial teaching or research use is permitted on fair use grounds. Each copy should include the notice of copyright.
Source should be acknowledged.
© 2013 PACT

http://www. projectpact.eu

Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society

Christian Fuchs

Abstract:

This research paper analyses societal implications of Deep Packet Inspection (DPI) technologies.

Deep Packet Inspection (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 includes the surveillance of 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. For each company, we have conducted a document analysis of the available files. It focused on the four following aspects:

1) Description and use of the 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 opportunities and problems that can arise in the context of Internet surveillance.

The assessment of societal implications of DPI is based on opinions of security industry representatives, scholars, and privacy advocates that were voiced in white papers, tech reports, research reports, on websites, in press releases, and in news media. The results can be summarized in the form of several impact dimensions:

1. Potential advantages of DPI

2. Net neutrality

3. The power of Internet Service Providers (ISPs) for undermining users' trust

4. Potential function creep of DPI surveillance

5. Targeted advertising

6. The surveillance of file sharers

7. Political repression and social discrimination

The conducted analysis of Deep Packet Inspection (DPI) technologies shows that there is a variety of potential impacts of this technology on society. A general conclusion is that for understanding new surveillance technologies, we do not only need privacy and data protection assessments, but broader societal and ethical impact assessments.

Keywords: *surveillance, DPI, Deep Packet Inspection, Internet surveillance, societal implications, technology assessment, society, information society, Internet Studies*

Short biography of the author/s: Christian Fuchs holds the chair professorship in Media and Communication Studies at Uppsala University's Department of Informatics and Media. He is chair of the European Sociological Association's Research Network 18 – Sociology of Communications and Media Research and co-ordinator of the research project "Social networking sites in the surveillance society" (funded by the Austrian Science Fund FWF). He is co-ordinator of Uppsala University's involvement in the EU FP7 projects "PACT – Public Perception of Security and Privacy: Assessing Knowledge, Collect-

ing Evidence, Translating Research into Action" and "RESPECT – Rules, Expectations & Security through Privacy-Enhanced Convenient Technologies"

1. Introduction

The Wall Street Journal wrote in August 2011 that the French company Amesys, a unit of the firm Bull SA, sold deep packet inspection technologies to Libya, where Gaddafi'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. August 30, 2011). The International Federation for Human Rights and the Ligue des Droits de l'Homme et du Citoyen filed criminal charges against Amesys (FIDH, FIDH and LDH File a Complaint Concerning the Responsibility of the Company AMESYS in Relation to Acts of Torture. October 19, 2011). Similarly, it was reported that the British firm Gamma International sold its FinSpy software to Egyptian security authorities and the Italian firm HackingTeam surveillance software to security agencies in North Africa and the Middle East (*EUobserver.com*, EU Companies Banned From Selling Spyware to Repressive Regimes. October 11, 2011). The Dutch MEP Marietje Schaake commented that the EU must make "the new technologies are not systematically used to repress citizens. […] There are standard lists of military technology banned for export during an embargo on a country. But this is not updated to include online weapons" (*EUobserver.com*, EU Companies Banned from Selling Spyware to Repressive Regimes. October 11, 2011). In September 2011, the EU Parliament passed a resolution suggested by the Austrian MEP Jörg Leichtfried "with 567 votes in favour, 89 against, and 12 abstentions" European Parliament News, Controlling dual-use exports, September 27th, 2011 that bans the export of IT systems that can be used "in connection with a violation of human rights, democratic principles or freedom of speech [...] by using interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of Internet use (e.g. via Monitoring Centres and Lawful Interception Gateways)" (EU regulation no. 1232/2011, European Union General Export Authorisation No EU005, annex IIe) from Europe to certain countries. The export regulation was passed in the form of the EU General Export Authorisation No. EU005 that concerns telecommunications. The regulation banned the export of IT surveillance systems to Argentina, China (including Hong Kong and Macao), Croatia, India, Russia, South Africa, South Korea, Turkey, and the Ukraine.

This report will focus on the analysis of the societal implications of the production and selling of Internet surveillance technologies using Deep Packet Inspection (DPI) by European companies.

There has been an increase and intensification of surveillance after 9/11 (Lyon 2003b, 2007). "Data mining, a technique for deriving usable intelligence from the analysis of massive amounts of computer-accessible information, became increasingly attractive to the government as a resource in the war on terrorism, although its strategic use within business for marketing and risk assessment had long been established" (Gandy 2009, 136).

Also in the European Union the belief that security, understood as "the protection of the individual, but also of the collective self, the nation state", "is a core value threatened by 'global terrorism' has spread" after 9/11 (Bigo 2010, 263). The EU FP6 CHALLENGE research project (The Changing Landscape of European Liberty and Security) concluded that after 9/11 "the framings of the relationship between liberty and security" has been redefined "in favour of control, surveillance, policing, and war" (Bigo, Guild and Walker 2010, 12). European security politics have therefore "been mainly oriented towards the right for governments to strengthen coercive and surveillance security measures" (Bigo 2010, 265f). At the same time, the focus on security and surveillance policies have brought about concerns about the power constituted by the employment of new surveillance technologies and the implications for privacy, data protection, human rights, freedom and equality these technologies have (Ball and Webster 2003; Bigo 2010; Gandy 2009, Jewkes 2011; Lyon 2003a, 2003b; Monahan 2010, Webb 2007). We live in times of heightened attention to surveillance, privacy and data protection. This situation is the context for the study of new surveillance technologies.

2. Deep Packet Inspection Internet Surveillance and the European Security Industry

2.1. Introduction

In 2011, 71% of the individuals aged 16-74 living in the EU27 countries accessed the Internet (within a 3 month period; data source: Eurostat. Internet use by individuals). This shows that Internet use has become an everyday activity for the majority of Europeans. The topic of Internet surveillance matters because it much affects the lives of humans in contemporary societies.

Scholars in surveillance studies and information society studies have stressed the importance of computing for conducting surveillance since more than 20 years. This has resulted in a number of categories that describe the interconnection of computing and surveillance, such as the new surveillance (Marx 1988, 2002), dataveillance (Clarke 1988), the electronic (super)panopticon (Poster 1990), electronic surveillance (Lyon 1994), digital surveillance (Graham and Wood 2007), or the world wide web of surveillance (Lyon 1998).

The Internet processes a huge amount of personal data (see the contributions in Fuchs, Boersma, Albrechtslund and Sandoval 2012). Therefore analysing surveillance-implications of the Internet is an important task, to which this report wants to contribute. This chapter focuses on the analysis of the implications of Internet surveillance technologies that have been produced in Europe.

As data source, we are using a selection of documents that have been published by WikiLeaks in the so-called "SpyFiles" that were published in October 2011. It is a collection of files that document surveillance technologies produced by Western companies (http://wikileaks.org/the-spyfiles.html). On January 23, 2012, there were 287 documents in this archive. The archive consists of digital versions of brochures, cata-

logues, 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, GPS tracking.

WikiLeaks has described the purpose of this archive in the following way: "When citizens overthrew the dictatorships in Egypt and Libya this year, they uncovered listening rooms where devices from Gamma corporation of the UK, Amesys of France, VASTech of South Africa and ZTE Corp of China monitored their every move online and on the phone. Surveillance companies like SS8 in the U.S., Hacking Team in Italy and Vupen in France manufacture viruses (Trojans) that hijack individual computers and phones (including iPhones, Blackberries and Androids), take over the device, record its every use, movement, and even the sights and sounds of the room it is in. Other companies like Phoenexia in the Czech Republic collaborate with the military to create speech analysis tools. They identify individuals by gender, age and stress levels and track them based on 'voiceprints'. Blue Coat in the U.S. and Ipoque in Germany sell tools to governments in countries like China and Iran to prevent dissidents from organizing online. […] trovicor, previously a subsidiary of Nokia Siemens Networks, supplied the Bahraini government with interception technologies that tracked human rights activist Abdul Ghani Al Khanjar. He was shown details of personal mobile phone conversations from before he was interrogated and beaten in the winter of 2010-2011 [...] The Wikileaks Spy Files reveal the details of which companies are making billions selling sophisticated tracking tools to government buyers, flouting export rules, and turning a blind eye to dictatorial regimes that abuse human rights (http://wikileaks.org/the-spyfiles.html).

The archive can be navigated with the help of a world map that allows searching for search for surveillance technologies producers in 21 countries

(http://wikileaks.org/The-Spyfiles-The-Map.html). It is a resource that provides material about companies that produce and sell communications surveillance technologies, including Internet surveillance technologies. The research team at Uppsala University downloaded all documents that were available on February 22nd, 2012, for the category of Internet surveillance for companies located in the EU 27 countries. These were a total of 17 companies from 9 European countries (Czech Republic, Denmark, France, Germany, Hungary, Italy, Netherlands, Poland, UK). We added three companies (Trovicor, Area Spa, 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 analyzed 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 additional 23 documents that

we included in the analysis. For 2 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. The two tables below show a) a list of the analysed companies and the number of documents for each and b) details for all analysed documents and their sources.

The SpyFiles are not covering all European surveillance technology producers, they provide however 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 is 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, 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 three following 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.

The following table gives an overview of the companies that were included in the analysis.

ID	Country	Company name	Number of files in SpyFiles
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

Table 1: A list of the companies included in the analysis

The following table gives an overview of the analysed documents, including their ID in the WikiLeaks Spy Files archive.

Internal ID	WikiLeaks ID (Spy Files archive) / source	Company	Document Description
1	190	Inveatech	Product sheet Lawful Interception System
2_1	37	Qosmos	Presentation "ixDP – Information eXtraction trhough Deep Packet Inspection. Layer 7 Identity Management for Lawful Interception". Patrick Pail. October 1st, 2008.
2_2	50	Qosmos	Presentation "Enabling True Network Intelligence Everywhere. Managing Virtual Identities Across IP Networks". Jean-Philippe Lion. ISS Prague, June 2009.
2_3	58	Qosmos	Presentation "Interception at 100 Gbps and more". Jerome Tollet. October 2011.
2_4	67	Qosmos	Presentation "Dealing with an ever Changing Sea of Application Protocols". Kurt Neumann. October 2011.
2_5	77	Qosmos	Presentation "Boosting Monitoring Centers with IP Metadata". Jerome Tollet. October 2011
2_6	Data source: download from http://www.qosmos.com/	Qosmos	Qosmos ixEngine product sheet
3_1	17	Thales	Presentation "IP Tr@pper". Jean-Philippe Lelievre. ISS Dubai 2007
3_2	40	Thales	Presentation "New Solutions for Massive Monitoring". Jean-Philippe Lelievre. ISS World Europe. Prague. October 3rd, 2008
3_3	Data source: download from http://www.thalesgroup.com	Thales	Thales: C4ISR Products and Solutions for Defence & Security 2011.
3_4	Data source: download from http://www.thalesgroup.com	Thales	Thales: Integrated Security Solutions
3_5	Data source: download from	Thales	Thales Corporate Responsibility Report 2010

	http://www.thalesgroup.com		
4_1	42	Aqsacom	Presentation "Convergence – LI and DR. A Strategic Concept", Alan Dubberley, ISS World 2009, Prague.
4_2	78	Aqsacom	Aqsacom: Lawful Interception is Our Business
4_3	79	Aqsacom	Standards-based lawful interception from Aqsacom
4_4	199	Aqsacom	Aqsacom White Paper: The USA Patriot Act: Implications for Lawful Interception
4_5	200	Aqsacom	Aqsacom White Paper: Lawful Interception for IP Networks
4_6	Data source: download from: http://www.aqsacom.com/	Aqsacom	ADRIS: The Aqsacom Data Retention Intelligence System
5_1	81	Alcatel-Lucent	Alcatel-Lucent 1357 ULIS Unified Lawful Interception Suite (version from 2008)
5_2	Data source: download from: http://www.alcatel-lucent.com	Alcatel-Lucent	Alcatel-Lucent 1357 ULIS Unified Lawful Interception Suite (version from March 2010)
5_3	Data source: download from: http://www.alcatel-lucent.com	Alcatel-Lucent	Alcatel-Lucent Corporate Responsibility 2010 Report
6_1	21	Amesys	Presentation "From Lawful to Massive Interception: Aggregation of Sources"
6_2	92	Amesys	Graph in HQ1-Annakoa
6_3	93	Amesys	casperT System Presentation
6_4	94	Amesys	Caspter-T WiFi Network Interception
6_5	95	Amesys	Amesys – Critical System Architect
6_6	96	Amesys	Cryptowall Mail Protect
6_7	97	Amesys	Cryptowall PC-Protect Professional Ed. (Multi-Volumes)
6_8	98	Amesys	Dumb-O E-mail Interceptor
6_9	99	Amesys	Eagle Glint Operator Manual
6_10	100	Amesys	Eagle Glint Operator Manual
6_11	101	Amesys	SMINT – Tactical Interception Based on EAGLE Core Technology
6_12	102	Amesys	GLINT – Strategic Nationwide Interception Based on EAGLE Core Technology
6_13	103	Amesys	NetTap @ ADSL. Passive Non-Intrusive ADSL Tapping Probe on A Analog Line
6_14	104	Amesys	NetTap @ ADSL. Sonde Passive D'Interception ADSL Sur Ligne Analogique
6_15	105	Amesys	Homeland Security Program: Technical Specification. Public Safety Systems and Passport Network of the Great Libyan Arab Jamahiriya
6_16	106	Amesys	RHF VME WB. Wide Band HF VME Reception Unit
6_17	107	Amesys	RHF VME-TA. 1.5 – 30 MHz Receiver
6_18	185	Amesys	Amesys Comint & Lawful Interception Solutions
7_1	124	Elaman	Elaman Company Information
7_2	124	Elaman	Communications Monitoring, October 2007
7_3	124	Elaman	TSCM – Government Technical Surveillance Counter Measure Solutions

7_4	124	Elaman	CS-2000 High End. High Performance Network Platform
7_5	124	Elaman	P2P Traffic Filter
7_6	124	Elaman	Poseidon Flyer. Portable IP Monitoring System
7_7	124	Elaman	Portable Modem Interception. Munin POTS
7_8	124	Elaman	Portable Modem Interception. Munin POTS
7_9	124	Elaman	POSEIDON. IMC – Internet Monitoring Center Internet Protocol (IP)
7_10	186	Elaman	Elaman Newsletter 01/2011
7_11	187	Elaman	Elaman – The Bridge to Trust and Security
7_12	188	Elaman	Elaman Communications Monitoring Solutions
8_1	44	Datakom	Thomas Fischer, Presentation "One is Enough… Combining Lawful Interception, Mediation & Data Retention in IP-Networks". ISS Prague. June 3-5, 2009.
8_2	Data source: download from: http://www.datakom.de	Datakom	Service & Qualität. Mess-Dienstleistungs-Portfolio.
8_3	Data source: download from: http://www.datakom.de	Datakom	ICC-Services
9	Data source: download from: http://www.trovicor.com	Trovicor	trovicor: Code of Business Conduct, 2010-09-13
10_1	24	Digitask	Michael Thomas, presentation "Remote Forensic Software"
10_2	25	Digitask	Thomas Kröckel, presentation "Future Challenges in the Lawful Interception of IP based Telecommunication"
10_3	45	Digitask	Tobias Hain, presentation "Challenges in Intercepting WiFi"
10_4	46	Digitask	Michael Thomas, presentation "Remote Forensic Software"
10_5	Data source: WikiLeaks: http://wikileaks.org/wiki/Skype_and_SSL_Interception_letters_-_Bavaria_-_Digitask	Digitask	Digitask: Leistungsbeschreibung für Bayerisches Staatsministerium der ustiz (Digitask: product description for the Bavarian State Ministry of Justice)
11_1	191	Ipoque	Supported Protocols and Applications
11_2	Data source: download from: http://www.ipoque.com	Ipoque	Data Sheet: DPX Network Probe
11_3	Data source: download from: http://www.ipoque.com/	Ipoque	Data Sheet: Net Reporter
11_4	Data source: download from: http://www.ipoque.com/	Ipoque	Data Sheet: PACE (Protocol & Application Classification Engine)
11_5	Data source: download from: http://www.ipoque.com/	Ipoque	Klaus Mochalski and Hendrik Schulze, White Paper "Deep Packet Inspection. Technology, Applications & Net Neutrality".
11_6	Data source: download from: http://www.ipoque.com/	Ipoque	Klaus Mochalski, Hendrik Schulze and Frank Stummer, White Paper "Copyright Protection in the Internet"
12_1	53	Utimaco Safeware	Dirk Schrader, presentation "What LI Can Learn from Anti-SPAM, Anti-Virus, IDS/IPS, and DPI Technologies"
12_2	54	Utimaco Safeware	Martin Stange, presentation "Building Blocks of a Carrier Grade Data Retention Solution"
12_3	Data source: download from:	Utimaco Safe-	Utimaco LIMS: Lawful Interception of Tele-

	http://lims.utimaco.com	ware	communication Services
12_4	Data source: download from: http://lims.utimaco.com	Utimaco Safe-ware	Utimaco LIMS: Lawful Interception in the Digital Age: Vital Elements of an Effective Solution
13	32	NETI	Zoltán Peller and Zsolt Köhalmi, presentation "Data in a Haystack. Monitoring Systems with Advanced Workflow Management"
15	205	Innova	Innova Investigation Instruments
16_1	144	IPS	IPS Visionary Intelligence
16_2	145	IPS	IPS GENESI Monitoring Centre
16_3	146	IPS	IPS Visionary Intelligence
17_1	29	Group 2000	Data Retention Challenges
17_2	30	Group 2000	LIMA Lawful Interception: Lawful Interception in the Evolving World of Telecom
17_3	48	Group 2000	Lawful Interception: The Bigger Picture
17_4	Data source: download from: http://www.group2000.eu	Group 2000	Network Forensics: Lawful Interception for Broadband
17_5	Data source: download from: http://www.group2000.eu	Group 2000	Network Forensics: LIMA DRS Data Retention
17_6	Data source: download from: http://www.group2000.eu	Group 2000	LIMA Management System: The Complete Management Solution for Lawful Interception
17_7	Data source: download from: http://www.group2000.eu	Group 2000	Network Forensics: LIMA DPI Monitor
17_8	Data source: download from: http://www.group2000.eu	Group 2000	Supported Protocols and Applications
18	35	Pine Digital Security	ETSI's IP Handover Standards
19	Data source: download from: http://projects.wsj.com/surveillance-catalog	Gamma Group	FinFisher: Governmental IT Intrusion and Remote Monitoring Solutions
20_1	16	Telesoft Technologies	Keith Driver, presentation "Intelligent Probing for Intelligence and LI Applications"
20_2	39	Telesoft Technologies	Keith Driver, presentation "Real Time Intercept from Packet Networks, Challenges and Solutions"
20_3	208	Telesoft Technologies	HINTO Network Independent CDR Application Note
20_4	Data source: download from: http://ww.telesoft-technologies.com	Telesoft Technologies	White Paper "Using Hardware Accelerated 10-40 Gb/s Packet Analysis in IMS Policy Applications"

Table 2: A list of the 89 files included in the analysis

A first view of the material showed that one particularly important term in the context of Internet surveillance is Deep Packet Inspection (DPI), which is an Internet surveillance technology. In order to understand what it is, we need to understand what the Open-Systems Interconnection (OSI) Model is. For the transmission of data within and across computer networks, communication standards are needed. Computer networks consist of software applications, computers, and network architecture. The communication process can be modelled with the help of three layers:

1) The network layer "is concerned with the exchange of data between a computer and the network to which it is attached" (Stallings 1995, 490)
2) The transport layer is logic that assures "that all the data arrive at the destination application and that the data arrive in the same order in which they were sent" (Stallings 1995, 490f)
3) The application layer "contains the logic needed to support the various user applications. For each different type of application, such as file transfer, a separate module is needed that is peculiar to that application" (Stallings 1995, 491).

One standard model of computer network data transmission is the Open-Systems Interconnection (OSI) Model. It consists of seven levels.

	Application layer	This layer provides access of applications to the network. The software applications reside at this level, such as browsers, e-mail programmes, FTP clients, chat software, voice over IP software, file sharing software, etc.	Application
	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-	
	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.	
	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 organised in several sequential steps.	Host-to-host/Transport (TCP)
	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 is transported from the source network to the destination network.	Internet (IP)
	Data link layer	This layer secures the reliable transfer of	Network access

		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.	
	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

Table 3: The layers of the OSI Reference Model and the TCP/IP Protocol (source: Stallings 1995, 2006; Comer 2004)

In Internet communication, the OSI Reference Model is translated into the TCP/IP Protocol that consists of five layers. Each device (like a computer or a printer) in a network connected to the Internet has a specific IP address, which is a unique 32 bit long identifier (such as 170.12.252.3). 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 Google, he enters search keyword into the Google search box. This is at the application level.

At the TCP level, the Transmission Control Protocol (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. TCP provides a reliable transport service. "After requesting TCP to establish a connection, an application program can use the connection to send or receive data: TCP guarantees to deliver the data in order without duplication. Finally, when the two applications finish using a connection, they request that the connection be terminated. TCP on one computer communicates with TCP on another computer by exchanging messages. All messages from one TCP to another use the TCP segment format, including messages that carry data, acknowledgements, and window advertisements, or message used to establish and terminate a connection" (Comer 2004, 386).

At the IP level, the IP address of the destination is determined as well as the routing over the Internet are determined. The Internet Protocol (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, 301). At the lower levels, the data is transmitted. The data is 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 that is than in the same way sent back to the user, who requested the information.

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

Table 4: A TCP/IP packet

Table 4 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, 666). The payload is "the data being carried in a packet" (Comer 2004, 667), the header contains data like the network address of source and destination. In the TCP/IP protocol 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, 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, 145). Deep Packet Inspection technologies "are capable of analysing the actual content of the traffic that is flowing" (Jason 2011, 118). "DPI allows network operators to scan the payload of IP packets as well as the header. […] It enables the network operator to analyze the datagrams passing through the network in real-time and discriminate among them according to their payload" (Bendrath and Mueller 2011, 1144). "Deep Packet Inspection ('DPI') is a computer network filtering technique that involves the inspection of the contents of packets as they are transmitted across the network. DPI is sometimes referred to as 'complete packet inspection'" (EPIC, Deep Packet Inspection and Privacy. http://epic.org/privacy/dpi/)

Parsons (2008) distinguishes between Shallow Packet Inspection, Medium Packet Inspection and Deep Packet Inspection technologies. Shallow Packet Inspection (SPI) technologies "examine the packet's header information" (Parsons 2008, 6; see also Daly 2010), the inspect data at the OSI layers 1-3. Examples are firewalls that scan source and destination IP addresses that are defined at layer 3 of the OSI (network layer) and TCP/IP (Internet/IP level) models. They can block data that comes from certain IP addresses (which are e.g. considered as distributing spam or viruses). Medium Packet Inspection (MPI) technologies can analyse data on the OSI layers 1-6. This includes the presentation layer of the OSI model, at which file formats are de-

fined. MPI technologies can e.g. block certain file types or be used for network management (prioritization of the transmission of certain file types). “MPI technologies can prioritize some packets over others by examining the application commands that are located within the application layer and the file formats in the presentation layer” (Parsons 2008, 8). Parsons defines Deep Packet Inspection technologies as surveillance methods that can “identify the origin and content of each packet of data” (Parsons 2008, 8). They can monitor data at the OSI layers 1-7. Deep packet inspection (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 includes the surveillance of content data.

2.2. The Analysed Companies’ Internet Surveillance Technologies

Annex A provides a more detailed analysis of 20 European security technologies Internet surveillance technologies. For each company in the sample, the following information is outlined:

* Place of business
* Website
* Self-description of the company’s activities
* Analysis: this section of each security company’s discussion gives an overview of which Internet surveillance technologies the specific company creates and how it views the usefulness and purpose of these technologies according to public statements (website, press releases, news articles).

The analysed security companies are the following ones:

1. Inveatech
2. Qosmos
3. Thales
4. AQSACOM
5. Alcatel-Lucent
6. Amesys
7. Elaman
8. Datakom
9. trovicor
10. Digitask
11. ipoque
12. Utimaco
13. NETI
14. Area Spa
15. Innova
16. IPS
17. Group 2000

18. Pine Digital Security
19. Gamm Group
20. Telesoft Technologies

2.3. Assessment of Deep Packet Inspection Internet Surveillance

DPI is a relatively new and not much analysed topic in the social sciences. A title search for DPI OR "deep packet" in the Social Sciences Citation Index (conducted on February 17, 2011) produced 9 results, of which only 2 were really about DPI. A similar search in the database Communications and Mass Media Complete (conducted on February 17, 2011) brought 10 results, of which 3 focused on DPI.

Bendrath and Mueller (2011) list seven areas, where DPI affects society: network security (viruses, Trojans, worms, etc), bandwidth management, governmental surveillance, content regulation (blocking, censorship), copyright enforcement (file sharing), ad injection.

For assessing the impact of DPI, the Uppsala University research team conducted a search for academic articles, tech reports, and assessments. We analysed these documents. The results can be summarized in the form of several impact dimensions.

1. Potential advantages of DPI
2. Net neutrality
3. The power of Internet Service Providers (ISPs) for undermining users' trust
4. Potential function creep of DPI surveillance
5. Targeted advertising
6. The surveillance of file sharers
7. Political repression and social discrimination

2.3.1. Potential Advantages of DPI

Cooper (2011, 144) argues that the analysis of Internet packets at TCP/IP layer 3 (destination and source IP addresses) has always been used by ISPs "to route packets to their destinations, and thus it would be difficult to argue that their continued use creates some new privacy risk". Privacy problems could be related to payload data (TCP/IP layer 5). "Payloads often contain application headers, and many of these headers – such as the HTTP version type and content encodings cited earlier – are fairly innocuous from a privacy perspective. However, other kinds of headers can reveal much more sensitive information about a person's Internet activities, such as URLs, email recipient addresses, user names, addresses, and many other kinds of data" (Cooper 2011, 144).

The advantages that are generally mentioned on the side of ISPs are the opportunities for bandwidth management and the creation of personalized for-profit services: "ISPs, meanwhile, see promising opportunities of many kinds in the growth of DPI. The technology can provide them with a powerful tool to address constantly evolving challenges in managing network congestion and security threats. It can provide in-

sight into how their networks are being used, allowing them to make more informed decisions about network upgrades and architecture. And perhaps most importantly, DPI is among a set of tools that can provide IPS with new revenue streams, whether by funnelling data about users to advertisers, selling expedited delivery to content providers, or levying extra fees on heavy network users" (Cooper 2011, 140). "Internet traffic has increasingly involved such data-rich applications as voice and streaming video. Not only are these quite demanding of bandwidth, these types of communications do not function well if subject to delays. One way carriers seek to solve the problem is by examining packets and determining traffic priorities; DPI would allow the carriers to do so" (Landau 2010, 141).

ipoque stresses in a white paper (#11_5) that DPI is used for different purposes, including spam filters, virus filters as well as bandwidth and network management that makes efficient use of networks by prioritizing the transmission of different file types. Different protocols and different applications make different use of the Internet. So e.g. VoIP (such as Skype) has a low use of the network, whereas file sharing in peer-to-peer networks makes heavy use of the Internet.

2.3.2. 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). "During the explosive rise of the Internet, one fundamental principle governed: All users and all content were treated alike. The physical network of cables and routers did not know or care about the user or the content. The principle of non-discrimination, or 'Net Neutrality', allowed users to travel anywhere on the Internet, free from interference" (Riley and Scott 2009, 3). "The connection between DPI and net neutrality became clear in 2007, when it was made public that Comcast used a SandVine DPI monitoring systems to disrupt peer-to-peer traffic, which resulted in a lawsuit before the US Federal Communication Commission (FCC)" (Bendrath and Mueller 2011). "In the USA, the cable operator Comcast began to block peer-to-peer (P2P) data transfers for its users using DPI. This resulted in the Federal Communications Commission (FCC) ordering Comcast to 'end discriminatory network management practices', since it had 'unduly interfered with Internet users' right to access the lawful Internet content and to use the applications of their choice'" (Daly 2010).

The FCC says that "reasonable network management", which is network management that is "tailored to achieving a legitimate network management purpose" (FCC 2010, 48) and for which DPI may be used, is no problem. Unreasonable discrimination of users that violates net neutrality would e.g. be the discrimination of certain applications (such as VoIP), hindering users to access certain content, services or applications, or the slow down of a service or website that a ISP disagrees with (FCC 2010, 42). The FCC (2010, 43) also says that "pay for priority" is likely to violate net neutrality.

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 (like big companies) use a fast Internet and everyday people, who do not have so much money, a slow Internet. "Indeed, corporate control over what information users create, disseminate and receive could also entail access to content or programmes which are not commercially lucrative is restricted only to those willing to pay more to the ISP to access it, or not available at all" (Daly 2010).

Lawrence Lessig and Robert W. McChesney argue that the net neutrality debate is a discussion about the fundamental qualities of the Internet: "Will we reinstate net neutrality and keep the Internet free? Or will we let it die at the hands of network owners itching to become content gatekeepers? […] The current legislation, backed by companies such as AT&T, Verizon and Comcast, would allow the firms to create different tiers of online service. They would be able to sell access to the express lane to deep-pocketed corporations and relegate everyone else to the digital equivalent of a winding dirt road. Worse still, these gatekeepers would determine who gets premium treatment and who doesn't" (Lawrence Lessig and Robert W. McChesney, No Tolls on the Internet. *The Washington Post*. June 8, 2006).

A tiered Internet monitored with the help of DPI could also result in "an encryption arms race in which disfavoured applications would encrypt all traffic to evade identification by DPI. Such an outcome would render the congestion-reduction purpose of DPI ineffective" (Riley and Scott 2009, 8)

2.3.3. The Power of ISPs for Undermining Users' Trust

Heavy use of DPI by ISPs may undermine trust that users have in the network and ISPs and this can result in self-censorship and inhibition of users (Cooper 2011, 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. Neither "Google nor any other service provider is as capable as an ISP of comprehensively monitoring the entirety of each individual subscriber's online activities. Every one of a subscriber's packets, both sent and received, must pass through the ISP's facilities. What separates ISPs from other service providers is the potential for their gaze over their subscribers to be omniscient" (Cooper 2011, 147). ISPs have with the help of DPI the power to monitor the entire Internet usage of subscribers. The discussions about the use of DPI for that were presented in this report have frequently involved discussions

about the role of ISPs, which shows that they are crucial actors in Internet surveillance and that they hold high 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. Heavy use of encryption can also slow down the speed of computer networks.

Parsons warns that with the help of DPI it is "possible to construct vast social network maps" (Parsons 2008, 12) because the technology allows to identify the source and destination (e.g. email-addresses or user names on social media like Facebook or Twitter) as well as the content of each online communication.

Bendrath and Mueller (2012, 1148) make an analogy between an ISP and a postal worker in order to show how DPI can potentially result in privacy violations: "Now imagine a postal worker who […]

* Opens up all packets and letters;
* Reads the content;
* Checks it against databases of illegal material and when finding a match sends a copy to the police authorities;
* Destroys letters with prohibited or immoral content;
* Sends packages for its own mail-order services to a very fast delivery truck, while the ones from competitors go to a slow, cheap sub-contractor.

Imagine also that the postal worker could do this without delaying or damaging the packets and letters compared to his (former, now fired) daydreaming colleague. This is what DPI technology is capable of. […] Such a postal system […] invades the privacy of communications and introduces opportunities for regulation and censorship whole increasing the feasibility of imposing intermediary responsibility on IPSs".

"DPI is a letter carrier who reads all your mail, listens to all your calls, follows you as you browse downtown and in the mal, notes your purchases, listens in as you ask questions of the research librarian, and watches over your shoulder as you read the daily paper – and then correlates all that information in real time" (Landau 2010, 220).

The question that arises is if such data processing is "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed" (*European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* 95/46/EC, article 6 (c)).

2.3.4. Potential Function Creep of DPI Surveillance

The notion of the surveillance creep was introduced by Gary Marx: "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. [...] The new forms of social control tend to be subtle, invisible, scattered, and involuntary. They are often not defined as surveillance, and many people, especially those born after 1960, are barely conscious of them" (Marx 1988, 2f). Surveillance creep is "the expansion into new domains of software or a surveillance system, and the ways that new functions are constantly found for surveillance technologies and practices" (Lyon 2007, 201). "Personal data, collected and used for one purpose and to fulfil one function often migrate to other ones that extend and intensify surveillance and invasions of privacy beyond what was originally understood and considered socially, ethically and legally acceptable. [...] Function creep usually happens quietly, unobtrusively, as a bit of administrative convenience" (Surveillance Studies Network 2010, 9).

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, etc). "Another distinguishing feature of ISPs' use of DPI is the potential for mission creep: having DPI equipment that was installed for one purpose used for multiple new purposes over time" (Cooper 2001, 148f). An important aspect here is that DPI can be employed "mostly invisibly on the network" (Cooper 2001, 149), thereby enabling invisible surveillance creep.

2.3.5. 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, 180).

"Web-based advertising companies have for many years used web-based technologies (such as cookies) to track the sites that users visit, allowing the companies to compile profiles of users' behaviour for advertising purposes. DPI creates that same possibility for ISPs by allowing them to identify the websites that their subscribers are visiting, the content of those sites, and the other kinds of applications and data that subscribers are using. ISPs or their advertising partners can extract this information from individual packets and compile it into profiles that can later be used to show targeted ads to subscribers as they surf the web" (Cooper 2011, 151).

On Facebook, targeted advertising is the standard option and there is no opt-in to this type of advertising. This circumstance was part of 22 complaints that the initiative "Europe versus Facebook" filed against Facebook. As Facebook Europe is located in Ireland, the Irish data protection authorities are in charge of such claims. After auditing Facebook, the Data Protection Commissioner of Ireland (2011) published an audit report. It wrote that Facebook needs to implement "an enhanced ability for users to make their own informed choices based on the available information" (42). "From the privacy perspective therefore it would be a far better position for users if there were no default settings upon sign-up. A user then would be asked via a process

what their broad preferences are with settings that reflect such broad preferences and a consequent ability for the user to refine those settings all of which should be available from one place" (40). "There are limits to the extent to which user-generated personal data can be used for targeted advertising. Facebook must be transparent with users as to how they are targeted by advertisers" (60).

The Data Protection Commissioner of Ireland's report made clear that targeted advertising is not unproblematic in respect to privacy violations and that special precautions need to be taken in order to protect consumer privacy on the Internet.

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. February 29, 2008.

http://www.theregister.co.uk/2008/02/29/phorm_roundup). In April 2008, the British Information Commissioner's Office issued a statement saying that Phorm's DPI-based advertising system Webwise needs to be implemented as opt-in system in order to comply to British communications regulations: "Phorm has developed a system where, with the cooperation of an individual's ISP they can profile the addresses and certain content of websites visited by users and then use that information to match that user against predefined broad advertising categories. […] When a user visits a website that has an agreement with Phorm their user ID is recognised and Phorm will use the broad advertising categories associated with that ID to enable relevant advertising channel to be shown on the website. […] Regulation 7 of PECR [Privacy and Electronic Communications Regulations] will require the ISP to get the consent of users to the use of their traffic data for any value added services. This strongly supports the view that Phorm products will have to operate on an opt in basis to use traffic data as part of the process of returning relevant targeted marketing to internet users"
(http://collections.europarchive.org/tna/20080422094853/http://ico.gov.uk/Home/about_us/news_and_views/current_topics/phorm_webwise_and_oie.aspx).

In a letter to the British Information Commissioner, the Foundation for Information Policy Research (FIPR) warned about potential privacy violations of Phorm's system: "The provision of this service depends on classifying Internet users to enable advertising to be targeted on their interests. Their interests are to be ascertained for this purpose by scanning and analysing the content of traffic between users and the websites they visit. This activity involves the processing of personal data about Internet users. That data may include sensitive personal data, because it will include the search terms entered by users into search engines, and these can easily reveal information about such matters as political opinions, sexual proclivities, religious views,

and health. [...] Classification by scanning in this way seems to us to be highly intrusive. We think that it should not be undertaken without explicit consent from users who have been given particularly clear information about what is liable to be scanned. Users should have to opt in to such a system, not merely be given an opportunity to opt out. We believe this is also required under European data protection law; failure to establish a clear and transparent 'opt-in' system is likely to render the entire process illegal and open to challenge in UK and European courts" (http://www.fipr.org/080317icoletter.html).

The inventor of the World Wide Web, Tim Berners-Lee, expressed his opposition to Phorm's DPI-based targeted advertising system: "The access by an ISP of information within an internet packet, other than that information used for routing, is equivalent to wiretapping a phone or opening sealed postal mail. The URLs which people use reveal a huge amount about their lives, loves, hates, and fears. This is extremely sensitive material. People use the web in crisis, when wondering whether they have STDs, or cancer, when wondering whether they are homosexual and whether to talk about it, to discuss political views which may be abhorrent, and so on. [...] The power of this information is so great that the commercial incentive for companies or individuals misuse it will be huge, so it is essential to have absolute clarity that it is illegal. The act of reading, like the act of writing, is a pure, fundamental, human act. It must be available without interference or spying" (Berners-Lee, Tim. 2009. *No Snooping*. http://www.w3.org/DesignIssues/NoSnooping.html).

Because of the Phorm case, the European Commission opened an infringement proceeding against the UK in order to see if the UK has correctly implemented the EU's ePrivacy and data protection rules. "Since April 2008, the Commission has received several questions from UK citizens and UK Members of the European Parliament concerned about the use of a behavioural advertising technology known as 'Phorm' by Internet Service Providers in the UK. Phorm technology works by constantly analysing customers' web surfing to determine users' interests and then deliver targeted advertising to users when they visit certain websites. In April 2008, the UK fixed operator, BT, admitted that it had tested Phorm in 2006 and 2007 without informing customers involved in the trial. BT carried out a new, invitation-based, trial of the technology in October-December 2008. BT's trials resulted in a number of complaints to the UK data protection authority – the Information Commissioner's Office (ICO) and to the UK police. [...] the Commission has concerns that there are structural problems in the way the UK has implemented EU rules ensuring the confidentiality of communications. [...] Under UK law, which is enforced by the UK police, it is an offence to unlawfully intercept communications. However, the scope of this offence is limited to 'intentional' interception only. Moreover, according to this law, interception is also considered to be lawful when the interceptor has 'reasonable grounds for believing' that consent to interception has been given. The Commission is also concerned that the UK does not have an independent national supervisory authority dealing with such interceptions. [...] The EU Directive on privacy and electronic communications requires EU Member States to ensure confidentiality of the communica-

tions and related traffic data by prohibiting unlawful interception and surveillance unless the users concerned have consented (Article 5(1) of Directive 2002/58/EC). The EU Data Protection Directive specifies that user consent must be 'freely given specific and informed' (Article 2(h) of Directive 95/46/EC). Moreover, Article 24 of the Data Protection Directive requires Member States to establish appropriate sanctions in case of infringements and Article 28 says that independent authorities must be charged with supervising implementation. These provisions of the Data Protection Directive also apply in the area of confidentiality of communications" (http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570). In autumn 2010, the European Commission decided to take this case to the Court of Justice of the EU (*Brand Republic News Releases*, EU to Take UK to Court over Internet Privacy Rules. October 4, 2010).

A Phorm-initiated privacy impact assessment of Webwise concluded that information systems require informed consent, but confirmed that although Phorm was working on respecting users' privacy, it would not intend to implement an opt-in system because "the market default for cookie-based consent systems is opt-out" and that "users will be given proper notice" (80/20 Thinking, *Privacy Impact Assessment for Phorm*. http://www.phorm.com/assets/reports/Phorm_PIA_Final.pdf, 19).

Andrew McStay (2011) interprets Phorm's Webwise as the third type of online behavioural advertising. In the first form, a web platform collects user data on its own site in order to target ads. In the second form, a second party runs an advertising network (such as DoubleClick) that collects and networks data from different websites in order to target ads. In the third form, deep-packet inspection "scans packets of data that passes through the gateway [of an ISP] and marries suitable data with relevant advertising" (McStay 2011, 312).

"Google may track your searches, your travel (Google Maps), and your appointments (Google Calendar), but the company's ability to do so is limited by the number of different Google services of which you avail yourself. If you object to Google's privacy policies, you can choose to use other services. By contrast, your ISP knows everything you do online. […] A single ISP will know what you are browsing, what your email says, VoIP, and so on. In a matter of days, possibly even hours, an ISP using DPI can develop a remarkably detailed dossier on a person" (Landau 2010, 220).

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.

2.3.6. The Surveillance of File Sharers

DPI can be used for detecting or blocking illegal file sharing (see the discussion in #11_6). "Since 2004, the European music industry has tried to use the courts to force ISPs to set up filtering technology that would detect and block copyrighted music automatically. [...] The DPI products of one company, Audible Magic, were promoted by the music industry as a suitable solution to the problem" (Bendrath and Mueller 2011, 1154).

The Belgian music industry association SABAM (Société d'Auteurs Belge – Belgische Auteurs Maatschappij) sued the ISP Scarlet and requested that it installs Audible Magic for copyright surveillance (Bendrath and Mueller 2011). In Ireland, EMI, Sony, Warner and Universal wanted to require Eircome to implement a similar system (ibid). SABAM also wanted to require the Belgian social networking site Netlog to install filtering systems that prevent copyright violations. In the Scarlet vs. SABAM case, in 2011 the "European Court of Justice has ruled that content owners cannot force Internet service providers to engage in large scale filtering and blocking of copyright-infringing material online. [...] It argued that blocking general access to P2P sites would be unfair on a provider, affecting its freedom to conduct business and requiring the ISP to 'install a complicated, costly, permanent computer system at its own expense'. The court also said that a filter would infringe upon the rights Internet users have to privacy and information protection" (Wired Magazine Online, *EU Court Rules that Content Owners Can't Force Web Filters on ISPs*. November 24, 2011. http://www.wired.co.uk/news/archive/2011-11/24/eu-rules-on-filtering).

In the Netlog vs. SABAM case, the European Court of Justice confirmed the Scarlet rule: "Netlog protested at having to install and maintain a costly computer system at its own expense for the benefit of another industry entirely, and took the case to the European Court of Justice, which said 'such an injunction would result in a serious infringement of Netlog's freedom to conduct its business'. However, that wasn't the only issue that the court took with SABAM's demands. It added: 'The filtering system may also infringe the fundamental rights of its service users – namely their right to protection of their personal data and their freedom to receive or impart information'. The court's conclusion? 'In adopting an injunction requiring the hosting service provider to install such a filtering system, the national court would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other'" (Wired Magazine Online, *Social Networks Don't Have to Police Copyright, Rules EU*. February 16, 2012. http://www.wired.co.uk/news/archive/2012-02/16/eu-social-networks-copyright).

In 2009, the British ISP Virgin Media announced the use of "deep packet inspection with the controversial Detica CView technology, which will ascertain levels of illegal music file sharing across the Virgin network. The trial will see Virgin monitoring 40

per cent of its customers, but none of these customers will be informed whether they are being checked out. Virgin insist that any data accumulated will be anonymous. The technology used is called CView, created by a company called Detica and based on the same technology that powered the controversial Phorm. CView looks at Web traffic, spots peer-to-peer packets, and takes a look inside. It then collects data if the files being shared are considered to be infringing copyright, based on information from record companies" (CNET UK, *Virgin Media and CView to Rifle Through Your Packets*. November 27, 2009. http://crave.cnet.co.uk/software/virgin-media-and-cview-to-rifle-through-your-packets-49304424). Privacy International argues that this case constitutes privacy violations and is based on the assumption that Virgin subscribers are criminals, which would reverse the presumption of innocence:

"Under the Privacy and Electronic Communications (EC Directive) Regulations (PECR) and the Regulation of Investigatory Powers Act (RIPA) as well as the European ePrivacy Directive, that interception and processing of communications requires either explicit informed consent from all parties or a warrant. […] We are further concerned that such a system generates a paradigm shift with regards to the balance of justice. Virgin Media's plans assume that all consumers are guilty of copyright infringement until their communications data proves otherwise – whereas the onus should be on the injured parties to provide their own evidence that an infringement has occurred" (Privacy International, *PI Warns that New ISP Interception Plans Will Be Illegal*. November 26, 2009. https://www.privacyinternational.org/article/pi-warns-new-isp-interception-plans-will-be-illegal). In early 2010, the European Commission announced that it would closely monitor Virgin Media's planned trial, later in the same year Virgin Media announced that it put its plans on hold (ZDNet UK, *Virgin Media Puts CView Packet Sniffing Trial on Hold*. September 30, 2010. http://www.zdnet.co.uk/news/security-threats/2010/09/30/virgin-media-puts-cview-packet-sniffing-trial-on-hold-40090353/)

Since 2007, Australia, Canada, the EU, Japan, Jordan, Mexico, Morocco, New Zealand, South Korea, Singapore, Switzerland, the United Arab Emirates, and the USA have engaged in negotiation about an Anti-Counterfeiting Trade Agreement (ACTA). The Electronic Frontier Foundation argues that it was planned to create a new legal regimes that encourages "Internet Service Providers […] to identify and remove allegedly infringing material from the Internet", "mandatory network-level filtering by Internet Service Providers", and a rule that ISPs have "to terminate citizens' Internet connection on repeat allegation of copyright infringement" (Electronic Frontier Foundation, *Anti-Counterfeiting Trade Agreement. What is ACTA?* https://www.eff.org/issues/acta). 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 case that individuals or organisations three times send undesirable content bans them from further use of the postal service and therefore from a fundamental means of human communication.

The discussed examples show that there are DPI technologies, such as Audible Magic and CView, that can be used by ISPs to monitor the Internet so that illegal file sharing is detected. There are examples, where the content industry has tried to legally enforce the use of these Internet surveillance technologies by ISPs. The European Court of Justice has ruled that such measures violate Internet users' right to privacy and information protection and ISPs' freedom to conduct business. An additional argument was that the automatic surveillance of traffic by ISP in order to detect illegal file sharing would reverse the presumption of innocence and assume that all Internet users are criminals.

2.3.7. 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. It is not exactly known how China's "Great Firewall" that filters and allows to censor Internet content, exactly works. Some observers say that it "is believed also to involve deep packet inspection. But China appears to be developing this capability in a more decentralized manner, at the level of its Internet service providers rather than through a single hub, according to experts" (*Wall Street Journal Online*, Iran's Web Spying Aided by Western Technology. June 22, 2009, http://online.wsj.com/article/SB124562668777335653.html).

Annex A shows that security companies tend to argue that DPI can help fighting crime (such as child pornography or illegal file sharing) and terrorism. From a European data protection perspective, some problems may however arise. Collection and automatic analysis of content data with the help of DPI may contain the filtering, storage and analysis of sensitive data. The European Data Protection Directive says that "Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" (*European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, article 8).

The EU has in the *Proposal of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation*) suggested to amend this passage: "The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited" (article 9).

In both cases are political opinions considered as sensitive data. Algorithmic analysis and collection can semantically not perfectly distinguish between sensitive and non-sensitive data. The use of DPI for targeted advertising and by governments faces the risk that sensitive data of users are being monitored. The examples about the al-

leged 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. The claim that DPI surveillance can help fighting crime and terrorism needs therefore to be complemented by the warning that DPI Internet surveillance at the content level of Internet data (the application level in the TCI/IP layer model) can bring about privacy violations and the processing of sensitive data and thereby result in repression against and discrimination of certain groups in society.

Annex A shows that 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). Gamma Group (UK).

2.3.7.1. Area Spa (Italy), Qosmos (France), Utimaco (Germany)

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, also technologies by Qosmos (France) and Utimaco (Germany) seem according to news reports to have been used: "Area is using equipment from American and European companies, according to blueprints and other documents obtained by Bloomberg News and the person familiar with the job. The project includes Sunnyvale, California-based NetApp Inc. (NTAP) storage hardware and software for archiving e-mails; probes to scan Syria's communications network from Paris-based Qosmos SA; and gear from Germany's Utimaco Safeware AG (USA) that connects tapped telecom lines to Area's monitoring-center computers" (*Bloomberg*, Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear. November 4, 2011. http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html).

"When the system is complete, Syrian security agents will be able to follow targets on flat-screen workstations that display communications and Web use in near-real time alongside graphics that map citizens' networks of electronic contacts, according to the documents and two people familiar with the plans. Such a system is custom-made for repression, says Mark Dubowitz, executive director of the Washington-based Foundation for Defense of Democracies, which promotes tighter sanctions against Syria. 'Any company selling monitoring surveillance technology to the Assad regime is complicit in human rights crimes,' he says. […] When Bloomberg News contacted Qosmos, CEO Thibaut Bechetoille said he would pull out of the project. 'It was not right to keep supporting this regime,' he says. The company's board decided about four weeks ago to exit and is still figuring out how to unwind its involvement,

he says. The company's deep- packet inspection probes can peer into e-mail and reconstruct everything that happens on an Internet user's screen, says Qosmos's head of marketing, Erik Larsson" (ibid.).

"The Syrian secret service appears to be monitoring the country's protest movement using technology from the German firm Utimaco, based in Oberursel, a suburb of Frankfurt. Contacted by Spiegel reporters on Friday, the company said it had sold no products directly to Syrian Telecom, the regime-owned telecommunications provider. The company had instead delivered products to the Italian firm Area, with which is has conducted business for years. The company said it could not confirm whether Area had then resold goods to Syrian dictator Bashar Assad's regime" (*Spiegel Online International,* Is Syria Monitoring Protesters with German Technology? November 8, 2011).

So there were media reports that said that Area Spa started installing Internet surveillance technologies in Syria, a country where hundreds of members of the political opposition have been killed by the government that tries to repress protests that started in January 2011. "Employees of Area SpA, a surveillance company based outside Milan, are installing the system under the direction of Syrian intelligence agents, who've pushed the Italians to finish, saying they urgently need to track people, a person familiar with the project says. The Area employees have flown into Damascus in shifts this year as the violence has escalated, says the person, who has worked on the system for Area. […] Area is using equipment from U.S. and European companies, according to blueprints and other documents obtained by Bloomberg and the person familiar with the job. The project includes Sunnyvale, Calif.-based NetApp Inc. storage hardware and software for archiving e-mails; probes to scan Syria's communications network from Parisbased Qosmos SA; and gear from Germany's Utimaco Safeware AG that connects tapped telecom lines to Area's monitoring-centre computers. […] When the system is complete, Syrian security agents will be able to follow targets on flat-screen workstations that display communications and web use in near-real time alongside graphics that map citizens' networks of electronic contacts, according to the documents and two people familiar with the plans. Such a system is custom made for repression, says Mark Dubowitz, executive director of the Washington based Foundation for Defense of Democracies […] Area, a privately held company that got its start in 1996 furnishing phone taps to Italian law enforcement, has codenamed the system 'Asfador,' a nod to a Mr. Asfador who cold-called the company in 2008 asking it to bid on the deal, according to one person knowledgeable about the project" (*The Calgary Herald*, Italian Firm Helping Syria Spy on E-Mails. System Made for Repression, says Think-Tank. November 5, 2011).

According to media reports, "Area chief executive Andrea Formenti says he can't discuss specific clients or contracts, and that the company follows all laws and export regulations" (ibid.). Later, Area's CEO was quoted in the press saying that the surveillance project has not been activated: "In response, Area SpA's CEO, Andrea Formenti, was quoted in Italy's Corriere della Sera newspaper this month announcing that his company had no employees in Syria and that the project had not made any progress

in the last two months. […] 'The interception system has never been activated and cannot be under current circumstances. There has been no repression carried out thanks to our equipment,' Formenti told Corriere della Sera" (*CNN Online*, Cyberwar Explodes in Syria. November 20, 2011).

"'We have a contract in place with Syria, this true; but everything has been halted for two months, and there are none of our technicians in Damascus.' After five days of silence, there is a statement by Andrea Formenti, chairman of Area SpA, the Italian software house that has become an international case because it is installing an intercept system of Internet traffic on behalf of [Syrian President] Bashar Assad's regime. Formenti, 42, explains his having 'landed' in Syria: 'We won a international bidding contest in 2008, outbidding 4 European countries, and other non-European companies. As interlocutors, we have never had people either in the military or in the intelligence services, but of the local telephone provider.' Area's chairman stated that the contract was worth 13 million euros, but denied currently having personnel at work in the Middle East country. 'For two months everything has been halted, and I would like to point out that the eavesdropping system has never been operated, and as things now stand, it never will.' The future is uncertain: 'We have contractual agreements that are very binding, and which, if not honoured, would force us to pay hefty penalties. On the other hand, we are following the situation in Syria as it evolves. We want no part of being accomplices to repression. We hope there will be some form of intervention by the international authorities to sort things out.' Yesterday, a protest was held in front of Area headquarters by anti-Assad representatives who live in Italy. Beside them were activists of the Italian Pirates Party" (*BBC Monitoring Europe*, Italian Software Company Denies Complicity in Syrian President's Repression. November 9, 2011).

Area Spa is producing and selling Monitoring Centres. It has obtained a contract for implementing an Internet surveillance system in Syria. The company has reacted to allegations after they were made public by the media, saying that the system has never been activated. The case is an example of how first surveillance technologies are sold to countries or organisations that are considered problematic by human rights groups and only after information about it has been made public do companies react to the allegations. The question that arises is what happens in those cases, where civil society watchdog organizations do not find out about the existence of specific cases or do not have the resources to engage in inquiries.

change.org gathered 20 000 signatures for a petition against the project (change.org, How We Won, December 1, 2011.

http://www.change.org/petitions/demand-us-and-european-cos-stop-supporting-deadly-syria-net-surveillance). It was initiated by the Internet freedom group Access and the Syrian blogger Anas Qtiesh. Area SpA withdrew from the project. Also Qosmos withdrew its technology supply and released a news statement about this circumstance.

Qosmos reacted to the media's charges: "Qosmos technology components are sold to third-party software vendors to improve performance in a wide variety of tele-

communications, network infrastructure and cyber security applications. We share the concern about the potential for misuse of surveillance applications. As a result, Qosmos withdrew from the Syrian 'Asfador' project – a decision made prior to the system being finalized and prior to the initial story reported by Bloomberg on 3 November. Qosmos will neither supply nor support its technology to those who sell to authoritarian regimes. Qosmos is fully compliant in adhering to all laws related to the sale and use of its technology. Although the use of Lawful Interception (LI) solutions by telecommunications companies is mandated throughout the EU, US and most other countries worldwide to collect communications in accordance with local laws, recent political events have shown that further regulation of LI, including more restrictive legislation, is required to prevent abuse" (*Qosmos*, Qosmos Statement about Recent Media Reporting. November 22, 2011. http://www.qosmos.com/news-events/qosmos-statement-about-recent-media-reporting).

Also the Germany company Utimaco reacted to the media reports: "It is thought that German surveillance technology has also been delivered to Syria, as part of a surveillance system made by the Italian firm Area. For years, the Italians have used specialized software by the German firm Utimaco in their systems. But as Utimaco senior executive Malte Pollmann insists, Area only built a test version, and the Italians have just cancelled the entire project. 'Our software was not used,' says Pollmann" (*Spiegel Online International*, Western Surveillance Technology in the Hands of Despots. December 8, 2011). In a statement on its website, Utimaco declared: "Utimaco and its majority shareholder, Sophos, have recently been included in media reports about an Italian OEM reseller (Area S.p.A.) allegedly selling Utimaco's LIMS technology to Syria. We take global trade compliance very seriously and require all of our partners to adhere to the German, European Union (EU) export regulations and United Nations embargo lists. We are thoroughly investigating the matter and have stopped any further activities with Area until we receive full clarification from them" (http://lims.utimaco.com/en/company/newsevents/statement-on-recent-media-reports-from-utimaco-safeware-ag/).

The export of surveillance technology was in this circumstance only prevented because critical journalists and civil society stepped in. The involved companies seemed to have at first had no scruples about the possible use of their technologies for the monitoring of political opposition, which shows that it is difficult if civil society has to take the role of a watchdog that tries to correct and stop companies behaviour after it has actually happened or started. Civil society tends to have limited resources and one can ask what happens in those cases that remain unknown. If civil society and the media had not created pressure (e.g. because of lack of knowledge, resources, employees, etc), one can imagine that project "Asfador" would have been implemented and resulted in humans being tortured and killed for their political believes with the help of European surveillance technologies.

2.3.7.2. Amesys (France)

In August 2011, the *Wall Street Journal* wrote that the Amesys sold deep packet inspection technologies to Libya, where, according to the Wall Street Journal, Gaddafi'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. August 30, 2011). The International Federation for Human Rights and the *Ligue des Droits de l'Homme et du Citoyen* filed criminal charges against Amesys (*FIDH*, FIDH and LDH file a complaint concerning the responsibility of the company AMESYS in relation to acts of torture. October 19, 2011):

"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 recently abandoned room is lined with posters and English-language training manuals stamped with the name Amesys, a unit of French technology firm Bull SA, which installed the monitoring center. A warning by the door bears the Amesys logo. The sign reads: 'Help keep our classified business secret. Don't discuss classified information out of the HQ'. The room, explored Monday by The Wall Street Journal, provides clear new evidence of foreign companies' cooperation in the repression of Libyans under Col. Gadhafi's almost 42-year rule. The surveillance files found here include emails written as recently as February, after the Libyan uprising had begun. [...] This kind of spying became a top priority for Libya as the region's Arab Spring revolutions blossomed in recent months. [...] 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. [...] Gadhafi's regime had become more attuned to the dangers posed by Internet activism, even though the nation had only about 100,000 Internet subscriptions in a population of 6.6 million. The Eagle system allows agents to observe network traffic and peer into people's emails, among other things. In the room, one English-language poster says: 'Whereas many Internet interception systems carry out basic filtering on IP address and extract only those communications from the global flow (Lawful Interception), EAGLE Interception system analyses and stores all the communications from the monitored link (Massive interception)'. [...] In a basement storage room, dossiers of Libyans' online activities are lined up in floor-to-ceiling filing shelves" (*Wall Street Journal Online*, Firms aided Libyan spies. First look inside security unit shows how citizens were tracked. August 30, 2011).

Peter Bouckaert, Human Rights Watch's emergencies director, expressed the concern that Western companies and governments take actions to destroy evidence of their support of Gaddafi and the surveillance of the political opposition in Libya (*The Times*, West tries to cover up Libya deals: The race is on to seek out and destroy any incriminating evidence. October 7, 2011).

In a press release, Amesys disputed the claim that it installed a surveillance system in Libya and announced that it reserves the right to file suit against those who make such claims:

"Amesys signed a contract with the Libyan authorities in 2007. The relevant hardware was delivered in 2008. The contract was related to the making available of analysis hardware concerning a small fraction of the Internet lines installed at that time (a few thousand). This did not include either Internet communications via satellite (as used in Internet cafes), encrypted data such as Skype-type communications, or filtering of Web sites. In addition, the hardware used did not allow for the monitoring of either fixed or mobile telephone lines.

The contract was concluded at a time when the international community was in the process of diplomatic rapprochement with Libya, which was looking to fight against terrorism and acts perpetrated by Al Qaeda (2007 was the year in which the Bulgarian nurses were released). (In December 2007 Muammar Gadhafi made an official visit to France; in July 2009 Muammar Gadhafi met with Barack Obama in Italy). All Amesys' business dealings comply rigorously with the legal and regulatory requirements set out in international, European and French conventions. Amesys does not operate any telephone or Internet monitoring centers, anywhere worldwide. [...] Amesys reserves its rights in relation to any infringement that may affect its image or reputation"

(Amesys, Press release. September 1, 2011. http://www.wcm.bull.com/internet/pr/new_rend.jsp?DocId=673289&lang=en).

So there are two different stories: On the one hand journalists and human rights activists who say that they discovered a Libyan monitoring centre and that "Amesys in 2009 equipped the center with 'deep packet inspection' technology". On the other hand Amesys that says that it does not operate such centres. And there is a document released by WikiLeaks (#5_15) that if authentic seems to suggest business relations between i2e and Libya.

2.3.7.3. trovicor (Germany) and Nokia Siemens Networks (Finland)

In April 2009, the Washington Times reported that Nokia Siemens sold a Monitoring Centre to Iran:

"Nokia Siemens Networks (NSN), a joint venture between the Finnish cell-phone giant Nokia and German powerhouse Siemens, delivered what is known as a monitoring center to Irantelecom, Iran's state-owned telephone company. A spokesman for NSN said the servers were sold for "lawful intercept functionality," a technical term used by the cell-phone industry to refer to law enforcement's ability to tap phones, read e-mails and surveil electronic data on communications networks. In Iran, a country that frequently jails dissidents and where regime opponents rely heavily on Web-based communication with the outside world, a monitoring center that can archive these intercepts could provide a valuable tool to intensify repression. Lily Mazaheri, a

human rights and immigration lawyer who represents high-profile Iranian dissidents, said she had suspected that the government had increased its capability to monitor its perceived enemies. Recently, one of her clients was arrested because of instant messaging he had participated in with Ms. Mazaheri, she said. 'He told me he had received a call from the Ministry of Intelligence, and this guy when he went to the interrogation, they put in front of him printed copies of his chats with me. He said he was dumbfounded, and he was sent to prison.' […] Hadi Ghaemi, spokesman for the International Campaign for Human Rights in Iran, said 12 women´s rights activists were arrested late last month at a private meeting to celebrate the Persian New Year. He said the raid suggested the state had access to private communications. 'This is an absolute threat to the privacy of all Iranian activists. It puts them in danger of being constantly monitored by the intelligence services, something that we know is already happening,' Mr. Ghaemi said" (*Washington Times,* Fed Contractor, Cell Phone Maker Sold Spy System to Iran. April 13, 2009).

The Iranian journalist Isa Saharkhiz was jailed for three years "on charges of insulting Iran's supreme leader and spreading propaganda against the regime. […] Last month, Saharkhiz filed a lawsuit against Nokia Siemens, accusing the company of delivering surveillance equipment to Iran that helped the authorities trace his whereabouts through his cell phone" (*BBC Monitoring World Media*, Prominent Iranian Journalist Jailed for Three Years. September 30, 2010).

Nokia Siemens commented on media reports: (*ARD Tagesthemen*, Siemens-Nokia Überwachungstechnik im Iran. June 24, 2009.

http://www.youtube.com/watch?v=8JbydEFBx5E). "The system can only record, it cannot identify anybody" (Stefan Zuber)[1]. The journalist Erich Möchel in contrast said: "One can geographically locate with these monitoring centres, where persons are, one can create their communication profile, with whom they communicate. Groups can be investigated"[2] (ibid). A product specification of the Nokia Siemens Monitoring Center (provided in one of Elaman's brochures) explains that it supports the "fully automatic recording of all data concerning all activities of the target" and makes "nationwide monitoring possible" (#7_2). So the relevant aspect is not that it does not censor the Internet, but rather that Nokia Siemens' Monitoring Center can monitor the activities and communications of political activists.

A former employee of Nokia Siemens reported that he was part of the installation of a Monitoring Centre in Iran (ZDF Frontal21, Nokia-Siemens-Networks im Iran. January 26, 2010. http://www.youtube.com/watch?v=oHqyKYa6Ffw). Siemens Board Member Joe Kaeser said: "There is today no reason for us to assume that NSN has act-

[1] "Das System kann nur aufzeichnen, es kann niemanden identifizieren. Es ist nicht geeignet, um Zensur zu üben".

[2] "Es können mit diesen Monitoring Centern Personen geographisch bestimmt werden, wo sie sind, es kann ihr Kommunikationsprofil erstellt werden, mit wem sie kommunizieren. Es können Gruppen ausgeforscht warden".

ed unlawfully or unorderly"[3]. In the same report, the two Iranian political activists Poojan Mahmudian and Kianoosh Sanjari reported that they were imprisoned and that their communications were monitored (ibid.).

In its Corporate Responsibility Report 2009, Nokia Siemens' CEO Rajeev Suri wrote: "Over the past year we have seen allegations that telecommunications technology, including that provided by Nokia Siemens Networks, has been used to suppress human rights instead of enhancing them. This is not a simple issue as technology that is designed to benefit society can be used for other purposes and, of course, governments can change over time" (Nokia Siemens Networks 2009, 4). This statement implies that a Monitoring Center is designed for benefiting society and that its use for repression of political opponents is an unintended side-effect. The question is if the purpose of the use of such a technology for repression is not foreseeable if a company enters a business deal with Iran.

In a statement issued in June 2009, Nokia Siemens argued that the surveillance centre it delivered to Iran had "the capability to conduct voice monitoring of local calls on its fixed and mobile network" and that it could not "provide data monitoring, internet monitoring, deep packet inspection, international call monitoring or speech recognition" (Nokia Siemens Networks, Provision of Lawful Intercept Capacity in Iran. June 22, 2009. http://www.nokiasiemensnetworks.com/news-events/press-room/press-releases/provision-of-lawful-intercept-capability-in-iran). It also said in the same statement that Nokia Siemens Networks' Intelligence Solutions was sold to Persua GmbH on March 31st, 2009 (ibid), which now operates it under the name Trovicor GmbH (*Spiegel Online International*, Western Surveillance Technology in the Hands of Despots. December 8, 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. August 23, 2011. http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html).

"Trovicor equipment plays a surveillance role in at least 12 Middle Eastern and North African nations, according to the two people familiar with the installations. […] Al Khanjar says the first of his communications used in the interrogations was intercepted in June 2009. At that time, the Nokia Siemens family of related companies was the only known supplier and maintainer of monitoring centers to Bahrain, the two people familiar with the installations say. The clusters of computers required constant upgrades by the companies, they say" (ibid.).

In April 2012, German media published allegations that Nokia Siemens also sold its Monitoring Centre to Syria. "German industrial giant Siemens sold network surveillance technology to the Syrian regime in 2000, public broadcaster ARD reported on

[3] "Es gibt heute für uns keinen Grund anzunehmen, dass NSN sich rechtswidrig oder nicht ordnungsmässig verhalten hat".

Tuesday night. According to their news show 'Fakt', a product called the 'Monitoring Center' was delivered to Syrian mobile communications company Syriatel. Nokia Siemens Networks confirmed the delivery, they reported. The corresponding business division at Siemens became the new joint venture Nokia Siemens Networks in 2007. The following year, that company signed a contract with Syrian landline provider STE, a deal that also included the 'Monitoring Center'. These contracts were then transferred in March 2009 to the Nokia Siemens Networks spin-off company Trovicor, which took over the 'Voice and Data Recording' division, ARD reported, citing documents they had obtained.

The Munich-based company Trovicor, which belongs to a financial investor today, declined to comment on the issue, 'Fakt' reported. But a human rights activist from Amnesty International told the show that the systematic online surveillance by Syrian security forces was likely playing a role in the capture of opposition members, who face torture after their arrest. […] Internet freedom activist and Pirate Party member Stephan Urbach criticized the export of surveillance technology from Germany. 'We need a broader debate about the ethical responsibility of companies', he said in a statement. 'The German government has completely missed this debate, particularly in the wake of revelations about such filtering and surveillance systems'. If it becomes unambiguously clear that German companies have delivered surveillance technology to totalitarian states, Berlin must 'swiftly correct this failure', he added" (*Spiegel Online International*, Monitoring the Opposition: Siemens Allegedly Sold Surveillance Gear to Syria. April 11th, 2012.

http://www.spiegel.de/international/business/0,1518,826860,00.html).

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 aganist to me while I was beaten"[4] (*FAKT*, Syrien überwacht mit Siemens-Technik. April 10, 2012. http://www.mdr.de/fakt/siemens106.html) .

If these reports are true, then it means that Nokia Siemens first sold Monitoring Centres to Iran and Syria, then sold its surveillance business unit to another company that renamed the business unit to trovicor and continued selling the technology to countries that use them for tracking, imprisoning and torturing political activists.

Erich Möchel, the first journalist who reported about Nokia Siemens relations to Iran, comments on the sale of the surveillance unit to a smaller company that there was no concern about human rights, but only a concern about image damage, and that the business with surveillance continues: "Meanwhile predominates the insight that the collateral damage for company policy probably will be much smaller if these Monitoring Centers [...] are outsourced to specialist companies and one self prepares eve-

[4] 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".

rything technically 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. So one sends ahead somebody else – companies that do not care because they come from this area. [...] If you sell to a state a complete GSM network family, then this really costs money. That's a lot of revenue. Well, now one says stop that, one lets others take care of it, the Monitoring Centres, and one rather makes the big business and not the small business because both get together badly [...] Nokia has suffered a huge reputational damage by the revelations in Iran. [...] For this reason one has retreated and said: The image loss is larger than the expected profit when we carry on further this way, so we stop it. That's basically a very wise business policy decision" (*NDR*. ZAPP: Interview mit Erich Möchel. December 7, 2011.

http://www.ndr.de/fernsehen/sendungen/zapp/media/moechel103.html)[6].

Möchel in the interview 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.

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

[5] "Inzwischen überwiegt die Einsicht, dass der Kollateralschaden für die Firmenpolitik wohl wesentlich geringer sein wird, wenn man diese Monitoring Centres […] an Spezialfirmen auslagert und man selbst bereitet eigentlich nur alles dazu vor technisch, dass dieses fremde Equipment (von Dritten zugelieferte) problemlos an die eigenen Telefonienetze andockbar ist. […] Es ist reine Marktpolitik, sonst nichts. Es hat nichts mit Menschenrechten zu tun, sondern nur damit, dass man sich selbst nicht anpatzen will damit. Sondern da schickt man jemanden anderen vor – Firmen, denen es egal ist, denn sie kommen aus dem Bereich. […] Wenn man an einen Staat ein Netz aus der kompletten GSM Familie verkauft, das kostet so richtig Geld. Das ist viel Umsatz. Naja, jetzt sagt man halt, man überlässt das anderen, die Monitoring Centres, und wir machen lieber das große Geschäft und das kleine Geschäft nicht, denn beide Geschäfte zusammen vertragen sich schlecht. […] Nokia hat einen immensen Imageschaden durch das Auffliegen im Iran davongetragen. […] Aus diesem Grund hat man sich zurückgezogen und hat gesagt: Der Imageschaden ist grösser als der zu erwartende Gewinn, wenn wir das weiter betreiben, also hören wir auf damit. Eine sehr kluge geschäftspolitische Entscheidung im Grunde ".

[6] "Inzwischen überwiegt die Einsicht, dass der Kollateralschaden für die Firmenpolitik wohl wesentlich geringer sein wird, wenn man diese Monitoring Centres […] an Spezialfirmen auslagert und man selbst bereitet eigentlich nur alles dazu vor technisch, dass dieses fremde Equipment (von Dritten zugelieferte) problemlos an die eigenen Telefonienetze andockbar ist. […] Es ist reine Marktpolitik, sonst nichts. Es hat nichts mit Menschenrechten zu tun, sondern nur damit, dass man sich selbst nicht anpatzen will damit. Sondern da schickt man jemanden anderen vor – Firmen, denen es egal ist, denn sie kommen aus dem Bereich. […] Wenn man an einen Staat ein Netz aus der kompletten GSM Familie verkauft, das kostet so richtig Geld. Das ist viel Umsatz. Naja, jetzt sagt man halt, man überlässt das anderen, die Monitoring Centres, und wir machen lieber das große Geschäft und das kleine Geschäft nicht, denn beide Geschäfte zusammen vertragen sich schlecht. […] Nokia hat einen immensen Imageschaden durch das Auffliegen im Iran davongetragen. […] Aus diesem Grund hat man sich zurückgezogen und hat gesagt: Der Imageschaden ist grösser als der zu erwartende Gewinn, wenn wir das weiter betreiben, also hören wir auf damit. Eine sehr kluge geschäftspolitische Entscheidung im Grunde ".

journalist Isa Saharkhiz and the political activists Poojan Mahmudian and Kianoosh Sanjari in Iran or the Bahraini human rights activist Abdul Ghani Al Khanjar. There are differing reports and views about what technical capacities the communications surveillance technologies exported to Iran and Bahrain actually had. So although the business practices are not entirely clear, it seems to be the case the companies like trovicor and Nokia Siemens produced or have produced surveillance technologies that are capable of intercepting the communications content of different forms of communication (Internet, fixed line telephony, mobile phone communication, etc) and that such technologies can in political contexts be used for repression against the political opposition.

On October 25th, 2010, the EU updated its export restrictions to Iran that were issued in 2007. The restriction includes an explicit restriction "on trade in dual-use goods and technology, as well as equipment which might be used for internal repression" (*EU Regulation No. 961/2010 of 25 October 2010 on Restrictive Measures against Iran*). This means that exports of Internet and phone surveillance technologies have been legal prior to this restriction. In March 2012, the EU updated this regulation saying that equipment that can be used for Internet and phone surveillance and internal repression shall not be exported from the EU to Iran (*EU Regulation No. 267/2012 of 23 March 2012 concerning Restrictive Measures against Iran*). The EU's export restrictions of that were passed on November 16th, 2011 apply for equipment that can be used "in connection with a violation of human rights, democratic principles or freedom of speech as defined by the Charter of Fundamental Rights of the European Union, by using interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of Internet use (e.g. via Monitoring Centres and Lawful Interception Gateways)" (*EU Regulation No. 1232/2011 of the European Parliament and the European Council)*. The restriction applies only for the following countries: Argentina, China (including Hong Kong and Macao), Croatia, India, Russia, South Africa, South Korea, Turkey, and Ukraine (ibid.). This means that export of communications surveillance technology to a country like Bahrain is still legal, whereas it is now illegal to export similar technologies (like Monitoring Centres) to Iran. So if the claims that trovicor exported communications surveillance tools to Bahrain were true, then it would definitely be the case that "trovicor complies with all export and customs controls in all regions where business is conducted" (#9, 7). The question that can however be posed is not only if legal standards have been respected or if fundamental ethical principles are respected (such as the human right of freedom of assembly and expression) and if trovicor's business practices respect the ethical goal that it has set itself in its Code of Business Conduct (#9) and that is not primarily a legal goal, namely that "trovicor's business ethics goal is, as an industry leader, to be among the world's best in corporate responsibility, corporate governance, promoting fair competition, adapt internationally recognized standards whenever feasible, and practicing good corporate citizenship wherever it does business" (#9, 4).

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. December 8, 2011) and "Birgitt Fischer-Harrow, Trovicor's head of marketing communications, said Trovicor's contracts prevent it from disclosing its customers or the countries where it does business. She declined to comment further" (*ArabianBusiness*, Western Spy Tools Aid in Crackdown on Arab Dissent. August 28, 2011). That businesses refuse to comment on their exports shows that under the current legal circumstances in the EU it is difficult to obtain transparency about which surveillance technologies have been exported and sold to which countries and organizations by European security companies.

In some of the cases presented thus far, companies engaging in the export of communications surveillance withdrew their projects or plans only after the media and civil society criticized them publicly, in other cases companies declined to comment. This shows the circumstance that there is a lack of transparency of the business practices of security companies.

2.3.7.4. Gamma Group (UK)

Gamma's FinFisher is a so-called "Trojan horse", a software that once installed allows the intruder remote access. FinFisher can infect computers, mobile phones, local networks and ISP networks and extract data from these systems (#7_10, 4-10). The product and training was advertised in Eleman's Communications Monitoring catalogue from October 2007 (#7_2). FinFisher can e.g. be tarned as a software update that is sent to a computer or mobile phone (*NDR*. ZAPP: Germany Spyware for Dictators. December 7, 2011.

http://www.ndr.de/fernsehen/sendungen/zapp/media/zapp4923.html).

"FinFisher is the leading offensive IT Intrusion program through which Gamma provides complementary solutions, products and advanced training capabilities to Government end-users who are seeking world class offensive techniques for information gathering from suspects and targets" (#19).

According to media reports, Gamma offered to sell its FinSpy software to Egyptian security authorities (*EUobserver.com*, EU companies banned from selling spyware to repressive regimes. October 11, 2011). "Egyptian anti-regime activists found a startling document last month during a raid inside the headquarters of the country's state security service: A British company offered to sell a program that security experts say could infect dissidents' computers and gain access to their email and other communications. […] Amid the scattered papers, interrogation devices and random furniture found during the raid, the activists uncovered a proposed contract dated June 29 from the British company Gamma International that promised to provide access to Gmail, Skype, Hotmail and Yahoo conversations and exchanges on computers targeted by the Interior Ministry of ousted President Hosni Mubarak. The proposal from Gamma International was posted online by Cairo physician Mostafa Hussein, a blogger who was

among the activists who seized the ministry's documents. 'It is important evidence of the intent of the state security and investigation division not to respect our privacy,' Mr. Hussein said. 'This proposal was sent to a notorious department known for torture, spying on citizens to help Mubarak's regime,' Mr. Hussein said, referring to the State Security Investigations Service. 'The company Gamma, I consider them to be partners in the crime of trying to invade our privacy and arrest activists' " (*Washington Times*, British Firm Offered Spy Software to Egypt: Activists Say They Were the Targets. April 26, 2011).

Also the German regional public service TV station NDR reported about a secret offer of Gamma to the Egyptian state for the FinFisher technology (*NDR*. ZAPP: Germany Spyware for Dictators. December 7, 2011.

http://www.ndr.de/fernsehen/sendungen/zapp/media/zapp4923.html).

The Egyptian blogger Mostafa Hussein, who discovered the documents, argued in the NDR report that this software is "exactly like weapons" (ibid.). The Egyptian Internet activist Israa Abdel Fattah was interviewed, saying that this software is "helping the dictators [...] to [...] attack the activism" (ibid.). Her own Internet communication was surveilled by the Egyptian government. She said that surveillance companies "only think about money" (ibid.). NDR also describes Gamma's attempts to sell surveillance technologies to Turkmenistan and Oman (ibid.). The Austrian IT journalist Erich Möchel said that surveillance technology companies encourage "repression and torture" (ibid.).

Gamma reacted to the accusations partly by refusing to comment and partly by denying them: "Peter Lloyd, an attorney for Gamma International, told The Washington Times that the company never sold the FinFisher software to the Egyptian security ministry. But the lawyer declined to answer questions about the company's malware division, or the detailed proposal found in the Egyptian ministry. 'Gamma complies in all its dealings with all applicable U.K. laws and regulations,' Mr. Lloyd said. 'Gamma did not supply to Egypt but in any event it would not be appropriate for Gamma to make public details of its transactions with any customer' " (*Washington Times*, British Firm Offered Spy Software to Egypt: Activists Say They Were the Targets. April 26, 2011).

Gamma explains the need of surveillance technologies by threats to national security. The Egyptian revolution certainly was a threat to the national security of the old Mubarak regime. The question that arises is if a government that is questioned in mass demonstrations by its own population has the moral right to defend national security with the help of surveillance technologies that are used to spy on, imprison, torture or kill opponents. On the one hand there are claims that Gamma offered to supply Internet surveillance technologies to Egypt, on the other hand the company has denied this. FinFisher definitely is a technology that has the potential to be used for the surveillance of and repression against political opponents.

2.3.7.5. A Problem Not Limited to Internet Surveillance: The Export of Mobile Phone Surveillance Technology

Discussions about the Swedish company Ericsson's business relations to Iran shows that not only the export of DPI Internet surveillance technology is controversial, but that the same topic extends into the realm of mobile phone networks.

On October 30, 2011, *Bloomberg* published an article titled *"Iranian Police Seizing Dissidents Get Aid Of Western Companies"* (http://www.bloomberg.com/news/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies.html) as part of their *Wired for Repression* article series on "Surveillance Tech & Repressive Regimes" (http://topics.bloomberg.com/wired-for-repression). The *Bloomberg* article says journalist Saeid Pourheydar was imprisoned by Iranian police in 2010. He was "held in Evin Prison for weeks following his arrest early last year for protesting, he says, he learned that he was not only fighting the regime, but also companies that armed Tehran with technology to monitor dissidents like him" (ibid). Pourheydar informs the sources that his mobile device was intercepted, stating "the power of this enemy became clear as intelligence officers brandished transcripts of his mobile phone calls, e-mails and text messages during his detention. About half the political prisoners he met in jail told him police had tracked their communications and movements through their cell phones" (ibid.). Following the incident, Pourheydar is quoted: "This is a commerce of death for the companies that place this technology in the hands of dictatorships" (http://www.insideofiran.org/en/human-rights/3042-iranian-police-seizing-dissidents-get-aid-of-western-companies.html).

The Swedish company Ericsson "confirmed that in the fourth quarter of 2009 it sold a mobile- positioning center for customer billing purposes to MTN Irancell Telecommunications Services Co" (ibid). The *Serving Mobile Positioning Centre* is a "box that can calculate a person's location and logs the data" (ibid.). The article claims an unnamed former employee of Ericsson was "urgently called in to fix the system in late 2009 says he was told that Iranian intelligence officers were attempting to pinpoint the location of someone in the Zahedan area of southeast Iran" (ibid.). According to Bloomberg, Ericsson "decided in October 2010 it would no longer sell any products into Iran due to recent efforts to tighten sanctions." (ibid.). The article claims that former Ericsson employee Saiviahs Fahimi was arrested in December 2009 by Iranian police based on interception of his mobile text messages, allegedly using Ericsson technology. The article claims Fahimi was familiar with how the technology can work, stating "I worked on the technology and I was a victim of the technology, as well," and: "They can monitor whoever they want, for their purposes, not for the benefit of society and people" (ibid).

In an article published by *Inside of Iran*, Iranian women's rights activist Mansoureh Shojaee claims she was detained and interrogated at the same prison Pourheydar was detained at. She claims the police had details of her phone activity, stating, "my mobile phone was my enemy, my laptop was my enemy, my landline was my enemy" (http://www.insideofiran.org/en/human-rights/3042-iranian-police-seizing-

dissidents-get-aid-of-western-companies.html). In 2010, *The Swedish Wire* published: *"Sweden's Ericsson accused of monitoring in Iran"* based on a statement by Nobel Peace Prize Laureate Shirin Ebadi that Ericsson is selling "software that allowed it to monitor text messages and mobile phone calls"
(http://www.swedishwire.com/business/7325-swedens-ericsson-accused-of-monitoring-in-iran).

On November 11, 2011 *The Local*, a Swedish online news website published an article titled "*Ericsson Rejects Claims of Aiding Iran*" (*The Local,*
http://www.thelocal.se/37098/20111101/). According to *The Local*, Ericsson's Fredrik Hallston rejected claims published in a *Bloomberg* article that they were providing Iran with "technology capable of tracking dissidents through their mobile phone activity", stating that what Ericsson really sold was a "location based charging" system that allowed mobile operator Irancell to charge the right tariffs based on the callers location, claiming that the technology is unable to track the callers location in real time. Hallston defends Ericsson's business relations by adding: "It is in everyone's interest that you call in and out of the country" (ibid). In 2006, *Cellular News* (*CN*, http://www.cellular-news.com/story/16540.php) published an article about Ericsson and British operated Vodafone's involvement in the illegal surveillance of the Greek Prime Minister Kostas Karamanlis. The British mobile operator Vodafone allegedly used technology equipment built by Ericsson to illegally wiretap "senior military officers, human rights activists, journalists, Arab businessmen and a mobile phone used by the U.S. Embassy, according to a list of numbers given to parliament by Vodafone" (ibid). According to the article: "The rogue wiretap program hijacked the Ericsson software to divert calls to mobile phones using hard-to-trace top up services, officials said" (ibid). The CEO of Ericsson's Greece division Bill Zouki claims that Vodafone was informed and responsible for the legal use of the software, although Vodafone denies these claims. In January 2012, *Crikey.com,* wrote: "Ericsson has also been accused of selling surveillance technology to Iran and Ericsson equipment is used by the savage Belarussian dictatorship of Alexander Lukashenko to wiretap opponents" (http://www.crikey.com.au/2012/01/10/tracking-the-trackers-the-cyber-snoops-working-in-australia/).

The example shows that discussions about the export of communication surveillance technology are not only limited to computing and the Internet, but also affects the realm of mobile phone surveillance. Supply of communications surveillance technologies seems to be inherently connected to possible abuse.

2.3.8. Summary of the Main Findings about European DPI Surveillance Technologies

2.3.8.1. The Technological Set-Up of Internet Surveillance

The Uppsala University research team analysed sample of documents that describes

the use of Internet surveillance technologies that are produced and sold by European companies. The question was to find out what kinds of Internet surveillance technologies are available.

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

* 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 Center (trovicor), formerly: Nokia Siemens Monitoring Center (Nokia Siemens Networks)
* Utimaco Lawful Interception Management System (LIMS) (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, mobile telephony). Deep Packet Internet surveillance is facing the challenge that Internet protocols are changing and that filtering, decoding and analysis of different protocols (such as e-mail, webmail, VoIp, chat, http, FTP, etc) is needed in order to thoroughly monitor Internet traffic.

For the purpose of Internet surveillance, not only DPI technologies are available on the European security market, but also Trojan horses. Two examples are:

* Remote Forensic Software (Digitask)
* FinFisher (Gamma Group)

Trojan horses are software programmes that are disguised as other programmes and once installed on a computer collect data about users that are secretly transmitted to the monitoring party. The use of such communication surveillance tools has been considered in law enforcement in cases, where subjects use Skype or encrypted e-mail communication. Digitask's Remote Forensic Software has in Germany resulted in an intense public debate about the constitutionality and ethical desirability of online investigations in the debate about the "Bundestrojaner" ("Federal Trojan").

Gamma Group's FinFisher has gained public attention when news reports claimed that the company had offered the technology to Egyptian security authorities.

2.3.8.2. The Self-Understanding of European Internet Surveillance Technology Producers

The Uppsala University research team also studied the self-description of the analysed companies and how they explain the relevance of Internet surveillance, i.e. why the company thinks it is important that it produces and sells such technologies. The question was how the selling of these technologies was justified. 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" (#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 characterised 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, 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 new surveillance of the 21st century 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 un-

dercuts 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, 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 (Kling, Rosenbaum and Sawyer 2005, 13, 188; Lister et al. 2003, 391; Shade 2003). Technological determinism assumes that "technologies change, either because of scientific advance or following a logic of their own; and [that] they then have effects on society" (MacKenzie and Wajcman 1999a, 3). It is based on "a simple cause-and-effect-sequence" (MacKenzie and Wajcman 1999b, xiv). "Such determinism treats technology as both panacea and scapegoat" (Shade 2003, 433). The identified worldview of the security industry looks for security by algorithms in a world of high insecurity. It advances a fethishism of technology – the belief that crime and terrorism can be controlled by technology. Technology is seen as promising an easy fix to complex societal problems.

Hall et al. (1978) argue that the law & order-worldview has been connected to the rise of neo-liberal 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. Neoliberalism aims at a society that is oriented on the "multiplicity and differentiation of enterprises" at all levels of society (149). It is in favour of the "formalization of society on the model of the enterprise" (Foucault 2008, 160). It advocates the idea that the human is a *homo oeconomicus* – an "entrepreneur of himself" (226). This model stands for the "economization of the entire social field" (242) and the creation of an "enterprise society" (242). The involvement of the security industry in the production of communications surveillance technology that is used by state actors is characteristic for this new mode of governance – policing is turned into a profitable business, companies make profit from surveillance technologies that are sold to state actors.

2.3.8.3. The European Internet Surveillance Industry's Expressed Views towards Privacy Aspects of Internet Surveillance

The Uppsala University research team also documented what the analysed companies said about problems and privacy violations arising in the context of Internet surveillance. In those cases, where there was public criticism of the companies, we also analysed how the companies reacted to criticism in public statements.

The question of reaction to public criticism was especially relevant in a number of analysed cases, where there were public charges published in 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 (see the detailed discussions in section 2.1.3.7. and annex A):

* 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

A range of positioning towards privacy questions of Internet surveillance could be found in the analysis, ranging from no mentioning on the one side to the discussion of advantages of DPI on the other side. Six positions could be identified.

a) No discussion of privacy aspects of Internet surveillance

Privacy aspects were often not mentioned in the analysed documents and on the analysed websites (e.g. Inveatech, Aqsacom, Datakom, NETI).

b) No commenting

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. December 8, 2011). Facing allegations that it planned to export the FinFisher Internet surveillance technology to Egypt, an attorney of the Gamma Group said that "Gamma did not supply to Egypt but in any event it would not be appropriate for Gamma to make public details of its transactions with any customer" (*The Washington Times*, British Firm Offered Spy Software to Egypt: Activists Say They Were the Targets. April 26, 2011).

c) Statements as the result of public pressure (media, civil society)

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

One analysed company said that a mistake was made and that they would pull out of the project (Qosmos). 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 outsourced to specialist companies and one self prepares everything technically 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. December 7, 2011.

http://www.ndr.de/fernsehen/sendungen/zapp/media/moechel103.html).

In autumn 2011, there were media charges that the Italian security company Area Spa sold monitoring centres to Syria, where heavy protests by the opposition have questioned Assad's regime since January 2011 and many protestors have been killed. Area Spa's CEO confirmed that a contract with Syria was in place and said that the interception system was never activated. The German company Utimaco reacted to the claim that Area Spa's planned project included Utimaco's LIMS technology by saying that activities with Area Spa have been stopped.

In one case, there was a denial of the charges that were made by the public (Amesys).

d) Approval of the surveillance of the communication of the political opposition

In a single case, we found a formulation that justified the surveillance of the communication of political opponents. One company (Elaman from Germany) 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).

A document that presents Elaman's "Communications Monitoring Solutions" (#7_12) for the surveillance of phone networks, satellite communication, SMS, the Internet, and Radio Frequency Monitoring (RFM), and various other tools (such as FinFisher and speech identification software) specifies one task of data retention technologies in the following way: "In the field of telecommunications, data retention generally refers to the storage of call related information (numbers, date, time, position, etc.) of telephony and internet traffic. The stored data is usually telephone calls made and received, emails sent and received, web-sites visited and location data. The primary objective in data retention is traffic analysis and mass surveillance. By ana-

lysing the retained data, governments can identify an individual's location, their associates and members of a group, *such as political opponents*" (#7_12, 17; emphasis added).

Elaman advertises its surveillance products and services as well as surveillance technologies by other companies as means for fighting terrorism and crime. The technologies described in this section can be classified as Deep Packet Inspection Technologies, they allow to monitor the content of Internet communication and other forms of communication. In the analysed documents, we could not find any comments about privacy violation concerns and the limitation of human rights that may arise from the use of DPI Internet surveillance and related forms of surveillance. In contrast, as shown, Elaman says that data retention can help governments to identify "members of a group, such as political opponents" (#7_12, 17). The question that arises here is if 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 ("Everyone has the right to freedom of peaceful assembly and to freedom of association at all levels, particular in political, trade union and civic matters, which implies the right of everyone to form and join trade unions for the protection of his or her interests"). The European Convention of Human Right allows restricting this freedom if it is "necessary in a democratic society in the interests of national security or public safety, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others". 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 and also raises the question if the formulation disrespects the EU's Data Protection Directive (95/46/EC) that prohibits "the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" (article 8).

e) Proactive addressing of the dangers 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 respect 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).

f) 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 e-mails and computer viruses. Telesoft Technologies says that DPI is needed for network management and that it can create new personalized content services with payment.

3. Conclusion: DPI Internet Surveillance

Deep packet inspection (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 includes the surveillance of content data.

The conducted analysis of Deep Packet Inspection (DPI) Internet surveillance shows that there is a variety of potential impacts of this technology.

* *Potential advantages* of DPI Internet monitoring mentioned in the literature include bandwidth management by network providers in order to optimize the network transmission speed and the use for spam filters and virus filters.

* *Violation of net neutrality*: DPI use by Internet Service Providers (ISPs) can result in a violation of net neutrality and as a consequence the creation of a tiered Internet that disadvantages certain users and application types in the transmission process, is controlled by big companies and has slow connection speed if a lot of users as a consequence of DPI surveillance start using encryption that cannot be monitored, which increases bandwidth. If encryption (e.g. by the use of Tor) as a result of DPI became more common, then those users not familiar with its use as a result of information inequality would be subject to surveillance, whereas more skilled users would not (Lace 2010, 222).

* *Total Internet surveillance*: There are concerns that DPI Internet surveillance can result in the emergence of a total or relatively total Internet surveillance system, in which all, most or a lot of a users' Internet activities are monitored and maps of social connections are created. The question that arises is if such data processing is "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed" (*European Union Data Protection Directive* 95/46/EC, article 6 (c)).

* *Surveillance creep*: DPI usage for one purpose (such as network management or spam filtering) may creep to other, more privacy-sensitive and controversial purposes (such as targeted advertising or content monitoring for political purposes or law enforcement, violation of net neutrality, etc).

* *Targeted advertising*: DPI surveillance can enable targeted online advertising at the level of ISPs that is based on the analysis of the content of all or large parts of the transmitted data of users. The concerns of privacy advocates are that such data processing is disproportionate, 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.

* *Surveillance of file sharers*: The use of DPI surveillance for detecting and blocking file sharing can, as ruled by the European Court of Justice, violate users' information freedom and privacy rights. It can also reverse the presumption of innocence and advance the assumption that all Internet users are criminals unless they prove the opposite.

* *Political repression and social discrimination*: The use of DPI for targeted advertising and by governments faces the risk that sensitive data of users are monitored. The examples of 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.

There is a variety of Internet surveillance technologies available on the European security technology market that uses Deep Packet Inspection (DPI).

A typical explanation given by European security companies why they sell Internet surveillance technologies is that criminals and terrorists use the Internet and that Internet surveillance can prevent and police crime and terrorism. This worldview was characterised as a conservative ideology of crime that believes in law & order politics and the technological deterministic view that there are technological fixes to societal problems.

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

As surveillance technology producers are not complied to release their customers and sales publicly, data about what these companies are doing, is likely to be incomplete because the companies themselves often treat it as a secret. The SpyFiles make available some of this data. In the end, it is often not clear, which communications surveillance technologies are sold by which companies to whom. Not much is known about it and only surfaces occasionally as the result of investigative journalism.

What could generally be observed is that some companies argued that they couldn't comment on any customers because they had to protect the latter's interests. In other cases, companies reacted to the charges after they became public. In some cases, security companies argued that they had stopped the criticized projects or that they sold their communications surveillance business units. **A general phenomenon that could be observed is that alleged details only became public with the help of civil society and journalists.** The question arises if there are cases that are unknown to the public. Public criticism does not automatically stop the recurrence of public charges, which is shown by the claims against Nokia Siemens and trovicor: Nokia

Siemens sold its communication surveillance business after media charges that it exported communications surveillance technologies to Iran and some time later comparable charges emerged against the follow-up company trovicor in respect to Bahrain. **Overall, not much is known about the selling and export of communications surveillance technologies. There is a lack of transparency and accountability. In those cases, where charges emerge, it remains often unclear what exactly happened. The relative frequency of such charges could be an indication that good business practices are not always voluntary achieved in the security industry and that an industry that sells technologies that can seriously harm human lives needs more public transparency of its sales than other industries.**

The Dutch MEP Marietje Schaake commented in this context in October 2011 that she perceived a lack of transparency in the European security industry: "We need to ask for more transparency from companies before they actually sell these technologies. It's not about sanctions and trade restrictions, it's about making sure the new technologies are not systematically used to repress citizens" (*EUobserver.com*, EU Companies Banned from Selling Spyware to Repressive Regimes. October 11, 2011).

Surveillance Studies scholar David Lyon defines transparency as the "quality of 'seeing through'" and argues that "the public should have access to information about the modes and purposes of surveillance" (Lyon 2007, 181). Transparency would be "vital for a healthy democracy and for human rights" (Lyon 2007, 182).

A question that European policy makers may find important is if transparency of the sales of communications surveillance technologies of European security companies should be created and how this could practically be implemented.

There are "surveillance trade show[s] known to industry insiders as 'The Wiretappers' Ball'" (*Privacy International*, Surveillance Who's Who, https://www.privacyinternational.org/big-brother-incorporated/countries). Examples are ISS (Intelligence Support Systems) World and MiliPol – Worldwide Exhibition of Internal State Security. Privacy International in collaboration with the Bureau of Investigative Journalism published a list of attending organisations. "ISS World is attended by brutal dictatorships and Western democracies alike. Governments and companies from all over the world meet, mingle, buy and sell" (ibid.).

Surveillance technology fairs are often not accessible for the general public. At ISS World that took place on February 13-15, 2012, in Dubai, "programs are by invitation only. Telecommunication service providers, government employees, LEA's and vendors with LI, Network, Security or investigative products and services are invited" (http://www.issworldtraining.com/ISS_MEA/register.cfm). The registration lists as different participant categories telecommunications service providers, government or private sector investigators, law enforcement, Department of Homeland Security, Intelligence Community, Department of Defense, surveillance technology vendors. The next Milipol event that will take place in Paris 2013 is by invitation only. The event's website says that it "is reserved for the professionals of the security industry. Access is only available with an official invitation card or with an electronic badge. Proof of identity will be requested together with the badge"

(http://en.milipol.com/To-visit-Milipol-expo/Useful-information). The access restrictions to such events imply that it is hard for critical citizens or investigative journalists to gain access. The secrecy surrounding such events adds to the lack of transparency of the security industry.

The *Office of the Privacy Commissioner of Canada* published a privacy review of DPI (*Office of the Privacy Commissioner of Canada,* Review of the Internet Traffic Management Practices of Internet Service Providers. February 18, 2009. http://www.priv.gc.ca/information/pub/sub_crtc_090728_e.cfm). It argues that one of the reasons "DPI technologies raise privacy concerns is because it can involve the inspection of information content sent from end-user to end-user, thus enabling third parties to draw inferences about users' personal lives, interests and activities. DPI devices have the ability to look at Layer 2 (link layer) through Layer 7 (application layer) of the Open Systems Interconnection (OSI) Model. DPI devices can, therefore, examine headers and data protocol structures as well as the actual payload of the message. In other words, DPI technology can look into the content of a message sent over the Internet. To use a real-world example, using DPI is akin to a third arty opening an envelope sent by surface mail, and reading its contents before it reaches its intended destination". The Office concludes that "the examination of content" with the help of DPI "may constitute an unreasonable invasion of an individual's privacy" and that the "prospective uses o DPI technology raise serious concerns about individual privacy". Privacy International believes that "online behavioural advertising for online commercial advertising using the technology of Deep Packet Inspection (DPI) is a dangerous and potentially unlawful technique that is fraught with unethical practice" (Privacy International, *Online Behavioural Targeted Advertising – Privacy International's Position*. April 19, 2009.

https://www.privacyinternational.org/article/online-behavioural-targeted-advertising-%E2%80%93-privacy-international%E2%80%99s-position).

Cooper (2011) argues that attempts for mitigating privacy risks of DPI can be to limit the depth and breadth of inspection as well as disclosing the presence and purposes of DPI. **Discussions about DPI show that privacy problems can especially arise if the content of communications that may include sensitive data is analysed for various purposes. Policy makers may want to think about legally limiting the depth of Internet surveillance so that communications content surveillance is not legally possible.**

One argument against legally limiting the allowed depth of packet inspection can be that virus scanning, spam mail filtering and bandwidth management on the side of the ISP can require unlimited DPI. At the same time there is however the danger that legally unregulated DPI results in an invisible surveillance creep, in which the limited use for one purpose is extended to other uses that can have negative consequences for the users. For managing the bandwidth in a network, it may be necessary to analyse the file type, but it is not necessary to analyse the full content of packets. Implementing virus scanning and spam mail at the ISP level entails the risk of invisible surveillance creep. A way to mitigate this risk is to implement these functions not auto-

matically in a network, but to give the subscribers/users the possibility to opt-in to network-wide scanning of certain data types (e.g. e-mails) for limited purposes such as detecting spam mail and viruses.

Technology analyst Evgeny Morozov argues that in "addition to the rosy narrative celebrating how Facebook and Twitter have enabled freedom movements around the world, we need to confront a more sinister tale: how greedy companies, fostered by Western governments for domestic surveillance needs, have helped suppress them. […] The obvious response is to ban the export of such technologies to repressive governments. But as long as Western states continue using monitoring technologies themselves, sanctions won't completely eliminate the problem – the supply will always find a way to meet the demand" (Morozov, Evgeny. Political repression 2.0. *New York Times*. September 1, 2011).

Morozov warns that if there is a demand by law enforcement and companies for communications surveillance tools, misuse is hard to control and that export bans alone are unlikely to eliminate the problem of technology-enhanced human rights violations because the use of communication surveillance against political opponents and civil society can in principle emerge in many different contexts. Political events are dynamic, the political situation can change quickly in a country, whereas passing laws and regulations is more time-consuming. An export ban of DPI communications surveillance for certain countries (as for Argentina, China, Croatia, India, Russia, South Africa, South Korea, Turkey, and the Ukraine in the EU) is facing the problem of the dynamics of political events. The charges that Nokia Siemens exported communication surveillance technology to Iran and the follow-up company trovicor to Bahrain show this problem. If the latter is true, then it certainly was not illegal because Bahrain is not included in the list of countries, to which the EU bans the export of communications monitoring devices. **The problem is that human rights violations are quite unpredictable and that technologies that can support such violations require special control, transparency and regulation.**

On the one hand, there are ICT companies that produce and sell communications surveillance technologies. Discussions relating to privacy violations and other concerns caused by such technologies on the other hand mostly come from civil society organisations that normally tend to neither automatically have a lot of money and resources nor a lot of political influence. It is therefore much more difficult for civil society to make is voice heard in the public sphere than it is for companies and governments. In relation to DPI, there is a number of active civil society groups, such as e.g.

NoDPI (https://nodpi.org),
Open Rights Group (http://www.openrightsgroup.org/),
AntiPhorm (http://www.antiphorm.co.uk),
BadPhorm – When Good ISPs Go Bad! (http://www.badphorm.co.uk),
Deny Phorm Blog (http://denyphorm.blogspot.com),
Dephormation (https://www.dephormation.org.uk),

InPhormationDesk (http://www.inphormationdesk.org),
Phorm Watch (http://phormwatch.blogspot.com).

Civil society groups that warn about actual or potential impacts of new technologies such as DPI are vital for a vivid democracy. Therefore hearing their voices and their visibility are of crucial importance and it is a task for politicians to think about how the role of civil society in politically assessing the implications of surveillance technologies can be advanced so that there is no dominance of interests by industry, government and law enforcement.

DPI is a strongly controversial technology that is enmeshed into various interests by governments, corporations and civil society. Governments have been using DPI for repressing citizens, law enforcement has been using it for surveillance of suspected criminals and terrorists, in the EU political representatives have also shown some concern about the potential and actual problems of DPI. DPI technologies are produced and sold by companies that strive for profits in the security business. The market for communications surveillance technologies seems to be highly intransparent and has been involved in controversies about human-rights violations-implicating exports, the violation of net neutrality and the creation of an unequal tiered Internet by DPI-based Internet services, the privacy implications of DPI based targeted advertising, and the limitation of users' privacy rights and information freedom by DPI-based surveillance of the Internet in order to prevent file sharing. DPI is a highly controversial new surveillance technology that has a lot of societal implications that need to be carefully considered.

The discussion of DPI Internet surveillance on the one hand brings up privacy concerns and on the other hand 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 and Raab 2006, 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 centralisation 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. 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.

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 have. The violation of civil rights is in these contexts therefore connected to the profits of what Ben Hayes (2009, 2010) terms the European security-industrial complex. He argues that there are "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, 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, 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.

The example of DPI Internet surveillance shows that **for understanding new surveillance technologies, we do not only need privacy and data protection assessments, but broader societal impact assessments that are guided by ethics and connected to the analysis of power structures in society.** ICTs and society mutually shape each other and are both conditioned by power and political economy (Fuchs 2008). Charles Raab and David Wright (2012, 382) argue in this context that the analysis of surveillance technologies should focus on "wider impacts, and ultimately impacts on society as a whole". Works by David Wright and Emilio Mordini (2012) and David Wright (2011) suggest a Privacy and Ethical Impact Assessment Framework for ICTs. "Privacy and data protection raise ethical issues, although ethical impact assessment addresses issues beyond simply those of privacy and data protection" (Wright 2011, 224).

There have been valuable attempts that have tried to establish ethical and societal impact assessment principles and frameworks for ICTs. Only some can be mentioned here. The Societal Impact Expert Working Group argues that the analysis of security technologies should be connected to the analysis of citizen's rights, societal relevance and benefits, necessity and proportionality of security technologies in a democratic society, civil liberties, and research ethics (Centre for Irish and European Security 2012). It suggests that security research projects should have independent parts that discuss ethical and societal implications.

Jacques Berleur (1999) argues that ICTs like the Internet are ethically related to issues like democracy, protection of the common good, universal service, human dignity, protection of minors, crime against humanity, justice, social exclusion, human rights, free speech and censorship, quality of life, right to information and transparency, personal qualities, non-abuse of power, respect for cultural differences, freedom of choice.

Scholars in the EU FP7 project "ETICA - Ethical Issues of Emerging ICT Applications" (http://ethics.ccsr.cse.dmu.ac.uk/etica) have argued that the assessment of emerging information technologies should be connected to topics like power relationships, sustainability, gender biases, responsibility, human dignity, freedom, autonomy, privacy, data protection, surveillance, justice, equality, solidarity, autonomy, consumer protection, cultural diversity, environmental protection, animal welfare, health, safety, equal access, health care, human rights, ownership, social inclusion, non-discrimination, participation, access to the labour market, security, proportionality, the precautionary principle, transparency, governance, global justice, integrity, welfare, human life, democracy and participation (Nagenborg and Capurro 2010, Stahl 2011, Stengel and Nagenborg 2010)-

Wright (2011) and Wright/Mordini (2012) suggest a framework for the ethical and societal impact assessment of ICTs that is based on ethical principles like dignity, informed consent, nonmaleficence, safety, solidarity, inclusion, human contact, non-discrimination, beneficence, universal service, accessibility, value sensitive design, sustainability, distributive justice, equality, fairness, social justice privacy, and data protection.

These discussions and the assessment of new surveillance technologies conducted in this chapter show that security technologies do not only have impacts on privacy and individuals, they have impacts on society at large. Contemporary societies are fundamentally structured by power asymmetries. It is therefore important that ICTs and security technologies are assessed in the context of questions that relate to society, power, democracy, justice, freedom, and political economy. For doing this, ethical assessment frameworks, guidelines, principles, systematic models and typologies of ICT ethics that are grounded in social theory and social philosophy are needed. Wright (2011, 224) concludes that "there would seem to be value in further research exploring the possibility of developing integrated privacy and ethical impact assessment" (Wright 2011, 224). Jacques Berleur and Marie d'Udekem-Gevers (2001) write about the long-standing difficulties in trying to establish general ethical guidelines in

the International Federation for Information Processing (IFIP). Although there were significant attempts and long debates in the IFIP, arguments have prevailed that hold that computer ethics can and should not be universalized and integrated. Approaches for establishing integrated and unified guidelines, frameworks and principles for ethical and societal impact assessments of ICTs and security technologies are definitely needed, but much work on this topic remains to be done, which requires resources, projects and possibilities for conducting this important work.

Annex A: An Analysis of the Internet Surveillance Technologies Produced by a Sample of European Security Companies

1. Inveatech

Place of business: Brno, Czech Republic
Website: http://www.invea-tech.com/
Self-description:
"INVEA-TECH is an university spin-off company devoted to the development of state-of-the-art solutions for high-speed network applications. [...] The main focus of INVEA-TECH is to use programmable hardware (FPGA technology) in the area of security and monitoring of high-speed network applications. The target technologies are Gigabit and 10 gigabit Ethernet" (http://www.invea-tech.com/company/about-us).

Analysis

Inveatch's LI (Lawful Interception System) is an Internet surveillance technology that is installed on the computer system of an Internet Service Provider (ISP) and allows the police or secret service to monitor the traffic over a web interface. It is a Deep Packet Inspection (DPI) technology.

Inveatech describes the usefulness and tasks of LI System in the following words: "Widespread information technologies provide fast and dynamic communication media even for criminals and terrorists. To be able to guarantee public safety, law enforcement agencies (LEAs) need to identify, intercept and analyse the content of the malicious communication. INVEA-TECH provides law enforcement and government agencies with the state of the art technology to solve the key part of the investigation process. INVEA-TECH LI System is the idea instrument for collecting evidence from wired IP-based networks" (#1).

The usefulness of the system is in the analysed documents justified with the potential use of the Internet by terrorists and criminals, which is seen in order to guarantee public safety. Privacy aspects and concerns about the surveillance of citizens and political opposition with the help of LI System are not mentioned in the analysed material.

2. Qosmos

Place of business: Paris, France (also: Bethesda, MD, USA; Singapore)
Website: http://www.qosmos.com/
Self-description:
"Qosmos sells Network Intelligence/DPI technology that identifies and analyzes data as it crosses networks. Qosmos advanced technology goes deeper than mere data classification – it recognizes thousands of protocols and traffic metadata at multi-Gbps throughputs to build the most accurate picture of network activity in real time. […] Networks are the common source of data – and sometimes the only source of data – in today's environment. Direct visibility into network activity provides the true picture of data usage, purpose and value. It is critical to identify abnormal behavior and defend against potential cyber attacks, provide a means of data retention to ensure compliance and provide audit trails and analyze performance to manage Quality of Service, for just a few examples" (http://www.qosmos.com/about-us/corporate-overview).

Analysis

Qosmos produces the Deep Packet Inspection (DPI) software iXEngine. "The latest version provides advanced Deep Packet Inspection (DPI) and metadata extraction features that deliver complete visibility into network traffic in real time, enabling developers to inject application-level insight into policy and traffic management, charging, Quality of Service (QoS), subscriber analytics and other solutions" (http://www.qosmos.com/news-events/enhancements-qosmos-ixengine-sdk-enable-smarter-mobile-network-solutions-through-network). According to the Qosmos iXEngine product sheet, the software goes beyond "traditional DPO" by also allowing to "extract protocol and application metadata, enabling detailed understanding of network transactions up to the application level" (#2_6). Qosmos says that the software has "triple R" qualities (resilience, robustness, reliability) and can thereby function under extraordinary circumstances (such as incomplete traffic or denial-of-service attacks). It can monitor, extract and analyse data that are transmitted over various Internet protocols. It conducts DPI and extracts metadata and content (#2_1).

Qosmos argues that it is a new challenge for law enforcement agencies that "the same person can communicate in several ways" (different email accounts, social media profiles, Voice over IP such as Skype, FTP, websites, etc). Its technologies would provide a surveillance solution that identifies "users and intercept[s] all type of communication initiated by the same user when a trigger such as 'user login' is detected" (#2_1). Qosmos' surveillance technology allows to monitor all communication on a device that is identified e.g. by an IP address (Internet Protocol address, identifies a specific computer in a computer network) a user's MAC address (Media Access Control address, an address of the hardware card that connects a computer to a network), or an IMSI (International Mobile Subscriber Identity, a number that uniquely identi-

fies a mobile phone). The monitored applications can all be viewed over one web application (#2_1). The software is installed on the broadband remote access server (BRAS) of an Internet service provider and/or the gateway GPRS support node (GGSN) of a mobile phone network provider (#2_1). Qosmos also sells ixMachine, which are "information extraction machines" that "extract extremely fine-grained information from the network" on which they are installed (#2_2).

Qosmos argues that a big challenge for surveillance is the "exponential growth of throughput" (#2_3), i.e. the growth of data that is transported over the Internet. The solution that Qosmos offers is to not analyse all data flows, but only focus on "relevant flows" in order to "optimize DPI usage" (#2_4). It advertises its technologies by saying it can equip "monitoring centres" with surveillance technologies and can reduce the data volume of surveillance ("reduce by 90% the data volume managed by the monitoring center") (#2_5). Qosmos also says that a "limited number of LEA [law enforcement] agents" requires the "need to automate investigation tasks" and that its products provide such features (#2_5).

Data is transported in the form of packets of certain sizes over the Internet. The transfer of an e-mail or a file is thereby connected in several steps and the transferred packets are assembled together to form a whole. Deep Packet Inspection (DPI) technologies monitor the packets that are coming into gateways, analyse, classify the data, extract parts are all of it, and make them visible to the surveillors. "Deep packet inspection (DPI) is a form of filtering used to inspect data packets sent from one computer to another over a network. […] The effective use of DPI enables its users to track down, identify, categorize, reroute or stop packets with undesirable code or data. […] DPI is normally more effective than typical packet filtering, which inspects only the packet headers. DPI inspects the packet's data part (and sometimes the packet header) when it goes over an inspection point, attempting to find protocol noncompliance, intrusions, spam, viruses or other predefined factors to determine whether the packet can pass or whether it must be directed to another location. […] Deep packet inspection is also known as complete packet inspection and information extraction. […] DPI is being used by governments to monitor and protect territorial cyber boundaries. DPI has also been used to inspect user activities, to maintain the security of big local and wide area networks, and to block malware and suspicious software. In addition, service providers make use of DPI to keep track of customers' Web-browsing habits. These customer details are then used by companies focused on targeted advertising" (Techopedia. *Deep Packet Inspection (DPI)*, http://www.techopedia.com/definition/24973/deep-packet-inspection-dpi; for a technical characterization of DPI see: Ramos 2007).

In the analysed documents, Qosmos gives no specific justification for the need of its technology beyond saying that it is "critical to identify abnormal behavior" (self-definition) and does not point out potential privacy problems, such as the targeting of political opposition by surveillance, of DPI surveillance.

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, also technologies by Qosmos seem according to news reports to have been used: "Area is using equipment from American and European companies, according to blueprints and other documents obtained by Bloomberg News and the person familiar with the job. The project includes Sunnyvale, California-based NetApp Inc. (NTAP) storage hardware and software for archiving e-mails; probes to scan Syria's communications network from Paris-based Qosmos SA; and gear from Germany's Utimaco Safeware AG (USA) that connects tapped telecom lines to Area's monitoring-center computers" (*Bloomberg*, Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear. November 4, 2011. http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html).

"When the system is complete, Syrian security agents will be able to follow targets on flat-screen workstations that display communications and Web use in near-real time alongside graphics that map citizens' networks of electronic contacts, according to the documents and two people familiar with the plans. Such a system is custom-made for repression, says Mark Dubowitz, executive director of the Washington-based Foundation for Defense of Democracies, which promotes tighter sanctions against Syria. 'Any company selling monitoring surveillance technology to the Assad regime is complicit in human rights crimes,' he says. […] When Bloomberg News contacted Qosmos, CEO Thibaut Bechetoille said he would pull out of the project. 'It was not right to keep supporting this regime,' he says. The company's board decided about four weeks ago to exit and is still figuring out how to unwind its involvement, he says. The company's deep- packet inspection probes can peer into e-mail and reconstruct everything that happens on an Internet user's screen, says Qosmos's head of marketing, Erik Larsson" (ibid.).

change.org gathered 20 000 signatures for a petition against the project (change.org, How We Won, December 1, 2011.

http://www.change.org/petitions/demand-us-and-european-cos-stop-supporting-deadly-syria-net-surveillance). It was initiated by the Internet freedom group Access and the Syrian blogger Anas Qtiesh. Area SpA withdrew from the project. Also Qosmos withdrew its technology supply and released a news statement about this circumstance.

"Qosmos technology components are sold to third-party software vendors to improve performance in a wide variety of telecommunications, network infrastructure and cyber security applications. We share the concern about the potential for misuse of surveillance applications. As a result, Qosmos withdrew from the Syrian 'Asfador' project – a decision made prior to the system being finalized and prior to the initial story reported by Bloomberg on 3 November. Qosmos will neither supply nor support its technology to those who sell to authoritarian regimes. Qosmos is fully compliant in adhering to all laws related to the sale and use of its technology. Although the use of Lawful Interception (LI) solutions by telecommunications companies is mandated throughout the EU, US and most other countries worldwide to collect communications in accordance with local laws, recent political events have shown that further

regulation of LI, including more restrictive legislation, is required to prevent abuse" (*Qosmos*, Qosmos Statement about Recent Media Reporting. November 22, 2011. http://www.qosmos.com/news-events/qosmos-statement-about-recent-media-reporting).

The export of surveillance technology was in this circumstance only prevented because critical journalists and civil society stepped in. The involved companies, including Qosmos, seemed to have at first had no scruples about the possible use of their technologies for the monitoring of political opposition, which shows that it is difficult if civil society has to take the role of a watchdog that tries to correct and stop companies behaviour after it has actually happened or started. Civil society tends to have limited resources and one can ask what happens in those cases that remain unknown. If civil society and the media had not created pressure (e.g. because of lack of knowledge, resources, employees, etc), one can imagine that project "Asfador" would have been implemented and resulted in humans being tortured and killed for their political believes with the help of European surveillance technologies.

3. Thales

Place of business: Neuilly-sur-Seine, France
Website: http://www.thalesgroup.com
Self-description:
"With operations in 50 countries and 68,000 employees, Thales is a world leader in mission-critical information systems for defence and security, aerospace and transportation. Building on its expertise in the most sophisticated technologies and large-scale software systems, Thales is stepping up to the security challenges of its customers in an increasingly complex world. With its global network of 22,500 high-level researchers, Thales has earned particular recognition for its ability to develop and deploy dual civil and military technologies. Leveraging its international operations and spanning the entire value chain from equipment to systems and services, Thales is playing a pivotal role in making the world a safer place"
(http://www.thalesgroup.com/AboutUs.aspx).

"The emergence of new types of threats – from terrorism and organised crime to drug trafficking, mass immigration and cyber attacks – means that defence organisations alone are not fully equipped to contend with the changing risks. Safety and security requirements now transpiring at the national, European and international levels reflect the expectations and demands of the world's citizens. Analysing and addressing the risks involved calls for expertise that encompasses rigorous methods, proven technological capability and the appropriate organisational and human resources.

This convergence between defence and security has prompted the need for new solutions and technologies that enable organisations to share existing information and communication systems whilst also ensuring the traceability of individuals and the protection of networks and infrastructures.

Thales invests a significant share (18%) of its revenues back into innovation. Combined with the company's solid skills and experience in security systems, which today account for 25% of turnover, this puts Thales in a unique position for addressing the requirements of public authorities by developing surveillance and intelligence systems, identity systems, etc., and for contributing to the dependability and security of large-scale critical infrastructure such as railways, energy supply networks, sensitive sites and bank information systems"
(http://www.thalesgroup.com/Markets/Security/What_we_do/).

Analysis

In its product catalogue 2011 (#3_3), Thales offers two Internet surveillance systems: Net Spyder and IP Tr@pper. Net Spyder is an Internet surveillance system that is undetectable and automatically classifies and decodes accessed web pages, e-mails, web-mail access, chat use, webcam use, file transfer, voice over IP (VoIP, e.g. Skype) on the computers of an Internet Service Provider (#3_3, page 179). IP Tr@pper is a

hardware device that is connected to a Local Area Network (LAN) or Internet host or router. It scans the traffic and can analyse e-mails, web access, chat, file transfer, voice over IP, and online video access (#3_1; #3_3, page 180). Both Internet surveillance technologies can be used as standalone tools or integrated into the Spyder Monitoring centre (#3_3, page 180). Both can be classified as Deep Packet Inspection (DPI) technologies.

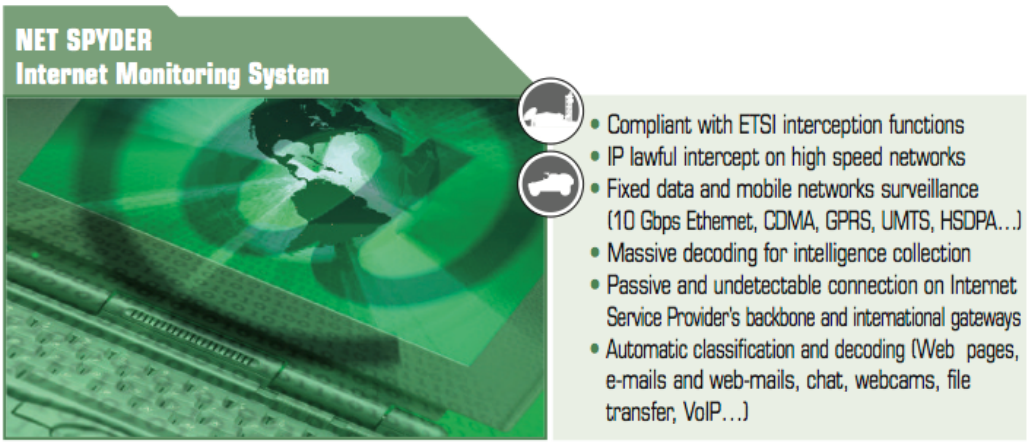


Figure 1: Product description of Thales' Net Spyder (data source: #3_3, page 179).

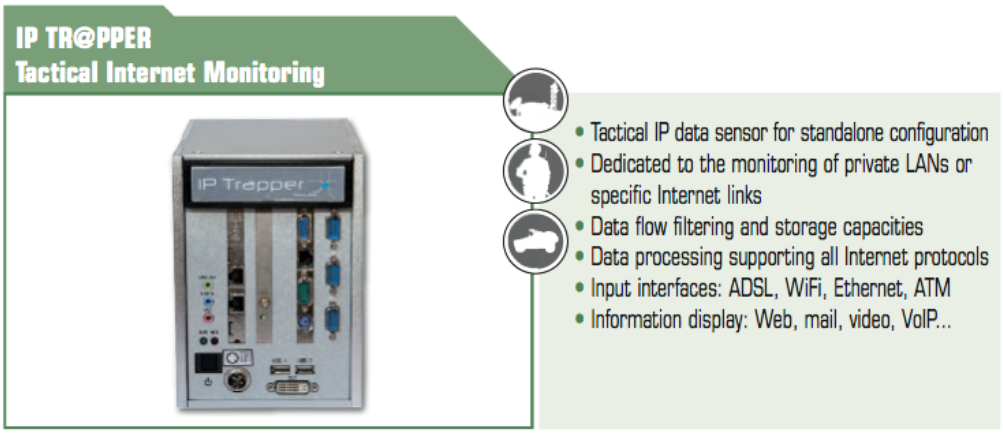


Figure 2: Product description of Thales IP Tr@pper (data source: #3_3, page 180)

In the analysed documents, potential negative aspects and privacy threats of Internet surveillance technologies are not mentioned. The world is presented as having become more insecure, which would require the employment of security and surveillance technologies in order to keep "populations, infrastructures and information secure" (#3_4): "Today's world is faced with multiple threats. Terrorism and cyber-

crime are on the rise, and natural disasters and epidemics loom. […] Digital information is circulating at rates never seen before […] Many traditional borders have become virtual, as globalisation is the norm. In this context, physical and cyber security are essential to protect all types of assets – people, infrastructures and data" (#3_4, 3). "State-of-the-art communications and surveillance systems are essential for effective early warning, crisis management, national defence and the protection of covert operations" (#3_4, 6). Producing and selling surveillance technologies is justified with reference to the need to keep society secure and the idea that we live in a risk society that is facing threats like terrorism and cybercrime.

In its 2010 Corporate Responsibility Report (#3_5), Thales says that one of its "principles is responsibility" is that "businesses should support and respect the protection of internationally proclaimed human rights and make sure that they are not complicit in human rights abuses" (#3_5, p. 4). It also addresses the topic of the export of weapons and security technologies (#3_5, pp. 18-19), saying 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). What is significant in this passage is that it is not mentioned that security technologies can harm the privacy and human rights of individuals, but that rather the focus is entirely on business interests and concerns about consequences that can negatively impact business performance.

4. AQSACOM

Place of business: Ulis Les, France
Website: http://www.aqsacomna.com
Self-description:
"Aqsacom develops and markets real time Lawful Interception, Data Retention, Mobility Tracking and Surveillance solutions. With its core business focused on lawful interception and related applications for over 14 years, Aqsacom provides end-to-end turnkey solutions for fulfilling lawful interception and data retention requirements anywhere in the world, especially over highly heterogeneous networking and services environments"
(http://www.aqsacomna.com/us/index.cfm?vSectionCode=ABOUTUS).

Analysis

Aqsacom argues that with "the popular acceptance of the Internet as a communications medium, there also comes a dark side to the Internet's power – namely the Internet's exploitation by criminals and terrorists" (#4_5, 3).

Aqsacom says that data should be captured and stored with the help of their technologies for multiple purposes: immediate action in matters of life and death and ongoing investigations, for possible investigations in the future (#4_1, 10). It refers to the EU's Data Retention Directive and says that technologies are needed that allow that "data will be stored between 6 months and up to 3 years" and that the "storing principles must allow effective mining" (#4_1, 14). Law enforcement agencies would "need ALL high priority data" that is relating to ongoing investigations and "people on 'high interest' list" (#4_1, 15). But also lower priority data would be needed in order to conduct "general analysis looking for 'fits' against defined criminal profiles" and for "potential later use if 'new' areas or people of interest are identified" (#4_1, 16). So Aqsacom is suggesting technologies that are used for storing a lot of data about Internet usage about suspicious people and the mass of users at large so that data analysis and data mining can be conducted based on these data for criminal investigation. Aqsacom's surveillance systems enable "extraction of call information and content from the network entities (voice or IP network equipment) and b) management of the data for effective delivery to the law enforcement agencies" (#4_2). The company explains that its surveillance technologies can operate at all seven layers of the OSI Reference Model, which means that they can also conduct the "direct extraction of intercepted content" (#4_5, 11). This means that Aqsacom's surveillance technologies can be classified as Deep Packet Inspection Internet surveillance technologies. It provides two surveillance systems:
ALIS (Aqsacom Lawful Interception System)
ADRIS (Aqsacom Data Retention Intelligence System)

ALIS is a system for the surveillance of "massive-scale public IP networks" (#4_2). It intercepts the IP address of specific users and then "routes a secure replication of all incoming/outgoing IP traffic to the law enforcement agency for analysis" (#4_2). The surveillor accesses the data "through an easy-to-use, common user interface" (#4_3). "ALIS' friendly graphical user interface allows for the easy automation of many operational interception tasks, such as the automatic triggering or stopping of an interception operation at predefined dates and times" (#4_5, 34). ALIS can also be used for the surveillance of voice over IP data (e.g. Skype).

ADRIS is a data storage system that can be used for data retention by Internet Service Providers (ISPs) and also enables the transport of retained data to law enforcement agencies. "The ADRIS Collection & Storage Module is responsible for the collection of retained data. This module can import transactional data from legacy platforms (e.g., billing systems) for non real-time Data Retention; however, a more dynamic, future-proof application of this module is in the real-time collection of live event data from switches, routers, probes, applications servers, and other network components. Once collected, the data are transformed on-the-fly (for real-time Data Retention) into an internal representation by the *Data Collection Mediation Function,* then sent to the *Data Retention Repository* (a large scale storage system). The ADRIS Consultation Module supports the querying of retained data that are stored in the Repository. This module contains the Retained Data Retrieval Function, which supports the Handover Interface (HI) with Law Enforcement Agencies to ensure a standards- compliant and secure means of requesting and obtaining the retained data. The Administration Module provisions ADRIS' communications with the required Law Enforcement Agencies. This module also instructs the Data Collection Mediation Function and network elements on what data are to be collected, while monitoring the data collection and delivery operations" (#4_6).

Aqsacom produces Internet surveillance technologies that can be classified as Deep Packet Inspection technologies. It also produces storage technologies for data retention. It justifies the production of these technologies by describing a threat of terrorist and criminal use of the Internet. It says that it is export-oriented, but on its website we could find no detailed information about which institutions in more than 30 countries are Aqsacom's customers and which technologies they have bought for which purposes.

Aqsacom does not specify to which countries it exactly has exported surveillance technologies. It mentions that it has customers from over 30 countries. AQSACOM's diversified customer portfolio includes clients from more than 30 countries, covering geographical areas as diverse as Central and Eastern Europe, Asia-Pacific, Africa and the Middle-East.

Aqsacom says that "due to the nature of LI [lawful interception], security must be taken very seriously to preserve the privacy of the target and the confidentiality of the investigation" (#4_3). Aqsacom wants to ensure its customers that its systems are secure so that "no confidential information can be extracted from the mediation management platform or its components" (#4_3) by unauthorized parties. Aqsacom does

not address concerns about the use of DPI for political repression and the creation of a society, in which everyone is seen as a potential criminal and terrorist, which reverses and practically abolishes the presumption of innocence and installs a large-scale surveillance of personal data. Aqsacom has not addressed critical questions that relate to privacy violations of citizens in the analysed documents.

5. Alcatel-Lucent

Place of business: Paris, France
Website: http://www.alcatel-lucent.com
Self-description:
"The long-trusted partner of service providers, enterprises, strategic industries and governments around the world, Alcatel-Lucent is a leader in mobile, fixed, IP and Optics technologies, and a pioneer in applications and services. Alcatel-Lucent includes Bell Labs, one of the world's foremost centres of research and innovation in communications technology. With operations in more than 130 countries and one of the most experienced global services organizations in the industry, Alcatel-Lucent is a local partner with global reach. The Company achieved revenues of Euro 16 billion in 2010 and is incorporated in France and headquartered in Paris" (http://www.alcatel-lucent.com/wps/portal/aboutus).

Analysis

Alcatel-Lucent is a global telecommunications company. One of the technologies it produces and sells is Alcatel Lucent 1357 ULIS – Unified Lawful Interception Sites (#5_1, #5_2). It argues that the "convergence of voice and data" (#5_2, 2) has made surveillance a difficult challenge and that ULIS 1357 provides a solution. The specific characteristic of this technology is that it can be used both for the monitoring of phone networks and the Internet, it is an integrated communication surveillance technology. The system "internal intercept function" allows "the intercept-related information and contents of communications" (#5_1, 4). This means that the technology can monitor Internet content, which makes it a Deep Packet Inspection surveillance tool. The system's "administration function" "delivers the data and content to the LEA" (law enforcement agency, #5_2, 4).

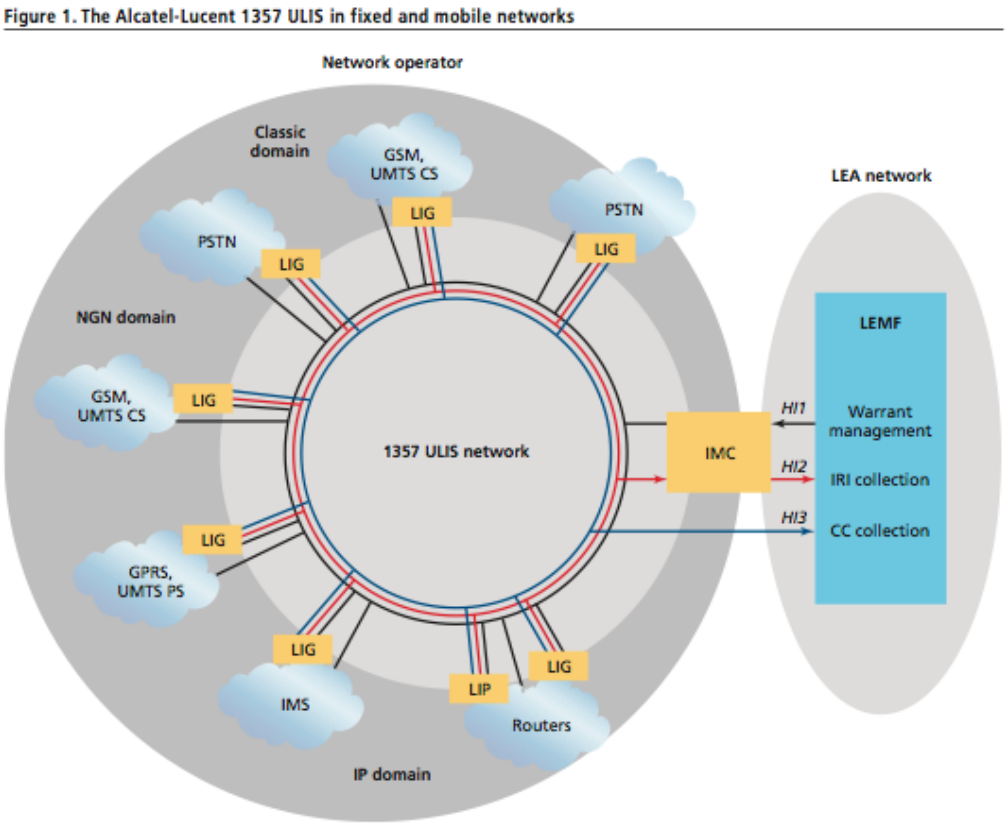


Figure 3: Altacel-Lucent's 1357 ULIS (data source: #5_2)

Alcatel-Lucent says that the 1357 ULIS system has been "deployed in more than 70 countries" (#5_2, 7; #5_1, 6), but does not specify which countries these are. Alcatel-Lucent says that it is "a long term leader in the Middle East, headquartered in Egypt with local presence in 19 countries", including besides Egypt e.g. Bahrain, Iran, and Syria (document Alctael-Lucent in the Middle East, http://www.alcatel-lucent.com/wps/ DocumentStreamerServlet?LMSG_CABINET=Docs_and_Resource_Ctr&LMSG_CONTENT_FILE=Corp_Governance_Docs/Midle_East-RU_PROFILE.pdf&lu_lang_code=en_WW) . Alcatel-Lucent also signed contracts with Libya Telecom and Technology (*Maghreb Confidential*. Alcatel-Lucent. May 9, 2008) and the Libyan Post Telecommunications & Information Technology Company (*Telecom Worldwide*. Alcatel-Lucent to provide fibre-optic backbone network contract for Libya. July 12, 2007) for installing Internet networks in Libya. We could find no information on Alcatel-Lucent's website to which countries it exported its 1357 ULIS system.

In its 2010 Corporate Responsibility Report (#5_3), Alcatel-Lucent devotes one of 108 pages to the topic of privacy. It says that it "is committed to respecting individuals' privacy rights and expectations and to protecting the personal data it collects

from unauthorized access, use, retention/storage and/ or disclosure" (#5_3, 23). The report addresses privacy protection at a very general level, no discussion of privacy concerns about Deep Packet Inspection Internet surveillance technologies such as 1357 ULIS is given. 1357 ULIS is neither mentioned, nor is it explained to which organizations, institutions and countries such technologies have been sold.

6. Amesys

Place of business: Les Milles, France
Website: http://www.amesys.fr
Self-description:
"Amesys est une entreprise française, leader dans la conception et l'intégration des systèmes critiques de haute technologie. Grâce à son expertise combinée de l'électronique et de l'informatique, Amesys s'adresse aux secteurs d'activités stratégiques": "Amesys is a French company, leader in the design and integration of critical systems of high technology. With its combined expertise in electronics and computing, Amesys targets strategic sectors"
(http://www.amesys.fr/index.php/fr/amesys/qui-sommes-nous)
"Acteur reconnu dans le domaine de la Défense, Amesys a construit sa renommée sur sa maîtrise des technologies militaires et son expertise technique en matière de guerre électronique"
"Recognized player in the field of defense, Amesys has built its reputation with its expertise in military technology and technical expertise in electronic warfare"
(http://www.amesys.fr/index.php/fr/secteurs-dactivites/defense).
In 2010, the French company Bull bought Amesys.

Analysis

Amesys distinguishes two types of surveillance systems: lawful interception and massive interception. "The main goal of Lawful interception is to analyze in deep the traffic of predefined targets. In LI systems, all the target's traffic is duplicated by the Service Provider (phone, mobile or Internet) and is sent to a centralized interception system. Then, the investigators analyze as deeply as possible all the traffic of each target" (#6_18, 5).

Massive interception allows the surveillance of "billions of communications" and to not only intercept a target's communication, but also "to provide the advanced tools needed to find potential new targets" (#6_18, 5). Such systems are able to "analyze the whole country's traffic in real time" and to store and archive data (#6_18, 5). They allow the "global search and surveillance of all Internet traffic" (#6_1). Figure 4 visualizes the differences between the two surveillance systems.

Amesys says that massive interception is needed "in the constant struggle against criminals and terrorism" (#6_1) in order to "reduce crime levels, protect from terrorism threats, and identify new incoming security danger[s]" (#6_1).

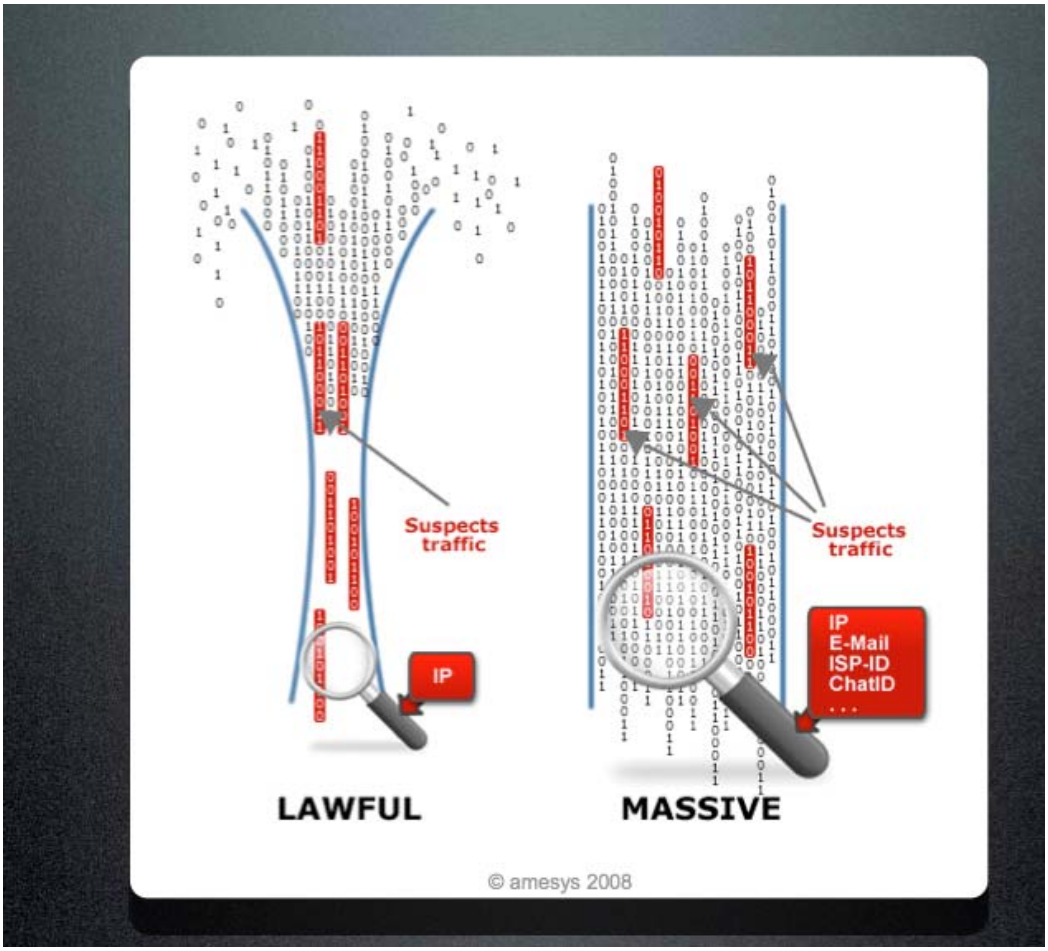


Figure 4: "Lawful interception" and "massive interception" (data source: 6_1).

Amesys' EAGLE surveillance system consists of a Captor collecting the data, a Data Center that classifies and stores data, the Monitoring Center and Smart Analysis Tools (#6_18, 6). Amesys describes EAGE as providing "a centralized point of view" because it can "aggregate different sources of information" and allows the surveillance of different networks (such as the Internet, analogical phones, mobile phones, satellite phones) (#6_1, see also figure 5). With the help of software, the results of the conducted surveillance are displayed to controllers sitting in monitoring centres (#6_5, 7).

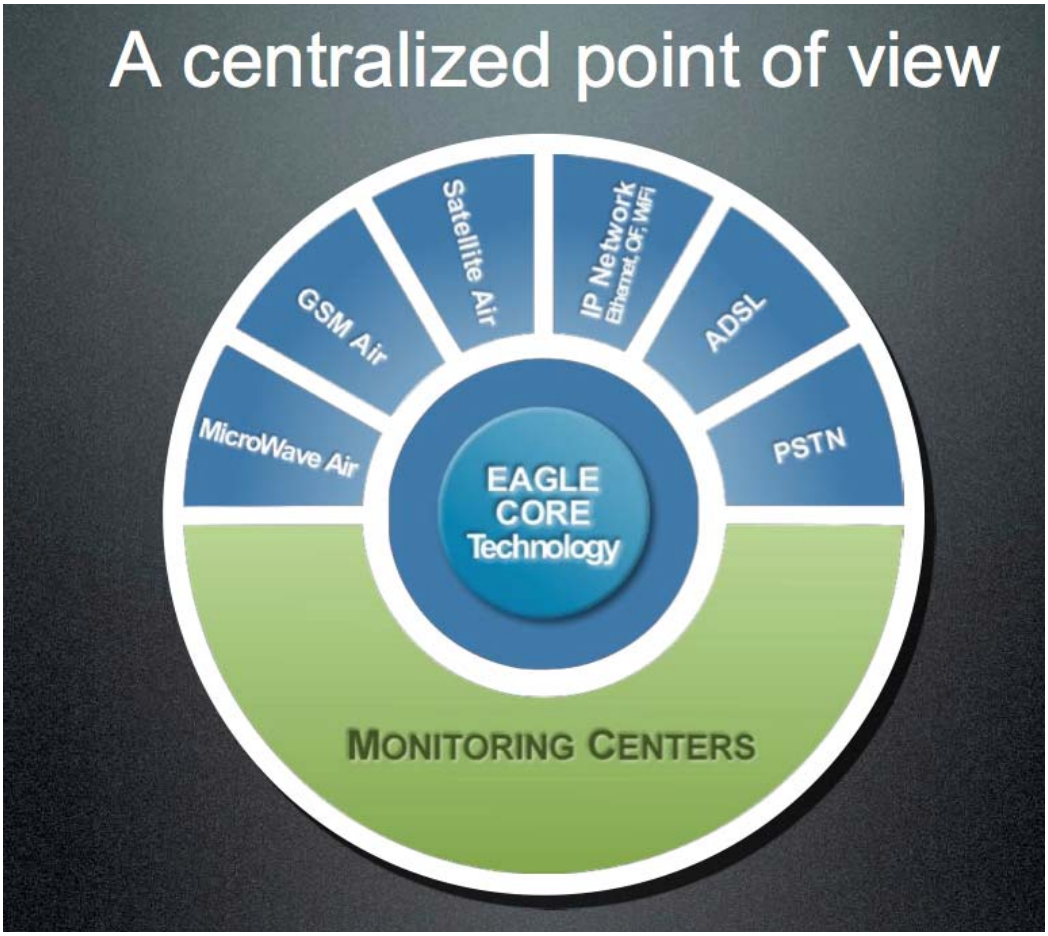


Figure 5: Amesys' EAGLE system (data source: #6_1)

Amesys' notion of surveillance systems that build a central point of view reminds of Foucault's notion of surveillance as panopticism. Surveillance is based on "a principle of compulsory visibility" that is exercised through the invisibility of disciplinary power (Foucault 1977, 187), it "must see without being seen" (171), is "capable of making all visible, as long as it could itself remain invisible" (214), it is a "system of permanent registration" (196) in which "all events are recorded" (197), a "machine for dissociating the see/being seen dyad" (202). "One is totally seen, without ever seeing" (202). "He is seen, but he does not see; he is the object of information, never a subject in communication" (200). "the panoptic mechanism basically involves putting someone in the center – an eye, a gaze, a principle of surveillance – who will be able to make its sovereignty function over all the individuals [placed] within this machine of power. To that extent we can say that the panopticon is the oldest dream of the oldest sovereign: None of my subjects can escape and none of their actions is unknown to me. The central point of the panopticon still functions, as it were, as a perfect sovereign" (Foucault 2007, 93f). Based on Foucault one can say that Amesys aims to build systems that perfect sovereignty by making unknowns known to those who control the system.

Figure 6 shows a model of the EAGLE surveillance system.

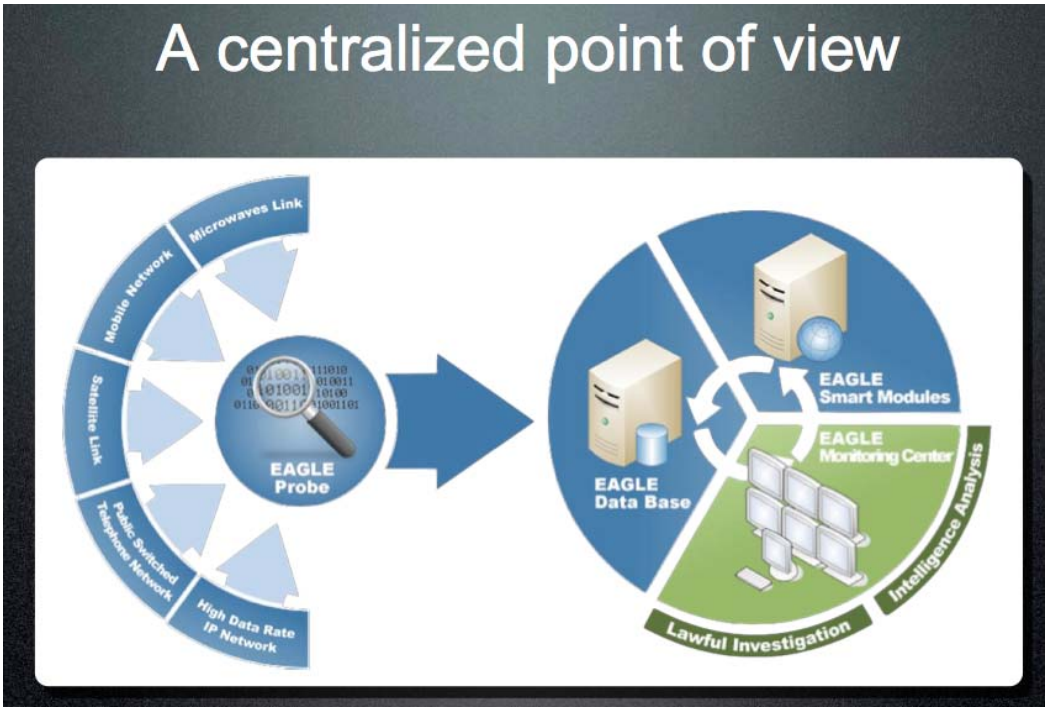


Figure 6: Amesys' EAGLE system

The EAGLE system provides "tactical" tools (SMINT, SMAW) and "strategic" tools (GLINT, GLAW) (#6_1). The tactical tools are portable and can be plugged into an IP network for analysing the content of a network (#6_5, 10). In contrast, the "massive system is designed to answer to the need of interception and surveillance on a scale of nation" (#6_5, 10).

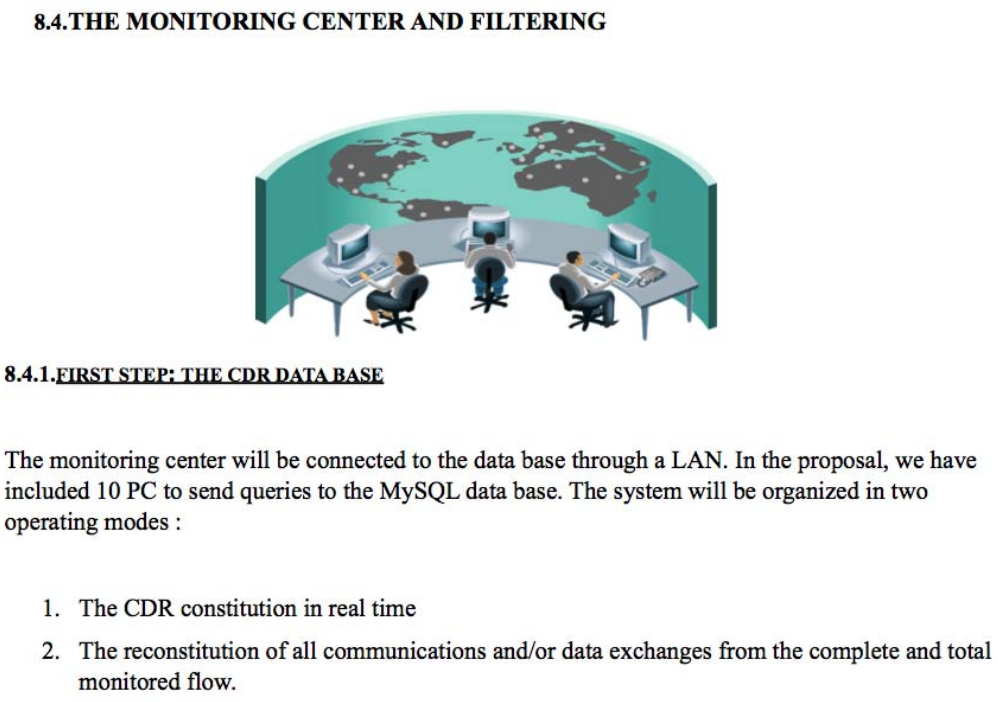
The EAGLE GLINT system can retrieve, store and analyse data coming from more than 300 different Internet protocols (mail, webmail, VoIP, chat, http, search engines, file transfer) (#6_9, 5f; #6_12). Amesys says that is a "core technology" that "is designed to help Law Enforcement Agencies and Intelligence organization[s] to reduce crime levels, to protect from terrorism threats and to identify new incoming security danger[s]" (#6_9, 4). It is a Deep Packet Inspection technology that can "record, decode, store and display the intercepted network traffic" (#6_12). "GLINT is a system designed to monitor and intercept in real time information on [a] very high data rate network" (#6_12). GLINT is not limited to Internet surveillance, but enables also the surveillance of fixed line-, mobile- and satellite phone networks, and microwave transmission (#6_12).

SMINT is a portable Deep Packet Inspection surveillance technology that is "pluggable directly" to an IP network, works on the most common protocols, focuses on the monitoring of IP traffic, can "record days of traffic", analyse surveillance data (#6_11). "SMINT is a tactical system designed to record, store, analyse and display in real time

information. This system is able to monitor a wide range of protocols, including mail, voice over IP (VoIP), webmail, chat, web browsing …" (#6_11).

i2e Technologies was created in 1979 and was fused in 2007 with Artware to form the company Amesys (http://www.crescendo-industries.de/index.php?g=0&s=2). A document (#6_15) specifies a surveillance system that i2e Technologies, according to the document, planned to deliver to Libya. The systems described are able to monitor phone networks and the Internet. The document says that there was a visit of i2e to Libya on the 10th and 11th of May, 2006, and a visit of Libyan officials to the company's French offices (#6_15, 3). "This document is our technical specification for your homeland security project. It covers all aspects discussed between the various teams of experts from your organisation and our company" (#6_15, 3).

The document among other things describes a "Network Stream Analyser" that "is mainly designed to monitor all Internet traffic and intercept those mails that may content information relevant to the Public Safety System Organisation" (#6_15, 26). The system can monitor various Internet protocols (#6_15, 27). It allows e.g. the surveillance of e-mail content, attachments, web sites browsed, chat messages, the search for keywords in captured e-mails, the capture of traffic from and to an IP address, the monitoring of specific telephone numbers (#6_15, 37). The document also talks about the set up of monitoring centres (see figure 7).



8.4.THE MONITORING CENTER AND FILTERING

8.4.1.FIRST STEP: THE CDR DATA BASE

The monitoring center will be connected to the data base through a LAN. In the proposal, we have included 10 PC to send queries to the MySQL data base. The system will be organized in two operating modes :

1. The CDR constitution in real time
2. The reconstitution of all communications and/or data exchanges from the complete and total monitored flow.

Figure 7: Monitoring centres (data source: #6_15, 32).

Figure 8 shows a model of the entire Internet surveillance system specified in the document. The document also specifies that 3 Libyan engineers should spend 2 months in Paris in order "to assist and help the Arabisation and customization of the

system", that there would be a 2 week long training and that "two i2e engineers will be installed in Tripoli for the 6 first months to help the customer in any matter" (#6_15, 43).

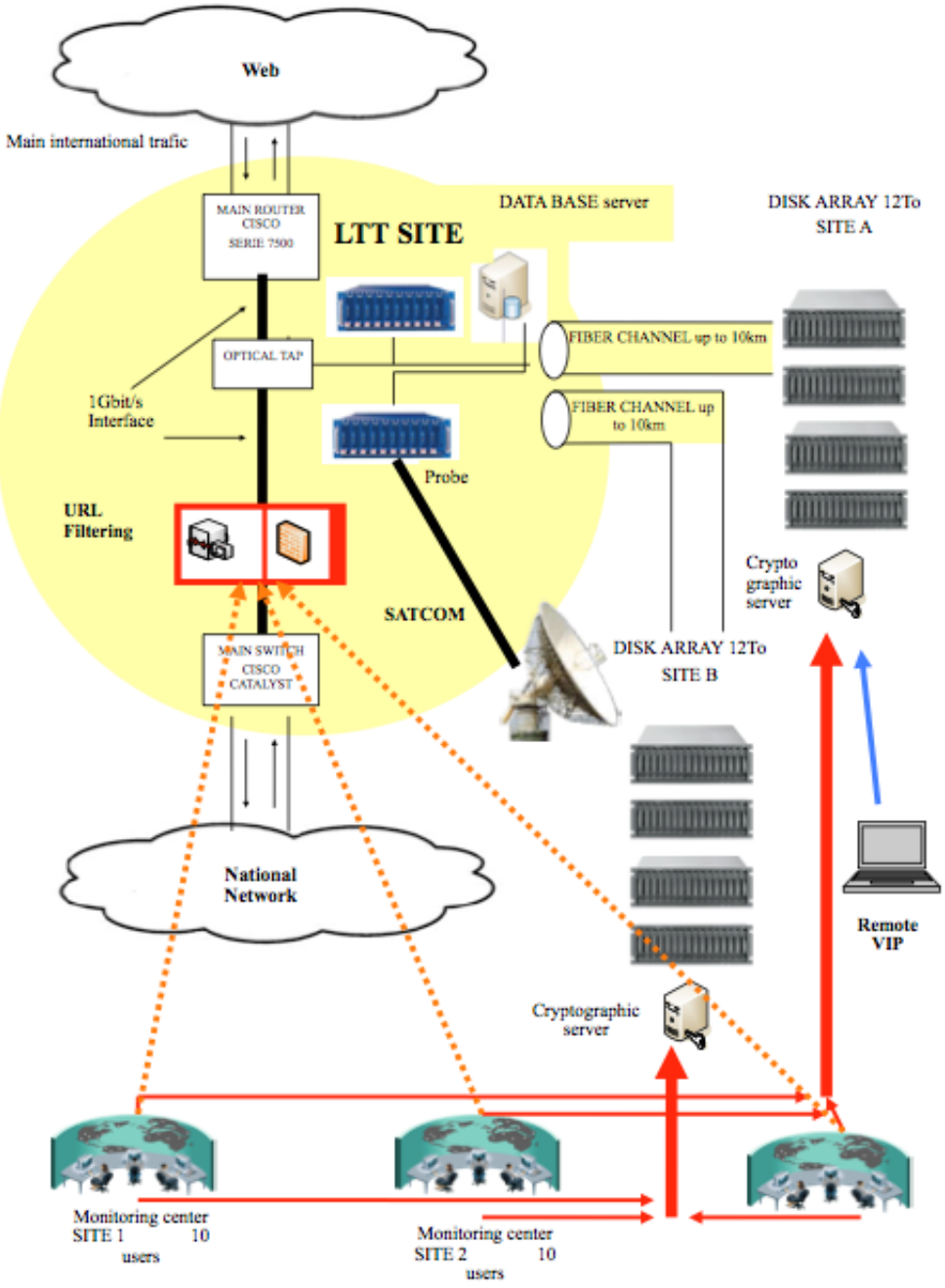


Figure 8: Internet surveillance system planned by i2e (data source: #5_15, 42)

Bull's CEO Philippe Vannier describes the activities of Amesys-Bull in the area of defence: "When it comes to defense of course one thinks of missiles, etc… But there's another aspect of the defense landscape that's all about controlling information, searching information… so naturally you'd try to be able to analyze everything that's circulating around these communications networks whether it's voice traffic, images, data and here, with the Amesys-Bull combination we're offering some totally unique tools" (subtitles taken from a French video by Bull: http://www.bull-world.com/c_TancXb_en_security).

In August 2011, the *Wall Street Journal* wrote that the Amesys sold deep packet inspection technologies to Libya, where, according to the Wall Street Journal, Gaddafi'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. August 30, 2011). The International Federation for Human Rights and the *Ligue des Droits de l'Homme et du Citoyen* filed criminal charges against Amesys (*FIDH*, FIDH and LDH file a complaint concerning the responsibility of the company AMESYS in relation to acts of torture. October 19, 2011):

"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 recently abandoned room is lined with posters and English-language training manuals stamped with the name Amesys, a unit of French technology firm Bull SA, which installed the monitoring center. A warning by the door bears the Amesys logo. The sign reads: 'Help keep our classified business secret. Don't discuss classified information out of the HQ'. The room, explored Monday by The Wall Street Journal, provides clear new evidence of foreign companies' cooperation in the repression of Libyans under Col. Gadhafi's almost 42-year rule. The surveillance files found here include emails written as recently as February, after the Libyan uprising had begun. […]

This kind of spying became a top priority for Libya as the region's Arab Spring revolutions blossomed in recent months. […] 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. […]

Gadhafi's regime had become more attuned to the dangers posed by Internet activism, even though the nation had only about 100,000 Internet subscriptions in a population of 6.6 million. The Eagle system allows agents to observe network traffic and peer into people's emails, among other things. In the room, one English-language poster says: 'Whereas many Internet interception systems carry out basic filtering on IP address and extract only those communications from the global flow (Lawful Interception), EAGLE Interception system analyses and stores all the communications from the monitored link (Massive interception)'. [...] In a basement storage room, dossiers of Libyans' online activities are lined up in floor-to-ceiling filing shelves"

(*Wall Street Journal Online*, Firms aided Libyan spies. First look inside security unit shows how citizens were tracked. August 30, 2011).

Peter Bouckaert, Human Rights Watch's emergencies director, expressed the concern that Western companies and governments take actions to destroy evidence of their support of Gaddafi and the surveillance of the political opposition in Libya (*The Times*, West tries to cover up Libya deals: The race is on to seek out and destroy any incriminating evidence. October 7, 2011).

In a press release, Amesys disputed the claim that it installed a surveillance system in Libya and announced that it reserves the right to file suit against those who make such claims:

"Amesys signed a contract with the Libyan authorities in 2007. The relevant hardware was delivered in 2008. The contract was related to the making available of analysis hardware concerning a small fraction of the Internet lines installed at that time (a few thousand). This did not include either Internet communications via satellite (as used in Internet cafes), encrypted data such as Skype-type communications, or filtering of Web sites. In addition, the hardware used did not allow for the monitoring of either fixed or mobile telephone lines.

The contract was concluded at a time when the international community was in the process of diplomatic rapprochement with Libya, which was looking to fight against terrorism and acts perpetrated by Al Qaeda (2007 was the year in which the Bulgarian nurses were released). (In December 2007 Muammar Gadhafi made an official visit to France; in July 2009 Muammar Gadhafi met with Barack Obama in Italy). All Amesys' business dealings comply rigorously with the legal and regulatory requirements set out in international, European and French conventions. Amesys does not operate any telephone or Internet monitoring centers, anywhere worldwide. [...] Amesys reserves its rights in relation to any infringement that may affect its image or reputation"

(Amesys, Press release. September 1, 2011.
http://www.wcm.bull.com/internet/pr/new_rend.jsp?DocId=673289&lang=en).

So there are two different stories: On the one hand journalists and human rights activists who say that they discovered a Libyan monitoring centre and that "Amesys in 2009 equipped the center with 'deep packet inspection' technology". On the other hand Amesys that says that it does not operate such centres. And there is a document released by WikiLeaks (#5_15) that if authentic seems to suggest business relations between i2e and Libya.

7. Elaman

Place of business: Munich, Germany
Website: http://www.elaman.de
Self-description:
"ELAMAN, with its headquarters in Munich/Germany and its subsidiaries in Dubai/United Arab Emirates and Malans /Switzerland, specializes in security requirements for government and law enforcement worldwide. Our aim is to provide comprehensive security products and solutions, technical consultancy and services as well as professional training for our customers" (http://www.elaman.de/company-profile.php) . The company was established in 2004 (#7_2, 1).

Analysis

Elaman justifies its production if surveillance technologies with the need to fight crime and terrorism: Lawful interception is needed "for investigating and prosecuting criminal activities and terrorism" (#7_10, 11).

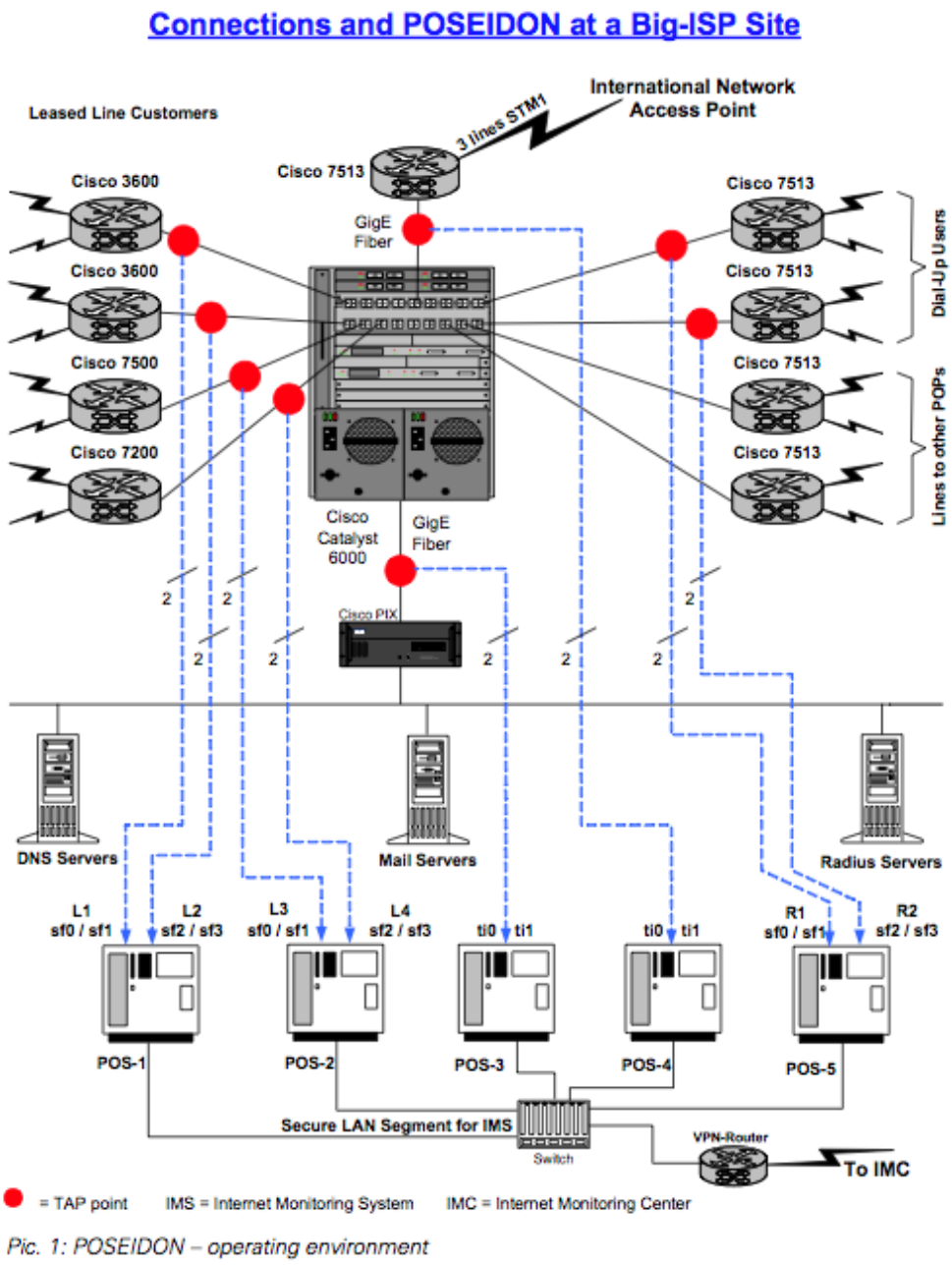
One of the analysed documents is a product specification of the CS-2000 High End (#7_4), a high performance network platform that has a Deep Packet processing module (DPPM) that can "detect and track up to 1 million simultaneous flows" (#7_4) and conduct "up to 5 gigabits per second L2-7 inspection and analysis". Other technologies advertised by Elaman include for example a peer to peer (p2p) traffic filter (#7_5), the portable IP monitoring system Poseidon Flyer (#7_6), the portable modem interception system Munin POTS (#7_7), or the POSEIDON Internet Monitoring Center (#7_9).

"POSEIDON Mobil is a portable system for recording, reconstruction and evaluation of IP-data and their applications, e.g. email, web-sessions, chat. […] POSEIDON Mobil consists od three functional parts. The recording of the raw data, picked up from different kinds of communication lines, the database management for internal organizational purposes of these data and the reconstruction function to analyze and evaluate the recorded IP-based data" (#7_6, 2).

Munin POTS intercepts Internet data sent from one source over a modem. It is "a true portable modem intercept solution to be used in operations, where direct access to the target lines is required. This unit can be deployed in the field close to the target or installed on a permanent basis in a monitoring centre" (#7_7, 3). It can monitor data from different protocols, such as websites, e-mails and attachments, chat, VoIP, and file transfer, messenger services.

The POSEIDON Internet Monitoring Center "is an equipment for recording, reconstruction and evaluation of IP-Data, which are passively recorded from different communication lines. It reads the data, filters them according to predefined filter criteria […], adds a timestamp to the data (NTP-Server) and saves the data in raw format

in a database. Using the Analyzer User Interface the data can – even online – be re-constructed and evaluated" (#7_9). Figure 9 shows that Poseidon typically processes Internet data from Internet Service Providers (ISPs). POSEIDON can monitor content from a lot of different protocols, for example e-mail, WWW (http, smtp), chat, FTP, or VoIP.



Pic. 1: POSEIDON – operating environment

Figure 9: POSEIDON Internet Monitoring Center (data source: #7_9, 3)

A document that presents Elaman's "Communications Monitoring Solutions" (#7_12) for the surveillance of phone networks, satellite communication, SMS, the Internet, and Radio Frequency Monitoring (RFM), and various other tools (such as FinFisher and speech identification software) specifies one task of data retention technologies in the following way: "In the field of telecommunications, data retention generally refers to the storage of call related information (numbers, date, time, position, etc.) of telephony and internet traffic. The stored data is usually telephone calls made and received, emails sent and received, web-sites visited and location data. The primary objective in data retention is traffic analysis and mass surveillance. By analysing the retained data, governments can identify an individual's location, their associates and members of a group, *such as political opponents*" (#7_12, 17; emphasis added).

Elaman advertises its surveillance products and services as well as surveillance technologies by other companies as means for fighting terrorism and crime. The technologies described in this section can be classified as Deep Packet Inspection Technologies, they allow to monitor the content of Internet communication and other forms of communication. In the analysed documents, we could not find any comments about privacy violation concerns and the limitation of human rights that may arise from the use of DPI Internet surveillance and related forms of surveillance. In contrast, as shown, Elaman says that data retention can help governments to identify "members of a group, such as political opponents" (#7_12, 17). The question that arises here is if 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 ("Everyone has the right to freedom of peaceful assembly and to freedom of association at all levels, particular in political, trade union and civic matters, which implies the right of everyone to form and join trade unions for the protection of his or her interests"). The European Convention of Human Right allows restricting this freedom if it is "necessary in a democratic society in the interests of national security or public safety, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others". 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 and also raises the question if the formulation disrespects the EU's Data Protection Directive (95/46/EC) that prohibits "the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" (article 8).

Elaman offers in a newsletter (#7_10) seminars for the use of Gamma International's FinFisher IT intrusion software as well as an intrusion portfolio offered together by Elaman and Gamma. FinFisher is a so-called "Trojan horse", a software that once installed allows the intruder remote access. FinFisher can infect computers, mobile phones, local networks and ISP networks and extract data from these systems (#7_10, 4-10). The product and training for it was also advertised in Eleman's Communica-

tions Monitoring catalogue from October 2007 (#7_2). FinFisher can e.g. be tarned as a software update that is sent to a computer or mobile phone (*NDR*. ZAPP: Germany Spyware for Dictators. December 7, 2011.
http://www.ndr.de/fernsehen/sendungen/zapp/media/zapp4923.html).

The German regional public service TV station NDR reported about a secret offer of the UK company Gamma to the Egyptian state for the FinFisher technology (*NDR*. ZAPP: Germany Spyware for Dictators. December 7, 2011.
http://www.ndr.de/fernsehen/sendungen/zapp/media/zapp4923.html).

The Egyptian blogger Mostafa Hussein, who discovered the documents, argued in the NDR report that this software is "exactly like weapons" (ibid.). The Egyptian Internet activist Israa Abdel Fattah was interviewed, saying that this software is "helping the dictators […] to […] attack the activism" (ibid.). Her own Internet communication was surveilled by the Egyptian government. She said that surveillance companies "only think about money" (ibid.). NDR also describes Gamma's attempts to sell surveillance technologies to Turkmenistan and Oman (ibid.). The Austrian IT journalist Erich Möchel said that surveillance technology companies encourage "repression and torture" (ibid.). Elaman does not produce FinFisher, it rather advertises this technology and seminars for its use. The NDR report also mentioned and problematized the quotation by Elaman about the surveillance of political opponents (ibid). NDR concluded that "critical questions are evidently unwelcome in this industry" (ibid.).

Elaman also advertised the Nokia Siemens Monitoring Centre in one of its documents (#7_2). The Austrian journalist Erich Möchel reported in April 2008 that "with high likelihood are surveillance systems developed by Siemens Munich used in countries like China, Iran and other totalitarian states for tracking dissidents, ethnical and religious minorities"[7] (Möchel, Erich. Datenjagd auf Dissidenten. April 7, 2008. http://www.fuzo-archiv.at/artikel/268868v2/). Asked for a comment by the Austrian Broadcasting Company ORF that published Möchel's report, Nokia Siemens commented: "Following the wish of our customers, we unfortunately cannot disclose, which organisations have bought our solutions"[8] (ibid.).

Elaman has in a document expressed that surveillance technologies can be used for identifying political opponents. Political reality shows that some of the technologies that it advertised in its documents have been used for this very purpose: According to reports, Gamma's FinFisher was used in Egypt to monitor the communications of political activists like Israa Abdel Fattah. Elaman has in one of its documents advertised the capacity of surveillance technology to "identify an individual's location, their associates and members of a group, such as political opponents" (#7_12, 17).

[7] "Mit hoher Wahrscheinlichkeit werden von Siemens München entwickelte Überwachungssysteme in Ländern wie China, dem Iran und anderen totalitären Staaten zur Verfolgung von Dissidenten, ethnischen und religiösen Minderheiten eingesetzt".

[8] "Dem Wunsch unserer Kunden entsprechend können wir leider nicht bekanntgeben, welche Organisationen unsere Lösung gekauft haben".

8. Datakom

Place of business: Ismaning, Germany
Website: http://www.datakom.de/
Self-description:
"The DATAKOM GmbH is a leading technology-integrator and service provider on the ICT market. Since 1986 offer we trend-setting test-, analysis-, security- and management-systems for all communications networks"[9] (http://www.datakom.de/ueber-uns.html)
"Monitoring means the plugging of a monitoring probe to data lines for surveillance of the network. At line speed, the data are detected, decoded, stored and analysed according to different aspects (Deep Packet Inspection, DPI)"
(http://www.datakom.de/netzwerk-analyse-simulation/netzwerk-monitoring.html)[10].

Analysis

Datakom says that for lawful interception "every bit and byte has to be analyzed" in order to create "Application/Content Awareness" (#8_1). It therefore promotes Deep Packet Inspection (DPI) technologies that create "TOTAL visbility at network speed" (#8_1; see also figure 10).

Datakom provides the installation of surveillance technologies as a service that is primarily directed at companies that want to monitor their internal networks (#8_2). Datakom also operates an Interception Centre in Bremen and offers to telecommunications operators the service to route law enforcement request for targeted surveillance over this monitoring centre (#8_3).

Datakom propagates the panoptic idea of "total visibility" of communication networks with the help of DPI surveillance technologies. We could in the analysed documents and on Datakom's website not find any discussion of data protection, privacy and ethical problems that may arise due to DPI.

[9] "Die DATAKOM GmbH ist führender Technologie-Integrator und Serviceprovider am ITK-Markt. Seit 1986 bieten wir richtungsweisende Test-, Analyse-, Sicherheits- und Managementsysteme für alle Kommunikationsnetze".

[10] "Monitoring bedeutet das Aufschalten einer Monitorprobe auf Datenleitungen zur Überwachung des Netzwerks. Die Daten werden in Leitungsgeschwindigkeit erfasst, decodiert, gespeichert und nach unterschiedlichen Gesichtspunkten analysiert (Deep Packet Inspection, DPI)".

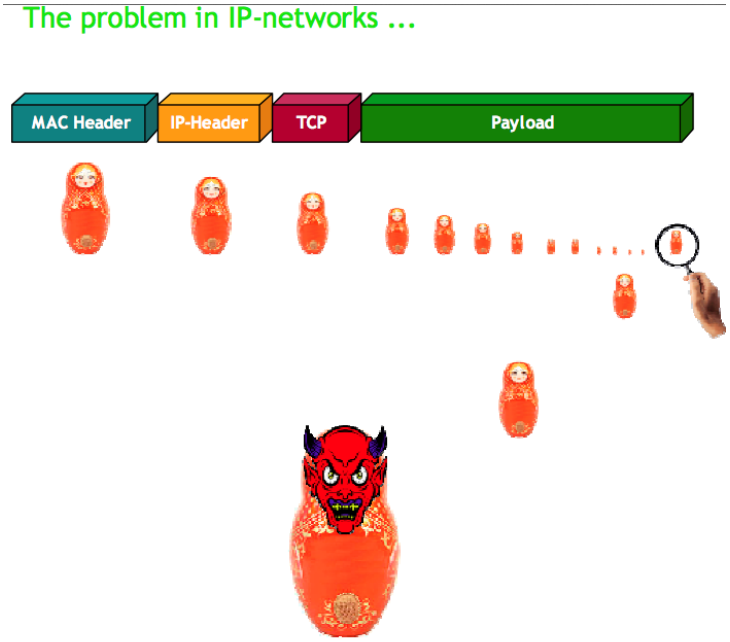


Figure 10: Datakom's vision of total visbility (data source: #8_1)

9. trovicor

Place of business: Munich, Germany
Website: http://www.trovicor.com/
Self-description:
"trovicor stands for almost two decades of customer-centric developments providing state-of-the-art intelligence solutions. trovicor is an industry leader who provides turnkey intelligence solutions. These solutions are based on our own state-of-the art core developments integrating best-in-class third party products and our customer-centric Care Programmes.
At present we employ some 170 experts worldwide. Our headquarters in Munich address Europe, the Community of Independent States (CIS) and both Americas; our subsidiaries in Dubai and Islamabad cater for the Middle East and Africa; the Kuala Lumpur office focuses on Asia Pacific.
Based on our vast experiences our main business goal has always been to generate sustainable benefits for law enforcement and government agencies. In the course of developing many and varied Monitoring Center solutions as well as other intelligence projects, we have gained an in-depth experience of their requirements"
(http://www.trovicor.com/en/about-us/in-brief.html).
"Our vision: 'Being the leading solution provider for the intelligence community' - reflects our passion to build a solution driven and sustainable business for a successful future.
Our mission: 'Making the world a safer place' - expresses the understanding of our mission for today and tomorrow. We are convinced that our expertise helps to maintain and enhance pre-emptive security, and thus contributes to the quality of all peoples' lives. […]
We don't just philosophise about warnings like 'without security, there is no freedom'; together with our partners we can help to increase safety and security. Good governance has to take appropriate actions to make the world a safer place for individuals, families and nations. We believe that this is where true freedom begins"
(http://www.trovicor.com/en/about-us/philosophy.html).

Analysis

On March 31st, 2009, Nokia Siemens Networks sold its Intelligence Solutions branch to Persua GmbH (Nokia Siemens Networks, Provision of Lawful Intercept Capacity in Iran. June 22, 2009. http://www.nokiasiemensnetworks.com/news-events/press-room/press-releases/provision-of-lawful-intercept-capability-in-iran) that now operates it under the name trovicor GmbH (*Spiegel Online International*, Western Surveillance Technology in the Hands of Despots. December 8, 2011). We will therefore in the analysis focus partly on Nokia Siemens Networks' surveillance technologies.

trovicor justifies its business operations with the need to fight crime and terrorism: "Never before has information been exchanged so fast and in so many ways. Needless to say that criminals and terrorist organisations have also been fast to realise the vast opportunities presented by modern telecommunications. 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).

trovicor produces and sells a Monitoring Center (MC): "The trovicor Monitoring Center (MC) has been specifically developed to serve the complex needs of law enforcement and national security agencies worldwide. It enables them to intercept, retain, analyse, investigate and distribute intercepted voice and data communication as well as historical data. It's usage spans from intercept of communications in fixed and mobile networks to Next Generation Networking and Internet"

(http://www.trovicor.com/en/business-sections/communication-monitoring.html).

"In order to deliver, store and analyse data, such as telephone numbers, date, time, content etc. that were gained through the interception of telecommunication networks a Monitoring Center (MC) is needed. The Monitoring Center can decode, store, view the data and prepare them for the respective analysis. The interface technology used between the Monitoring Center and the telecommunication network is related to its format, e.g. PSTN, GSM, UMTS, CDMA, IP. Additionally the network provider defines the switch technology used (Nokia-Siemens, Ericsson, Alcatel-Lucent, Cisco, etc.)"

(http://www.trovicor.com/en/business-sections/lawful-interception.html).

Elaman's Communication Monitoring product catalogue from October 2007 (#7_2) contains a product sheet of the Nokia Siemens Monitoring Center. It is described as "making the world safer with trend-setting intelligence solutions", "using telecommunications to target terrorism and crime" (#7_2). The vision communicated is "that our expertise will enhance peace and thereby contribute to the quality of peoples' lives" (#7_2). This part of Elaman's product catalogue holds the address and a copyright notice by Nokia Siemens Networks. The Nokia Siemens Monitoring Center can intercept data from mobile and fixed line phone networks and the Internet (#7_2). The task for the use of the Monitoring Center would be to "discover hidden patterns and criminal structures, anticipate and prevent crimes", "fighting crime and thwarting terrorist attacks" because "criminal groups and terrorist organizations also have been quick to realize the vast opportunities presented by modern communications" (#7_2). Another system advertised in Elaman's Communication Monitoring catalogue is Siemens' IP Interception System – IPIS (#7_2) that "is capable of intercepting data in the Internet, in other IP based networks and VoIP in Next Generation Networks" (#7_2). IP data can be extracted from email, the WWW, VoIP, and instant messaging (#7_2).

In April 2009, the Washington Times reported that Nokia Siemens sold a Monitoring Centre to Iran:

"Nokia Siemens Networks (NSN), a joint venture between the Finnish cell-phone giant Nokia and German powerhouse Siemens, delivered what is known as a monitoring center to Irantelecom, Iran's state-owned telephone company. A spokesman for NSN said the servers were sold for 'lawful intercept functionality,' a technical term used by the cell-phone industry to refer to law enforcement's ability to tap phones, read e-mails and surveil electronic data on communications networks. In Iran, a country that frequently jails dissidents and where regime opponents rely heavily on Web-based communication with the outside world, a monitoring center that can archive these intercepts could provide a valuable tool to intensify repression. Lily Mazaheri, a human rights and immigration lawyer who represents high-profile Iranian dissidents, said she had suspected that the government had increased its capability to monitor its perceived enemies.

Recently, one of her clients was arrested because of instant messaging he had participated in with Ms. Mazaheri, she said. 'He told me he had received a call from the Ministry of Intelligence, and this guy when he went to the interrogation, they put in front of him printed copies of his chats with me. He said he was dumbfounded, and he was sent to prison.'

[…] Hadi Ghaemi, spokesman for the International Campaign for Human Rights in Iran, said 12 women´s rights activists were arrested late last month at a private meeting to celebrate the Persian New Year. He said the raid suggested the state had access to private communications.

'This is an absolute threat to the privacy of all Iranian activists. It puts them in danger of being constantly monitored by the intelligence services, something that we know is already happening,' Mr. Ghaemi said" (*Washington Times,* Fed Contractor, Cell Phone Maker Sold Spy System to Iran. April 13, 2009).

The Iranian journalist Isa Saharkhiz was jailed for three years "on charges of insulting Iran's supreme leader and spreading propaganda against the regime. […] Last month, Saharkhiz filed a lawsuit against Nokia Siemens, accusing the company of delivering surveillance equipment to Iran that helped the authorities trace his whereabouts through his cell phone" (*BBC Monitoring World Media*, Prominent Iranian Journalist Jailed for Three Years. September 30, 2010).

Nokia Siemens commented on media reports: (*ARD Tagesthemen*, Siemens-Nokia Überwachungstechnik im Iran. June 24, 2009.

http://www.youtube.com/watch?v=8JbydEFBx5E). "The system can only record, it cannot identify anybody" (Stefan Zuber)[11]. The journalist Erich Möchel in contrast said: "One can geographically locate with these monitoring centres, where persons are, one can create their communication profile, with whom they communicate.

[11] "Das System kann nur aufzeichnen, es kann niemanden identifizieren. Es ist nicht geeignet, um Zensur zu üben".

Groups can be investigated"[12] (ibid). A product specification of the Nokia Siemens Monitoring Center (provided in one of Elaman's brochures) explains that it supports the "fully automatic recording of all data concerning all activities of the target" and makes "nationwide monitoring possible" (#7_2). So the relevant aspect is not that it does not censor the Internet, but rather that Nokia Siemens' Monitoring Center can monitor the activities and communications of political activists.

A former employee of Nokia Siemens reported that he was part of the installation of a Monitoring Centre in Iran (ZDF Frontal21, Nokia-Siemens-Networks im Iran. January 26, 2010. http://www.youtube.com/watch?v=oHqyKYa6Ffw). Siemens Board Memebr Joe Kaeser said: "There is today no reason for us to assume that NSN has acted unlawfully or unorderly"[13]. In the same report, the two Iranian political activists Poojan Mahmudian and Kianoosh Sanjari reported that they were imprisoned and that their communications were monitored (ibid.).

In its Corporate Responsibility Report 2009, Nokia Siemens' CEO Rajeev Suri wrote: "Over the past year we have seen allegations that telecommunications technology, including that provided by Nokia Siemens Networks, has been used to suppress human rights instead of enhancing them. This is not a simple issue as technology that is designed to benefit society can be used for other purposes and, of course, governments can change over time" (Nokia Siemens Networks 2009, 4). This statement implies that a Monitoring Center is designed for benefiting society and that its use for repression of political opponents is an unintended side-effect. The question is if the purpose of the use of such a technology for repression is not foreseeable if a company enters a business deal with Iran.

In a statement issued in June 2009, Nokia Siemens argued that the surveillance centre it delivered to Iran had "the capability to conduct voice monitoring of local calls on its fixed and mobile network" and that it could not "provide data monitoring, internet monitoring, deep packet inspection, international call monitoring or speech recognition" (Nokia Siemens Networks, Provision of Lawful Intercept Capacity in Iran. June 22, 2009. http://www.nokiasiemensnetworks.com/news-events/press-room/press-releases/provision-of-lawful-intercept-capability-in-iran). It also said in the same statement that Nokia Siemens Networks' Intelligence Solutions was sold to Persua GmbH on March 31st, 2009 (ibid), which now operates it under the name Trovicor GmbH (*Spiegel Online International*, Western Surveillance Technology in the Hands of Despots. December 8, 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

[12] "Es können mit diesen Monitoring Centern Personen geographisch bestimmt werden, wo sie sind, es kann ihr Kommunikationsprofil erstellt werden, mit wem sie kommunizieren. Es können Gruppen ausgeforscht warden".

[13] "Es gibt heute für uns keinen Grund anzunehmen, dass NSN sich rechtswidrig oder nicht ordnungsmässig verhalten hat".

Bahrain (*Bloomberg*, Torture in Bahrain Becomes Routine With Help From Nokia Siemens. August 23, 2011. http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html).

"Trovicor equipment plays a surveillance role in at least 12 Middle Eastern and North African nations, according to the two people familiar with the installations. […] Al Khanjar says the first of his communications used in the interrogations was intercepted in June 2009. At that time, the Nokia Siemens family of related companies was the only known supplier and maintainer of monitoring centers to Bahrain, the two people familiar with the installations say. The clusters of computers required constant upgrades by the companies, they say" (ibid.).

In April 2012, German media published allegations that Nokia Siemens also sold its Monitoring Centre to Syria. "German industrial giant Siemens sold network surveillance technology to the Syrian regime in 2000, public broadcaster ARD reported on Tuesday night. According to their news show 'Fakt', a product called the 'Monitoring Center' was delivered to Syrian mobile communications company Syriatel. Nokia Siemens Networks confirmed the delivery, they reported.

The corresponding business division at Siemens became the new joint venture Nokia Siemens Networks in 2007. The following year, that company signed a contract with Syrian landline provider STE, a deal that also included the 'Monitoring Center'. These contracts were then transferred in March 2009 to the Nokia Siemens Networks spin-off company Trovicor, which took over the 'Voice and Data Recording' division, ARD reported, citing documents they had obtained.

The Munich-based company Trovicor, which belongs to a financial investor today, declined to comment on the issue, 'Fakt' reported. But a human rights activist from Amnesty International told the show that the systematic online surveillance by Syrian security forces was likely playing a role in the capture of opposition members, who face torture after their arrest. […]

Internet freedom activist and Pirate Party member Stephan Urbach criticized the export of surveillance technology from Germany. 'We need a broader debate about the ethical responsibility of companies', he said in a statement. 'The German government has completely missed this debate, particularly in the wake of revelations about such filtering and surveillance systems'. If it becomes unambiguously clear that German companies have delivered surveillance technology to totalitarian states, Berlin must 'swiftly correct this failure', he added" (*Spiegel Online International*, Monitoring the Opposition: Siemens Allegedly Sold Surveillance Gear to Syria. April 11th, 2012. http://www.spiegel.de/international/business/0,1518,826860,00.html).

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 aganist

to me while I was beaten"[14] (*FAKT*, Syrien überwacht mit Siemens-Technik. April 10, 2012. http://www.mdr.de/fakt/siemens106.html) .

If these reports are true, then it means that Nokia Siemens first sold Monitoring Centres to Iran and Syria, then sold its surveillance business unit to another company that renamed the business unit to trovicor and continued selling the technology to countries that use them for tracking, imprisoning and torturing political activists.

Erich Möchel, the first journalist who reported about Nokia Siemens relations to Iran, comments on the sale of the surveillance unit to a smaller company that there was no concern about human rights, but only a concern about image damage, and that the business with surveillance continues: "Meanwhile predominates the insight that the collateral damage for company policy probably will be much smaller if these Monitoring Centers [...] are outsourced to specialist companies and one self prepares everything technically 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. So one sends ahead somebody else – companies that do not care because they come from this area. [...] If you sell to a state a complete GSM network family, then this really costs money. That's a lot of revenue. Well, now one says stop that, one lets others take care of it, the Monitoring Centres, and one rather makes the big business and not the small business because both get together badly [...] Nokia has suffered a huge reputational damage by the revelations in Iran. [...] For this reason one has retreated and said: The image loss is larger than the expected profit when we carry on further this way, so we stop it. That's basically a very wise business policy decision" (*NDR*. ZAPP: Interview mit Erich Möchel. December 7, 2011.

http://www.ndr.de/fernsehen/sendungen/zapp/media/moechel103.html)[15].

Möchel in the interview pointed out that public pressure (by the media and civil society) on one company does not automatically stop unethical business practices, but

[14] 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".

[15] "Inzwischen überwiegt die Einsicht, dass der Kollateralschaden für die Firmenpolitik wohl wesentlich geringer sein wird, wenn man diese Monitoring Centres […] an Spezialfirmen auslagert und man selbst bereitet eigentlich nur alles dazu vor technisch, dass dieses fremde Equipment (von Dritten zugelieferte) problemlos an die eigenen Telefonienetze andockbar ist. […] Es ist reine Marktpolitik, sonst nichts. Es hat nichts mit Menschenrechten zu tun, sondern nur damit, dass man sich selbst nicht anpatzen will damit. Sondern da schickt man jemanden anderen vor – Firmen, denen es egal ist, denn sie kommen aus dem Bereich. […] Wenn man an einen Staat ein Netz aus der kompletten GSM Familie verkauft, das kostet so richtig Geld. Das ist viel Umsatz. Naja, jetzt sagt man halt, man überlässt das anderen, die Monitoring Centres, und wir machen lieber das große Geschäft und das kleine Geschäft nicht, denn beide Geschäfte zusammen vertragen sich schlecht. […] Nokia hat einen immensen Imageschaden durch das Auffliegen im Iran davongetragen. […] Aus diesem Grund hat man sich zurückgezogen und hat gesagt: Der Imageschaden ist grösser als der zu erwartende Gewinn, wenn wir das weiter betreiben, also hören wir auf damit. Eine sehr kluge geschäftspolitische Entscheidung im Grunde ".

can result in the selling of business units to other companies that engage in comparable practices.

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. There are differing reports and views about what technical capacities the communications surveillance technologies exported to Iran and Bahrain actually had. So although the business practices are not entirely clear, it seems to be the case the companies like trovicor and Nokia Siemens produced or have produced surveillance technologies that are capable of intercepting the communications content of different forms of communication (Internet, fixed line telephony, mobile phone communication, etc) and that such technologies can in political contexts be used for repression against the political opposition.

On October 25th, 2010, the EU updated its export restrictions to Iran that were issued in 2007. The restriction includes an explicit restriction "on trade in dual-use goods and technology, as well as equipment which might be used for internal repression" (*EU Regulation No. 961/2010 of 25 October 2010 on Restrictive Measures against Iran*). This means that exports of Internet and phone surveillance technologies have been legal prior to this restriction. The EU's export restrictions of that were passed on November 16th, 2011 apply for equipment that can be used "in connection with a violation of human rights, democratic principles or freedom of speech as defined by the Charter of Fundamental Rights of the European Union, by using interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of Internet use (e.g. via Monitoring Centres and Lawful Interception Gateways)" (*EU Regulation No. 1232/2011 of the European Parliament and the European Council)*. The restriction applies only for the following countries: Argentina, China (including Hong Kong and Macao), Croatia, India, Russia, South Africa, South Korea, Turkey, and Ukraine (ibid.). This means that export of communications surveillance technology to a country like Bahrain is still legal, whereas it is now illegal to export similar technologies (like Monitoring Centres) to Iran. So if the claims that trovicor exported communications surveillance tools to Bahrain were true, then it would definitely be the case that "trovicor complies with all export and customs controls in all regions where business is conducted" (#9, 7). The question that can however be posed is not only if legal standards have been respected or if fundamental ethical principles are respected (such as the human right of freedom of assembly and expression) and if trovicor's business practices respect the ethical goal that it has set itself in its Code of Business Conduct (#9) and that is not primarily a legal goal, namely that "trovicor's business ethics goal is, as an industry leader, to be among the world's best in corporate responsibility, corporate governance, promoting fair competition, adapt internationally recognized standards whenever feasible, and practicing good corporate citizenship wherever it does business" (#9, 4).

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. December 8, 2011) and "Birgitt Fischer-Harrow, Trovicor's head of marketing communications, said Trovicor's contracts prevent it from disclosing its customers or the countries where it does business. She declined to comment further" (*ArabianBusiness*, Western Spy Tools Aid in Crackdown on Arab Dissent. August 28, 2011). That businesses refuse to comment on their exports shows that under the current legal circumstances in the EU it is difficult to obtain transparency about which surveillance technologies have been exported and sold to which countries and organizations by European security companies.

In some of the cases presented thus far, companies engaging in the export of communications surveillance withdrew their projects or plans only after the media and civil society criticized them publicly, in other cases companies declined to comment. This shows the circumstance that there is a lack of transparency of the business practices of security companies.

10. Digitask

Place of business: Haiger, Germany
Website: http://www.digitask.de
Self-description:
"We are a leading company for the system-integrating realization of data investigation- and assessment systems in the area of telecommunications. National and international companies and security agencies are among our customers"[16]
(http://www.digitask.de/index.php?option=com_content&view=frontpage&Itemid=1
).

Analysis

Digitask says that it is the "market leader for LI [lawful interception] in Germany" (#10_1, 1). Digitask argues that there is data that might get lost in LI, such as instant messages, encrypted communication, WWW data transmitted over the secure protocol https, encrypted e-mail data (TLS, SSL), VPN connections, traffic encrypted with software like Tor or JAP, data encrypted on harddisks, data of "nomadic targets" that seek open WLANs (#10_1). "Everything may be lost. With a few hours effort, today's LI systems can be turned blind and deaf" (#10_1, 11). As a solution, DigiTaks offers "Remote Forensic Software", which is "stealth software installed on [the] computer of [the] target to overcome encryption, handle nomadic targets, monitor activity for criminal investigations [and] intelligence gathering" (#10_1, 12). This software is a so-called Trojan horse that is secretly installed on a computer and gathers information about the user's activity without his/her knowledge. According to a presentation, the software can also collect audio data, screenshots, keylogs, registry settings, and search for files (#10_1, 13).

Other products includes systems for the analysis of intercepted data (DigiBase, DigiNet) (#10_2). DigiNet can decode "all standard Internet traffic protocols" (#10_2, 3; SUCH AS: HTTP, POP3, SMTP, IMAP, FTP, Telnet, VoIP, webmail, IRC, ICQ, MSN, etc, see: #10_2, 7) and provides the opportunity of "mass storage" of intercepted data (#10_2, 4). Another product is the WiFi-Catcher, a "modular unit for interception of WLAN traffic" (#10_2, 14). Digitask's products also enable "deep view into packets of intercepted data" (#10_2, 13). It is a mobile system that can capture, filter and visualize data that is obtained from a WiFi hotspot (#10_3, 11). It "can be used undercover on public hotspots by bringing just a small receiver unit close to the target and analyzing the traffic from the distance or with bigger directional antennas from the distance" (#10_2, 12).

[16] "Wir sind ein führendes Unternehmen für die systemintegrierte Realisierung von Datenerhebungs- und Bewertungssystemen im Bereich der Telekommunikation. Firmen und Sicherheitsbehörden aus dem In- und Ausland zählen zu unseren Kunden".

In January 2008, WikiLeaks published a document (#10_5) that, if authentic, seems to be an offer of Digitask to the Bavarian State Ministry of Justice for a software that is a "Skype capture unit" (#10_5). The German Internet portal Heise argued that the document "suggests the use of Trojans to wiretap Internet phone calls on private PCs by the police"[17] (*Heise Online*, Ein "Bayerntrojaner" zum Abhören von Internet-Telefonie? January 24, 2008). The development of the Remote Forensic Software was in Germany publicly discussed in the context of the "Bundestrojaner"/"Staatstrojaner"-debate ("federal Trojan", "state Trojan") if it is appropriate of a privacy violation if the police uses software secretly installed on suspects' computers in order to collect data (*Heise Online*, Einsatz des Staatstrojaners: Zwischen fehlendem Rechtsrahmen und Verfassungswidrigkeit. October 11, 2011).The Austrian news magazine profil reported in October 2010 that one of Digitask's lawyers confirmed that the company sold its Remote Forensic Software that serves the purpose of online investigations to Austrian authorities and that online investigation software has been used in Austria by the police (*Profil*, Trojanische Sitten. Der Bundestrojaner wurde ohne rechtliche Grundlage eingesetzt. October 22, 2010). The German news magazine *Der Spiegel* reported that in one of the cases the software transmitted Skype conversations and automatically taken pictures of the user to the police (*Spiegel Online*, Fahnder: Massiver Eingriff. February 28, 2011).

In Germany, the Law for the Defence against Threats of International Terrorism by the Federal Criminal Police Office (*Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt*) allows the "covert use of technical means"[18] for "the defence of the existence or security of the state or a person's body, life or freedom or things of significant value, whose preservation is in the public interest, against an urgent threat"[19] (*Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt*, §20h). *Der Spiegel* argued that in one specific case where online investigation was used, there was no capital offence, but rather the suspicion of the illegal export of narcotic substances (*Spiegel Online*, Fahnder: Massiver Eingriff. February 28, 2011). In October 2011, *Der Spiegel* wrote that Digitask delivered its online investigation software to several German federal states and the Zollkriminalamt (Customs Criminological Office; *Spiegel Online*, Digitask: Trojaner-Hersteller beliefert etliche Behörden und Bundesländer. October 11, 2011). *Der Spiegel* reported that online investigation software was used more than 50

[17] "Ein bislang unbestätigtes Schreiben des bayerischen Justizministeriums, das der Piratenpartei nach eigenen Angaben in die Hände geraten ist, legt den Einsatz von Trojanern zum Abhören von Internet-Telefonaten auf privaten PCs durch die Polizei nahe".

[18] "verdeckten Einsatz technischer Mittel"

[19] "Das Bundeskriminalamt kann zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Staates oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen 1. das nichtöffentlich gesprochene Wort einer Person abhören und aufzeichnen, […] 2. Lichtbilder und Bildaufzeichnungen über diese Person herstellen, wenn die Abwehr der Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre".

times in Germany (*Spiegel Online*, Innere Sicherheit: Trojaner im Abo. October 17, 2011). The Chaos Computer Club analysed a used online investigation tool, about which Digitask said that it is likely that it is one of its products and found that by remote control the software can activate the full functionality of searching, reading, writing and manipulating files (*Spiegel Online*, Staatstrojaner: Digitask wehrt sich gegen Inkompetenz-Vorwurf. October 12, 2011). The German Federal Constitutional Court (Bundesverfassungsgericht) argued that extensive parts of private life can take place online or be stored on a computer and that this needs to be taken into account in the case of online investigations. In a decision from February 2008, it said that "the secret infiltration of an information system that allows the surveillance of the system and reading its storage media is only constitutionally legitimate if actual evidence of a concrete danger for an outstandingly important legal interest are given"[20] (*Bundesverfassungsgericht*, Leitsätze zum Urteil des Ersten Senats vom 27. Februar 2008). This means that the use of online investigation tools that have the capability of not only intercepting actual communication, but accessing stored data, is unconstitutional according to German law (*Spiegel Online*, Schnüffel-Software: Bayerns Innenminister stoppt Trojaner-Einsatz. October 11, 2011). In November 2011, the Bavarian Data Protection Commissioner Thomas Petri announced to investigate if 22 cases, in which online investigation software was used to monitor suspects, respected data protection policies or not (*Heise Online*, Datenschützer prüft alle 22 Trojanereinsätze in Bayern. November 24, 2011).

Digitask produces tools that allow intercepting wireless networks, the deep packet inspection of Internet content and the online investigation of activities of users by the installation of a Trojan horse on their computers. The latter kind of tools have resulted in a heavy public debate about the constitutionality of "state Trojans" in Germany. Online investigation tools have especially in cases, where suspects encrypt their e-mails or use Skype, been used. The constitutionality of such tools and the actual use by the police are heavily disputed in Germany.

[20] "Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen".

11. ipoque

Place of business: Leipzig, Germany
Website: http://www.ipoque.com/
Self-description:
"ipoque provides network intelligence and policy control solutions helping fixed and mobile broadband operators to better understand traffic patterns, monetize new data services and improve the quality of experience for their subscribers. Our application classification and analysis engine enables bandwidth and congestion control, prioritized quality of service delivery and detailed network visibility. ipoque was founded in 2005 in Leipzig, Germany, and has become a Rohde & Schwarz company in 2011. Over 200 broadband operator customers in more than 60 countries across the globe rely on ipoque's policy control solution to limit equipment and operating expenditures, increase profitability and maximize subscriber satisfaction. In addition, many network equipment providers use ipoque's deep packet inspection technology in their network security, WAN optimization and network management products to analyze data traffic of hundreds of millions of Internet users"
(http://www.ipoque.com/en/company/company-profile).

Analysis

ipoque says that it is "the leading European provider of deep packet inspection (DPI) solutions for Internet traffic management and analysis"
(http://www.ipoque.com/en/company). It offers various DPI systems. PRX Traffic Manager "detects applications with a combination of layer-7 deep packet inspection (DPI) and behavioral traffic analysis. All major protocols including peer-to-peer file sharing (P2P), instant messaging (IM), media streaming and Internet telephony (VoIP) are supported. The integrated quality of service (QoS) management allows prioritization, shaping and blocking of classified traffic"
(http://www.ipoque.com/en/products/prx-traffic-manager).

It allows "to prioritize, shape, block and log traffic of individual applications either in total or for individual users or user groups" and can "enforce legal file sharing" (ibid.), which means that it can detect and block illegal file sharing.
Net Reporter works based on PRX Traffic Manager and "collects, aggregates and stores" network data that PRX Traffic Manager extracts with the help of DPI from a network (#11_3). It also "presents them via its Web-based graphical user interface" (ibid.). DPX Network Probe "is a passive IP probe for lawful interception, mass interception and network monitoring. It uses ipoque's Deep Packet Inspection (DPI) technology to identify and filter network flows according to their application protocol. Target triggers comprise protocol-specific filtering criteria including network addresses, user names, protocol-specific attributes and arbitrary content keywords"

(#11_2). It supports almost 200 different protocols and enables keyword search in all intercepted content in order to filter out certain messages (#11_2).

PACE (Protocol & Application Classification Engine) "is a software library which detects and classifies protocols and applications from a network packet stream. It uses a wide range of deep packet inspection (DPI) technologies, including pattern matching, behavioral, statistical and heuristic analysis" (#11_4). It provides DPI technology that "is able to identify the protocol of network traffic based on a combination of deep packet inspection (DPI) and behavioral analysis" (#11_1).

ipoque produces DPI technologies both for the commercial use (e.g. by Internet Service Providers) and the use by law enforcement. It has realized that there is a critical debate about DPI and has reacted to it by publishing the white paper "Deep Packet Inspection: Technology, Applications & Net Neutrality" (#11_5). ipoque argues in this paper that also relatively accepted technologies such as spam and virus filters and firewalls use DPI. The company especially discusses the use of DPI for network management and concerns about the scanning of content. It says that "DPI in bandwidth management does not read all packets" and "is not automatically a privacy violation" (#11_5, 3). ipoque argues that DPI needs to be used by ISP in order to optimize the use of the network. Different protocols and different applications make different use of the Internet. So e.g. VoIP (such as Skype) has a low use of the network, whereas file sharing in peer-to-peer networks makes heavy use of the Internet. ipoque argues that an advantage of DPI-based bandwidth management is that it "can improve the average performance for Internet users" (#11_5, 5) by "assignment of priorities to different application classes", e.g. "giving voice traffic a higher priority than P2P" (#11_5, 7).

ipoque defines net neutrality as the principle "that all IP packets should be treated equally on a best effort basis" (#11_5, 6) and says that today net neutrality does not exist because "less than 20 percent of network users generate over 80 percent of the traffic", which would be unfair (#11_5, 6). 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). The US Federal Communication Commission (FCC) says that "reasonable network management", which is network management that is "tailored to achieving a legitimate network management purpose" (FCC 2010, 48) and for which DPI may be used, is no problem. Unreasonable discrimination of users that violates net neutrality would e.g. be the discrimination of certain applications (such as VoIP), hindering users to access certain content, services or applications, or the slow down of a service or website that a ISP disagrees with (FCC 2010, 42). The FCC (2010, 43) also says that "pay for priority" is likely to violate net neutrality. ipoque says that an advantage of DPI-based bandwidth management "can provider users with a tailored service, including 'soft' QoS [quality of service] guarantees, at a higher or lower price, depending on the required service level; users that only use Web and e-mail would get a lower price; everyone pays only for what they

use" (#11_5, 5). Media reform groups have argued that the creation of a tiered Internet is a risk.

The FCC and media reform groups tend to agree with ipoque's argument that network management by ISPs can help improving their service, but at the same time they much warn against transforming DPI bandwidth management into a commodity by creating a tiered Internet, where users have to pay for priority.

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: "FACT #2: Network discrimination through a 'tiered Internet' will severely curtail consumer choice, giving consumer control over the Internet to the network owners. The idea of a discriminatory or 'tiered' Internet is based on a simple concept: the network owner intervenes between the consumer and the content provider to charge fees for delivery. Under the old neutrality rules, the network owners could charge the customer for communications services, and any application or content that would work within that level of service had to be allowed to flow – no questions (or additional fees) asked. [...] Without Network Neutrality, the network operator has total control. Different fees can be charged based on the type of service (voice, video or data); different fees can be charged based on the type of provider (individual, small business or big business); different fees can be charged based on the affiliation of the provider with the network operator; different fees can be charged to guarantee delivery at a particular rate of speed or quality; different fees can be charged based on political affiliation or the day of the week. In fact, without neutrality rules, the network owners can charge whatever they want to whomever they want for any reason they choose. They can create 'fast lanes' and 'slow lanes' and decide who gets to be in each. There is nothing to stop AT&T from pushing content providers into exclusive deals denied to Comcast or Time Warner subscribers. There is nothing to stop Verizon from slowing down Web sites they dislike and speeding up others with impunity. [...] Network Neutrality keeps telephone companies off of consumers' backs and out of our wallets (Free Press, Consumer Federation of American and Consumers Union 2006, 9).

A second warning is that a tiered Internet is a stratified system, in which rich players (like big companies) use a fast Internet and everyday people, who do not have so much money, a slow Internet: "FACT #4: Network discrimination through a 'tiered Internet' will fundamentally alter the consumer's online experience by creating fast and slow lanes for Internet content. The process of network prioritization is a zero-sum game. The fact is that every time one Web site or service is sped up, another must be slowed down. Who will be in the slow lane? Anyone without the cash or the connections to negotiate fast lane deals with every network operator in the country (each of which has their own regional fiefdoms). Basically, anyone that lacks deep pockets or high volume will be relegated to the slow lane, while the big corporate

Web sites will gain premium treatment, capturing a larger percentage of users by virtue of their higher quality of service“ (Free Press, Consumer Federation of American and Consumers Union 2006, 11).

ipoque argues: “DPI as such has no negative impact on online privacy. It is, again, only the applications that may have this impact. Prohibiting DPI as a technology would be just as naive as prohibiting automatic speech recognition because it can be used to eavesdrop on conversations based on content. Although DPI can be used as a base technology to look at and evaluate the actual content of a network communication, this goes beyond what we understand as DPI as it is used by Internet bandwidth management – the classification of network protocols and applications. Other applications of DPI, for instance lawful interception and targeted injection of advertisements, do indeed go further, but they are beyond the scope of this paper“ (#11_5, 7). ipoque in its discussion focuses primarily on the issues of net neutrality and bandwidth management when discussing DPI, privacy concerns about the use of DPI in relation to the surveillance and repression of political opponents and targeted advertising are not discussed. Also the whole range of arguments in the net neutrality debate (for an overview see: Free Press, Consumer Federation of American and Consumers Union 2006) is not discussed.

In another white paper, titled “Copyright Protection in the Internet” (#11_6), ipoque discusses countermeasures against the “illegitimate sharing of copyright-protected material“ that “has a negative economical impact both on a national and international scale“ (#11_6, 1). The solutions that the authors find most feasible include the use of DPI for blocking illegal sharing: “New business models are inevitable. In the long run, this will make illegitimate sharing of copyright-protected material through the Internet a lot less interesting. Until then, two of the discussed countermeasures promise to be the most effective and viable ones: hash-based detection of copyrighted files and the prevention of their transfer in the network; and the active monitoring combined with the prosecution of infringers“ (#11_6, 8). Hash-based blocking “can be implemented using currently available traffic management systems based on deep packet inspection deployed at network access or peering points. [...] Blacklisting based on file hashes or other file IDs can provide a viable way to severely limit the distribution of copyright-protected content“ (#11_6, 5). ipoque on the one hand mentions technical solutions, on the other hand solutions at the level of society. The latter include the culture flat rate, digital rights management, and cheaper offers (#11_6, 8). However, the solution suggested by some, such as the Pirate Party[21], to

[21] “The official aim of the copyright system has always been to find a balance in order to promote culture being created and spread. Today that balance has been completely lost, to a point where the copyright laws severely restrict the very thing they are supposed to promote. The Pirate Party wants to restore the balance in the copyright legislation. All non-commercial copying and use should be completely free. File sharing and p2p networking should be encouraged rather than criminalized. Culture and knowledge are good things, that increase in value the more they are shared. The Internet could become the greatest public library ever created. The monopoly for the copyright holder to exploit an aesthetic work commercially should be limited to five years after publication. Today's copyright terms are simply absurd. Nobody needs to make money seventy years after he is dead. No film studio or rec-

decommodify digital culture and legalize file sharing is not at mentioned as an option, which shows that ipoque is thinking only about a certain limited range of alternatives.

ipoque sells deep inspection technologies (DPI) for network and bandwidth management, commercial purposes and law enforcement. It is aware of the circumstance that DPI is a controversial technology. The analysed documents have limited the discussion of DPI to network neutrality, bandwidth management, and file sharing, whereas topics like the surveillance of political activists and targeted advertising have rather been neglected. The analysed discussions of net neutrality and file sharing have not engaged with the full range of criticisms made in the debate by media reform groups.

---

ord company bases its investment decisions on the off-chance that the product would be of interest to anyone a hundred years in the future. The commercial life of cultural works is staggeringly short in today's world. If you haven't made your money back in the first one or two years, you never will. A five years copyright term for commercial use is more than enough. Non-commercial use should be free from day one. We also want a complete ban on DRM technologies, and on contract clauses that aim to restrict the consumers' legal rights in this area. There is no point in restoring balance and reason to the legislation, if at the same time we continue to allow the big media companies to both write and enforce their own arbitrary laws" (http://www.piratpartiet.se/international/english).

12. Utimaco Safeware

Place of business: Aachen, Germany
Website: http://lims.utimaco.com/en/home/
Self-description:
"Since 1994 Utimaco has been providing lawful interception systems for mobile and fixed network operators and Internet service providers. The Utimaco Data Retention Suite was introduced in response to the EU directive 2006/24/EC and at the request of telecom customers for integrated LI and DR solutions. With more than 160 installations in 60 countries, Utimaco is a leading global supplier in the LI market. Since 1994 Utimaco has been developing hardware based security solution. Today, Utimaco is one of the world's leading manufacturers of innovative and professional solutions for hardware security module technology"
(http://lims.utimaco.com/en/company/about-utimaco).

Analysis

Utimaco explains the need for communications surveillance with the use of communication technology by criminals and terrorists: "This worldwide explosion of communication technologies creates significant challenges for law enforcement agencies and national security organizations responsible for battling various forms of crime and terrorism. The sophistication of criminal enterprises in exploiting emerging communication channels has increased with the rising popularity of these channels, posing a very real challenge to organizations responsible for protecting public safety and reducing the impact of crime on communities. Given the broad availability of communication options and the relative ease with which criminal networks and terrorist groups can exchange information across these channels – by both data and voice communication – the impetus to intercept illicit exchanges and track the operations of criminal enterprises is strong and compelling" (#12_4, 5). "Countries around the world have responded to the threats of terrorism and criminal activity by enacting legislation that provides the legal basis for lawful interception" (#12_4, 6).

Utimaco DRS is a data retention system that collects communication data and subscriber data, retains them, allows fast search in data records and "automates request processing and delivers data to authorized agencies by fax, e-mail, or secure IP interfaces" (#12_2). The company explains the need for data retention by saying that it can help to fight crime and terrorism: "Telecommunications data retention refers to the process of storing call detail records and subscriber data for various telecommunications services for a period of months and years. […] Law enforcement agencies and intelligence services regard the access to retained telecom data as a pillar of crime investigation and the prevention of terrorism. Retained electronic data is regularly used to identify and trace suspects, uncover terrorists' social networks, or to collect admissible evidence for court proceedings. […] Many countries around the world have passed laws to define the authority of police and intelligence agencies and the

responsibility of service providers. In Europe, for instance, the EU directive 2006/24/EC was introduced in March 2006 as a response to the coordinated terror attacks in Madrid 2004 and London 2005"

(http://lims.utimaco.com/en/solutions/data-retention-suite).

Ultimaco also sells "lawful interception solutions" that make use of DPI. "Utimaco Lawful Interception Management System (LIMS™) is a comprehensive solution that provides state-of-the-art surveillance capabilities for fixed and mobile communication networks and for various communication services, including telephony, messaging and IP-based services like e-mail and VoIP"

(http://lims.utimaco.com/en/solutions/lawful-interception-management-solution/). Utimaco explains the need for this technology by saying that it can help to fight crime and prevent terrorism. "Lawful Interception (LI) is the legally approved surveillance of telecommunications services. It has become an important tool for law enforcement and intelligence agencies around the world for investigating and prosecuting criminal activities and terrorism" (ibid.).

"The main functions of any LI solution are to access Interception-Related Information (IRI) and Content of Communication (CC) from the telecommunications network and to deliver the information in a standardized format via the handover interface to one or more monitoring centers of law enforcement agencies" (12_3, 3).

"Citizens of many countries are rightfully wary of governments and law enforcement bodies intruding on their private activities. Because of this, ethical concerns and essential privacy rights must be central considerations in any lawful interception solution. [...] A delicate balance exists between the capabilities of the government to detect and prevent crime and terrorism – as supported by the laws and prevailing regulations in a country – and the individual rights and privacy concerns of the citizens of that country. A responsible, ethically grounded lawful interception solution recognizes that this balance can only be achieved by giving equal weight to both the legalities of the law enforcement tasks at hand and the individual rights of the citizens. Achieving this balance in a solution requires careful consideration of both the technological aspects of the challenge, as well as the legal and ethical issues that are intricately associated with the monitoring of any form of communication" (#12_4, 14).

In November 2011, there were news reports that the Italian firm Area Spa planned to equip the Syrian intelligence with surveillance technologies (project "Asfador") that can be used for monitoring the political opponents of Bashar al-Assad's government and that Utimaco was also involved. "Area is using equipment from American and European companies, according to blueprints and other documents obtained by Bloomberg News and the person familiar with the job. The project includes Sunnyvale, California-based NetApp Inc. (NTAP) storage hardware and software for archiving e-mails; probes to scan Syria's communications network from Paris-based Qosmos SA; and gear from Germany's Utimaco Safeware AG (USA) that connects tapped telecom lines to Area's monitoring-center computers" (*Bloomberg*, Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear. November 4, 2011.

http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html).

"The Syrian secret service appears to be monitoring the country's protest movement using technology from the German firm Utimaco, based in Oberursel, a suburb of Frankfurt. Contacted by Spiegel reporters on Friday, the company said it had sold no products directly to Syrian Telecom, the regime-owned telecommunications provider. The company had instead delivered products to the Italian firm Area, with which is has conducted business for years. The company said it could not confirm whether Area had then resold goods to Syrian dictator Bashar Assad's regime" (*Spiegel Online International,* Is Syria Monitoring Protesters with German Technology? November 8, 2011).

Utimaco reacted to the media reports: "It is thought that German surveillance technology has also been delivered to Syria, as part of a surveillance system made by the Italian firm Area. For years, the Italians have used specialized software by the German firm Utimaco in their systems. But as Utimaco senior executive Malte Pollmann insists, Area only built a test version, and the Italians have just cancelled the entire project. 'Our software was not used,' says Pollmann" (*Spiegel Online International*, Western Surveillance Technology in the Hands of Despots. December 8, 2011). In a statement on its website, Utimaco declared: "Utimaco and its majority shareholder, Sophos, have recently been included in media reports about an Italian OEM reseller (Area S.p.A.) allegedly selling Utimaco's LIMS technology to Syria. We take global trade compliance very seriously and require all of our partners to adhere to the German, European Union (EU) export regulations and United Nations embargo lists. We are thoroughly investigating the matter and have stopped any further activities with Area until we receive full clarification from them"

(http://lims.utimaco.com/en/company/newsevents/statement-on-recent-media-reports-from-utimaco-safeware-ag/).

Utimaco's Internet surveillance technologies support Deep Packet Inspection and can be implemented in a way that allows the surveillance of political opponents. In a White Paper (#12_4), Utimaco shows some concerns about privacy aspects. It seems to be aware of discussions of potential privacy violations by Internet surveillance technologies. It does however not address the practical problem of how exactly one should prevent that DPI is used for violating the privacy of political activists, consumers, and citizens. The plan of the export of DPI technology to Syria shows that this technology is difficult to control. Utimaco reacted to the media reports about Area Spa's project by ending its business relations with this company. This move came however only after civil society pressure. The question is what would have happened if no investigative journalists and activists had intervened. This problem is fortified by the circumstance that trade deals in the security industry have a high level of secrecy. There is hardly public accountability and transparency of who sells which surveillance technologies to whom.

13. NETI

Place of business: Budapest, Hungary
Website: http://www.neti.hu/
Self-description:
"NETI is a pioneer in the development of systems based on custom designed applications supporting analytic security solutions. – These systems provide our customers with robust and efficient tools for the handling of massive dataflow monitoring in various areas" (http://www.neti.com/en/services/services).

Analysis

NETI says that the Internet is unpredictable, dynamically growing, and brings about many new data types (#13, 4). This would pose challenges for law enforcement. A solution would be NETI's BONGO monitoring centre that is "fine-tuned for the needs of Law-Enforcement and National Security Agencies as well as Telecom and Internet Service Providers" (#13, 11).

BONGO is advertised as "Monitoring Solution for Everyday Security" (http://www.neti.com/en/products/bongo). "The system inherited its name from the Bongo antelope, the elusive king of the Equatorial Rain Forest, who finds his way easily and undetected in the thickest of jungles, while can see and hear everything. Today's monitoring tasks are no less challenging. The systems have to be capable of fast and reliable navigation, selection, storage and presentation of the valuable pieces of information out of the massive and ever-growing jungle of networks and data masses of the Twenty-first Century" (ibid.). It "can intercept huge amount of data from a wide array of telecom and IP networks and other information sources. […] The structure of BONGO can be realized on a single workstation, but it can unleash its great power as a large, or even national system with hundreds of servers and operators. […] The system is ready to handle massive amount of data intercepted from telecom and IP systems. The effective handling of great masses of data is assured by the complex set of background processes with strong support provided to the operators' processing tasks" (ibid.). BONGO can monitor both the Internet and phone networks. It can filter data according to "phone number, IMEI, IMSI, radius identification, IP address, e-mail address, MAC address, etc" (ibid).

NETI produces and sells monitoring centres that can intercept content of both telecommunications and the Internet. The BONGO system is a deep packet inspection surveillance technology. We could find no discussions of privacy and other concerns about DPI in the analysed documents and on NETI's website (accessed on February 5, 2012).

14. Area Spa

Place of business: Vizzola Ticino, Italy
Website: http://www.area.it
Self-description:
"From 1996 until today, AREA has constantly pursued the objectives of cutting edge technology and qualitative excellence in the LI sector. As the first operator in Italy to introduce a multi-channel audio digital recording system based on standard market components and featuring total accessibility through IP networks, the company is now the national leader in this sector, with over 300 installations of its MCR System around the world"
(http://www.area.it/irj/portal/anonymous?NavigationTarget=navurl://6fff78b6f13c2127ce9b4fe3c17cf995)
Analysis
Area commits itself formally to both surveillance and the respect of privacy: "Intelligence is an extremely complex and delicate process, called upon to meet the new challenges introduced by the growing technological complexity of telecommunication systems and the need to guarantee the utmost protection and respect of privacy, while simultaneously offering concrete support in the analysis of data and information"
(http://www.area.it/irj/portal/anonymous?NavigationTarget=navurl://6fff78b6f13c2127ce9b4fe3c17cf995).

The company produces and sells Monitoring Centres: "MCR System satisfies all operational and strategic requirements of monitoring activities. The MCR System offers a single integrated platform to capture and analyse data coming from any transmission source and to obtain a comprehensive overview providing added value to investigative work. With its high scalability and customisation, MCR is able to transform any installation into a unique and valuable project. MCR complete systems are implemented through a solid networking architecture, to allow the maximum operation efficiency and security. Thus, information flows may be monitored on a global scale, maximising LI times, avoiding loss of information and never endangering the safety of the whole process"

(http://www.area.it/irj/portal/anonymous?NavigationTarget=navurl://cbecc21b801cae301af69b4db9e8c152). The MCR system can capture data "from networks and unconventional sources" and it can record and analyse this data

(http://www.area.it/irj/portal/anonymous?NavigationTarget=navurl://cbecc21b801cae301af69b4db9e8c152). MCR is a technology that can monitor different data sources and intercept their content. Content interception is also possible for Internet communication, which means that MCR is a deep packet inspection surveillance technology.

In November 2011, there were media reports that said that Area Spa started installing Internet surveillance technologies in Syria, a country where hundreds of

members of the political opposition have been killed by the government that tries to repress protests that started in January 2011. "Employees of Area SpA, a surveillance company based outside Milan, are installing the system under the direction of Syrian intelligence agents, who've pushed the Italians to finish, saying they urgently need to track people, a person familiar with the project says. The Area employees have flown into Damascus in shifts this year as the violence has escalated, says the person, who has worked on the system for Area. […] Area is using equipment from U.S. and European companies, according to blueprints and other documents obtained by Bloomberg and the person familiar with the job. The project includes Sunnyvale, Calif.-based NetApp Inc. storage hardware and software for archiving e-mails; probes to scan Syria's communications network from Parisbased Qosmos SA; and gear from Germany's Utimaco Safeware AG that connects tapped telecom lines to Area's monitoring-centre computers. […] When the system is complete, Syrian security agents will be able to follow targets on flat-screen workstations that display communications and web use in near-real time alongside graphics that map citizens' networks of electronic contacts, according to the documents and two people familiar with the plans. Such a system is custom made for repression, says Mark Dubowitz, executive director of the Washington based Foundation for Defense of Democracies […] Area, a privately held company that got its start in 1996 furnishing phone taps to Italian law enforcement, has codenamed the system 'Asfador,' a nod to a Mr. Asfador who cold-called the company in 2008 asking it to bid on the deal, according to one person knowledgeable about the project" (*The Calgary Herald*, Italian Firm Helping Syria Spy on E-Mails. System Made for Repression, says Think-Tank. November 5, 2011).

According to media reports, "Area chief executive Andrea Formenti says he can't discuss specific clients or contracts, and that the company follows all laws and export regulations" (ibid.). Later, Area's CEO was quoted in the press saying that the surveillance project has not been activated: "In response, Area SpA's CEO, Andrea Formenti, was quoted in Italy's Corriere della Sera newspaper this month announcing that his company had no employees in Syria and that the project had not made any progress in the last two months. […] 'The interception system has never been activated and cannot be under current circumstances. There has been no repression carried out thanks to our equipment,' Formenti told Corriere della Sera" (*CNN Online*, Cyberwar Explodes in Syria. November 20, 2011).

"'We have a contract in place with Syria, this true; but everything has been halted for two months, and there are none of our technicians in Damascus.' After five days of silence, there is a statement by Andrea Formenti, chairman of Area SpA, the Italian software house that has become an international case because it is installing an intercept system of Internet traffic on behalf of [Syrian President] Bashar Assad's regime. Formenti, 42, explains his having 'landed' in Syria: 'We won a international bidding contest in 2008, outbidding 4 European countries, and other non-European companies. As interlocutors, we have never had people either in the military or in the intelligence services, but of the local telephone provider.' Area's chairman stated that the contract was worth 13 million euros, but denied currently having personnel at work

in the Middle East country. 'For two months everything has been halted, and I would like to point out that the eavesdropping system has never been operated, and as things now stand, it never will.' The future is uncertain: 'We have contractual agreements that are very binding, and which, if not honoured, would force us to pay hefty penalties. On the other hand, we are following the situation in Syria as it evolves. We want no part of being accomplices to repression. We hope there will be some form of intervention by the international authorities to sort things out.' Yesterday, a protest was held in front of Area headquarters by anti-Assad representatives who live in Italy. Beside them were activists of the Italian Pirates Party" (*BBC Monitoring Europe*, Italian Software Company Denies Complicity in Syrian President's Repression. November 9, 2011).

Area Spa is producing and selling Monitoring Centres. It has obtained a contract for implementing an Internet surveillance system in Syria. The company has reacted to allegations after they were made public by the media, saying that the system has never been activated. The case is an example of how first surveillance technologies are sold to countries or organisations that are considered problematic by human rights groups and only after information about it has been made public do companies react to the allegations. The question that arises is what happens in those cases, where civil society watchdog organizations do not find out about the existence of specific cases or do not have the resources to engage in inquiries.

15. Innova

Place of business: Trieste, Italy
Website: http://www.innovatrieste.it
Self-description:
"Innova is a technology based company that markets integrated interception systems for lawful activities and intelligence operations. […]. Thanks to a deep expertise in telecommunication applied to security sector, Innova products support Public Prosecutor's Offices and Law Enforcement Agencies in any type of monitoring activity with advanced technology for:
* fixed and mobile telephone interception
* wired and wireless communication decoding
* mobile targets tracking
* high quality audio monitoring
* data analysis and information management"
(http://www.innovatrieste.it/eng/azienda.htm).

Analysis

Innova produces and sells surveillance technologies, including tools for monitoring the Internet. One of this systems is called EGO. It is "an advanced interception system, which manages telephone, internet and audio targets on the same user-interface and can intercept up to 1000 targets simultaneously. […] Ego enables to intercept, decode and restore on the same interface all types of IP communication, such as Video-communications, MMS, internet key, e-mail and webmail, etc. […] A huge data base together with integrated advanced data analysis tools can be used to elaborate research activities, information matching operations (phone records, telephone calls, numbers etc), data cross comparisons and for immediate report creation" (#15). EGO is a flexible communications surveillance technology that can monitor different networks (telephone, Internet, etc) and inspect the content. In terms of Internet surveillance, it can be classified as a deep packet inspection technology.

Innova explains the need of its Internet surveillance business by saying that the "development of IP network and the increasing use of internet-based services led Law Enforcement Agencies to new investigation needs and to the use of advanced products for IP communication interception" (#15). We could find no discussion of privacy concerns of Internet surveillance in the analysed documents (#15, Innova website accessed on February 8, 2012).

16. IPS

Place of business: Aprilia, Italy
Website: http://www.ips-intelligence.com
Self-description:
"IPS designs and manufactures products and solutions for the most diversified applications in the Communication Security and Electronic Surveillance domains. […] The Company solutions portfolio includes Lawful Interception and Electronic Surveillance systems, Monitoring Centre and special solutions for monitoring and intercepting Web 2.0 applications. […] Our values: …To carry out an industrial project, by developing innovative technologies, with the aim of strengthening the customer's trust, thanks to the continuous growth of the company and its people, placing honesty and reliability as fundamental values, beyond any business opportunities" (http://www.resi-group.eu/ips/?page_id=2&lang=en).

Analysis

Monitoring Centres are one of the technologies that IPS produces and sells. "GENESI Monitoring Centre is an innovative centralized system, supporting the Law Enforcement Agencies investigations to manage in a unified manner audio, video and data interception as well as telephone Call Detail Records and Log Files analysis" (#16_1). It can "view in real time and off-line data communications" (Fax, Sms, Videoconference, Internet, etc.)" (#16_1). GENESI's Network Interception Platform "is a system with real-time monitoring and intercepting capabilities for the traffic being generated by IP network users" (#16_3). It can "monitor and intercept Internet traffic data […] of different types of Internet Content and Services (i.e. e-mail messages, Web accesses, Chat sessions, etc.)" (#16_3). The system works with probes that are placed in specific networks and then intercept the traffic. Interception criteria include user names, the MAC address of a computer, IP addresses, IP address ranges, and the filtering of content by "identifying the Internet traffic containing specific text strings within the protocol header (i.e. URL, e-mail account etc.) or the application content (i.e. keywords inside e-mail messages or Web pages, etc.)" (#16_3). The GENESI system can intercept content of Internet communication and other networks. In terms of Internet surveillance it can be classified as a Deep Packet Inspection surveillance technology.

IPS has also specialized in providing web 2.0 surveillance technologies: "Web 2.0 has brought to the Internet users a large set of new applications increasing the communication and collaboration capabilities thus providing a new way of interacting, sharing information and organizing activities. Web Mails, Social Networks and Blogs are currently largely adopted by common people and companies for communication purposes. Also criminal organizations exploit these applications taking advantage of the an-

onymity granted by the Internet. Social Networks monitoring or Web Mails interception can gather the intelligence helping to identify people involved in criminal activities, and to detect relevant events in advance. IPS innovative solutions are especially designed to support this tasks by delivering a new level of intelligence capability, including active and passive network systems, complementing traditional Lawful interception infrastructure and analysis tools which can be even integrated in existing Monitoring Centres" (http://www.resi-group.eu/ips/?page_id=210&lang=en).

Target Profiling is a Facebook surveillance software that "allows you to analysing communications, klick in detail and make an analysis of relations of the people involved. […] The application lists all users who come into contact with the users intercepted highlighting the following features: profile photo, name assigned on Facebook, user ID Facebook […], the number of messages exchanged with other registered users". The system can also chart relationships of monitored users and display the content of exchanged messages" (#16_3).

IPS explains the need of its surveillance technologies by arguing that "Telecom Operators as well as any Communication Service Provider have to support the investigations needs of Law Enforcement Agencies" (http://www.resi-group.eu/ips/?page_id=32&lang=en). In its self-description it says that its values are being an industrial project that satisfies customers and develops innovative technologies. The identified goals are economic, technological, and law enforcement needs. In the analysed documents we could not find an engagement with potential risks of and privacy concerns regarding Internet surveillance.

17. Group 2000

Place of business: Almelo, The Netherlands
Website: http://www.group2000.eu
Self-description:
"Group 2000 is the leading and innovative partner for Network Forensics, Communication Services and ICT Services. Our approach and solutions help Telecommunication Service Operators, Internet service providers, Governments, industries and business Services to solve communication and security issues"
(http://www.group2000.eu/en/g2k/about_group_2000).
"Network Forensics focuses on intercepting digital communications to support legal and/or criminal investigations. Group 2000 covers the entire scope, including telephone networks and the internet a as well as wireless voice and data networks. We have over 15 years of experience providing carrier grade systems that enable our clients to pinpoint the communications they are after – amidst the vast amount of data traversing today's networks – and then easily tap in, with the option of storing intercepted content" (http://www.group2000.eu/en/network_forensics).

Analysis

Group 2000 sees Data Retention, due to the EU's Data Retention Directive, as one important challenge (#17_1). Data retention technologies must support the collection, preparation, storage, management, retrieval, hand-over and destruction of data (#17_1). The LIMA DRS system is a data retention system that collects "communications data [...] and subscriber data from any telecommunications network", it retains "large amounts of data in a powerful and secure data warehouse", provides "fast search and analytics for millions of data records" automates "request processing and delivers data to authorized agencies by e-mail, or secure IP interfaces" (#17_5).

Lawful interception is considered as another challenge (#17_2, #17_3). Group 2000 sells the system the Lawful Interception Mediation Architecture (LIMA, #17_4). The LIMA DPI Monitor (#17_7) "uses deep packet inspection (DPI) technology to classify network flows according to their application protocol. Based on user-definable rules, content and signalling data of these flows can be recorded and forwarded to external devices such as mediation systems for further processing. These rules comprise target information including IP addresses, user names, protocol-specific filtering criteria, and arbitrary content keywords. This combination of DPI and flexible target rules delivers high quality interception avoiding the capturing of a larger volume of unnecessary network traffic" (#17_7). The intercepted data can be managed with the help of the LIMA Management System (#17_6). Group 2000 also sells technologies that make use of DPI for bandwidth management by Internet Service Providers (#17_9, #17_10, #17_11).

Group 2000 reacted with a press release to the publication of the WikiLeaks SpyFiles, in which it was mentioned as provider of communications surveillance

technologies. The company says that "Wikileaks Spy Files benefits Group 2000" because although "the expertise and tooling from Group 2000 has drawn attention from countries like Iran and Syria", Managing Director Richard Coppens says: "we clearly reject any form of relation with such kind of 'customers'. We strive to openness. As a company we comply with Legislation and do respect human rights. Our solutions are for instance deployed in Latin America to track down drug trafficking". (http://www.group2000.eu/en/g2k/news/news_december/press_release/).

"According to Coppens the Spy Files are incomplete and poorly justified" (ibid.). As surveillance technology producers are not complied to release their customers and sales publicly, data about what these companies are doing, is likely to be incomplete because the companies themselves often treat it as a secret. The SpyFiles make available some of this data. In the end, it is often not clear, which communications surveillance technologies are sold by which companies to whom. Not much is known about it and only surfaces occasionally as the result of investigative journalism.

18. Pine Digital Security

Place of business: The Hague, The Netherlands
Website: https://www.pine.nl
Self-description:
"Since 1997, Pine Digital Security takes care of (digital) availability and security for companies and government agencies. The specific focus on the technical side of computer security is the driving force behind our security services" (https://www.pine.nl/over-pine).

Analysis

Pine Digital Security produces and sells the EVE Lawful Interception Solution. It can be used "for the interception of IP data, (e-)mail messages and Voice over IP telephony. Our customers are Internet Service Providers (ISPs) and telecommunication companies" (http://www.lawfulinterception.com). Pine provides a Deep Packet Inspection Internet surveillance technology (EVE). It says that this technology is primarily sold to the communication industry. According to the company's self-presentation, governments or law enforcement are not important customers. On Pine's websites (https://www.pine.nl, http://www.lawfulinterception.com), we could not find a discussion of potential risks and privacy limitations of the commercial use of DPI surveillance.

19. Gamma Group

Place of business: Andover, UK
Website: https://www.gammagroup.com
Self-description:
"Gamma TSE is a government contractor to State Intelligence and Law Enforcement Agencies for Turnkey Surveillance Projects producing high quality Surveillance Vans and Cars and Technical Surveillance Equipment"
(https://www.gammagroup.com/gammatse.aspx).

Analysis

Gamma explains its production and selling of communications surveillance technologies with threats to national security. "In today's high-tech cyber environment computers, mobile phones or PDAs are being used to transmit and supply information that could potentially threaten national security. 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 [...] Conventional interception technologies can no longer cope with these challenges. Government Agencies require new mission-critical intelligence technologies to enhance existing capabilities which, to date, are insufficient within most government product portfolios" (#19).

Gamma's FinFisher is a so-called "Trojan horse", a software that once installed allows the intruder remote access. FinFisher can infect computers, mobile phones, local networks and ISP networks and extract data from these systems (#7_10, 4-10). The product and training was advertised in Eleman's Communications Monitoring catalogue from October 2007 (#7_2). FinFisher can e.g. be tarned as a software update that is sent to a computer or mobile phone (*NDR*. ZAPP: Germany Spyware for Dictators. December 7, 2011.
http://www.ndr.de/fernsehen/sendungen/zapp/media/zapp4923.html). "FinFisher is the leading offensive IT Intrusion program through which Gamma provides complementary solutions, products and advanced training capabilities to Government end-users who are seeking world class offensive techniques for information gathering from suspects and targets" (#19).

According to media reports, Gamma offered to sell its FinSpy software to Egyptian security authorities (*EUobserver.com*, EU companies banned from selling spyware to repressive regimes. October 11, 2011). "Egyptian anti-regime activists found a startling document last month during a raid inside the headquarters of the country's state security service: A British company offered to sell a program that security experts say could infect dissidents' computers and gain access to their email and other communications. [...] Amid the scattered papers, interrogation devices and random furniture found during the raid, the activists uncovered a proposed contract dated June 29 from the British company Gamma International that promised to provide access to Gmail, Skype, Hotmail and Yahoo conversations and exchanges on computers targeted by the

Interior Ministry of ousted President Hosni Mubarak. The proposal from Gamma International was posted online by Cairo physician Mostafa Hussein, a blogger who was among the activists who seized the ministry's documents. 'It is important evidence of the intent of the state security and investigation division not to respect our privacy,' Mr. Hussein said. 'This proposal was sent to a notorious department known for torture, spying on citizens to help Mubarak's regime,' Mr. Hussein said, referring to the State Security Investigations Service. 'The company Gamma, I consider them to be partners in the crime of trying to invade our privacy and arrest activists' " (*Washington Times*, British Firm Offered Spy Software to Egypt: Activists Say They Were the Targets. April 26, 2011).

Also the German regional public service TV station NDR reported about a secret offer of Gamma to the Egyptian state for the FinFisher technology (*NDR*. ZAPP: Germany Spyware for Dictators. December 7, 2011. http://www.ndr.de/fernsehen/sendungen/zapp/media/zapp4923.html). The Egyptian blogger Mostafa Hussein, who discovered the documents, argued in the NDR report that this software is "exactly like weapons" (ibid.). The Egyptian Internet activist Israa Abdel Fattah was interviewed, saying that this software is "helping the dictators […] to […] attack the activism" (ibid.). Her own Internet communication was surveilled by the Egyptian government. She said that surveillance companies "only think about money" (ibid.). NDR also describes Gamma's attempts to sell surveillance technologies to Turkmenistan and Oman (ibid.). The Austrian IT journalist Erich Möchel said that surveillance technology companies encourage "repression and torture" (ibid.).

Gamma reacted to the accusations partly by refusing to comment and partly by denying them: "Peter Lloyd, an attorney for Gamma International, told The Washington Times that the company never sold the FinFisher software to the Egyptian security ministry. But the lawyer declined to answer questions about the company's malware division, or the detailed proposal found in the Egyptian ministry. 'Gamma complies in all its dealings with all applicable U.K. laws and regulations,' Mr. Lloyd said. 'Gamma did not supply to Egypt but in any event it would not be appropriate for Gamma to make public details of its transactions with any customer' " (*Washington Times*, British Firm Offered Spy Software to Egypt: Activists Say They Were the Targets. April 26, 2011).

Gamma explains the need of surveillance technologies by threats to national security. The Egyptian revolution certainly was a threat to the national security of the old Mubarak regime. The question that arises is if a government that is questioned in mass demonstrations by its own population has the moral right to defend national security with the help of surveillance technologies that are used to spy on, imprison, torture or kill opponents. On the one hand there are claims that Gamma offered to supply Internet surveillance technologies to Egypt, on the other hand the company has denied this. FinFisher definitely is a technology that has the potential to be used for the surveillance of and repression against political opponents.

20. Telesoft Technologies

Place of business: Blandford, UK
Website: http://www.telesoft-technologies.com/
Self-description:
"Telesoft Technologies is a trusted, leading global supplier of reliable, cost effective signaling, media and packet processing solutions to service providers, governments and OEM developers worldwide" (https://www.gammagroup.com/gammatse.aspx).

Analysis

Telesoft Technologies argues that DPI technologies are needed both for law enforcement and commercial purposes: "Network operators and law enforcement agencies need the ability to identify, sort and block selected packets in IP and converged networks. Packet filtering is also becoming the basis of a new set of revenue-generating applications as the deployment of network policy solutions accelerates. Telesoft's range of packet filtering solutions perform can be deployed to perform monitoring, filtering and grooming of packets across a range of network interfaces" (http://www.telesoft-technologies.com/products/packet-filtering).

The company offers packet filtering cards as well as probes that provide "law enforcement and intelligence agencies with real-time access to content" by using "Advanced Deep Packet Inspection capabilities" that "enable the identification of specific communication content at full packet rates from multiplexed data streams" (http://www.telesoft-technologies.com/products/network-monitoring-security-control/deep-packet-inspection). "The SIP & GTP Probe supports Deep Packet Inspection from Layers 5 to 7, enabling delivery of specified content for specific subscribers, based on SIP-URI, email address, telephone number, MSISDN and IMEI, for example" (ibid.).

Telesoft Technologies says that DPI is "an essential tool for preserving network health and integrity" (20_4). Furthermore it sees economic advantages for companies: "DPI is also being deployed to deliver innovative, revenue-generating policy services. Policy control will enable the next generation of personalised services, optimised for individual users and subscribers and based on specific offers and charging plans" (20_4). It would deliver "optimised user experience and manages sessions according to charging and personal profiles".

References

Babbie, Earl. 2010. *The practice of social research*. Belmont, CA: Wadsworth.

Ball, Kirstie and Frank Webster, ed. 2003. *The intensification of surveillance. Crime, terrorism and warfare in the information age*. London: Pluto Press.

Bendrath, Ralf and Milton Mueller. 2011. The end of the net as we know it? Deep packet inspection and Internet governance. *New Media & Society* 13 (7): 1142-1160.

Bennett, Colin. 2008. *The privacy advocates*. Cambridge, MA: MIT Press.

Bennett, Colin and Charles Raab. 2006. *The governance of privacy.* Cambridge, MA: MIT Press.

Berleur, Jacques. 1999. Ethics and governance of the Internet. Introduction and recommendations of IFI-SIG9.2.2. In *Ethics and governance of the Internet*, ed. Jacques Berleur, Penny Duquenoy and Diane Whitehouse, 9-19. Laxenburg: International Federation for Information Processing.

Berleur, Jacques and Marie d'Udekem-Gevers. 2001.Codes of ethics/Conduct for computer sciences. The experience of IFIP. In *Technology and ethics. A European quest for responsible engineering, ed.* Goujon Philippe and Heriard Dubreuil Bertrand, 327-350. Leuven: Peeters.

Bigo, Didier. 2010. Delivering liberty and security? The reframing of freedom when associated with security. In *Europe's 21st century challenge. Delivering liberty*, ed. Didier Bigo, Sergio Carrera, Elspeth Guild and R.B.J. Walker, 263-287. Farnham: Ashgate.

Bigo, Didier, Elspeth Guild and R.B.J. Walker. 2010. The changing landscape of European liberty and security. In *Europe's 21st century challenge. Delivering liberty*, ed. Didier Bigo, Sergio Carrera, Elspeth Guild and R.B.J. Walker, 1-27. Farnham: Ashgate.

Centre for Irish and European Security. 2012. *Societal impact expert working group*. European Commission DG Enterprise Report.

Clarke, Roger. 1988. Information technology and dataveillance. *Communications of the ACM* 31 (5): 498-512.

Comer, Douglas E. 2004. *Computer networks and Internets*. Upper Saddle River, NJ: Pearson.

Cooper, Alissa. 2011. Doing the DPI dance. Assessing the privacy impact of Deep Packet Inspection. In *Privacy in America. Interdisciplinary perspectives*, ed. William Aspray and Philip Doty, 139-165. Plymouth: Scarecrow Press.

Daly, Angela. 2010. *The legality of deep packet inspection*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1628024

Fishman, Mark and Gray Cavender, ed. 1998. *Entertaining crime: Television reality programs*. Hawthorne, NY: Aldine de Gruyter.

Foucault, Michel. 1977. *Discipline & punish*. New York: Vintage.

Foucault, Michel. 2007. *Security, territory, population*. Basingstoke: Palgrave Macmillan.

Foucault, Michel. 2008. *The birth of biopolitics. Lectures at the Collège de France 1978-1979*. Basingstoke: Palgrave Macmillan.

Fuchs, Christian. 2008. *Internet and society. Social theory in the information age*. New York: Routledge.

Fuchs, Christian, Kees Boersma, Anders Albrechtslund and Marisol Sandoval. 2012. Introduction: Internet and surveillance. In *Internet and surveillance*, ed. Christian Fuchs, Kees Boersma, Anders Albrechtslund and Marisol Sandoval, 1-28. New York: Routledge.

Gandy, Oscar H. 2009. *Coming to terms with chance. Engaging rational discrimination and cumulative disadvantage*. Farnham: Ashgate.

Graham, Stephen and David Wood. 2003. Digitizing surveillance: categorization, space, inequality. *Critical Social Policy* 23 (2): 227-248.

Hall, Stuart et al. 1978. *Policing the crisis*. Basingstoke: Palgrave Macmillan.

Hayes, Ben. 2009. *NeoConOpticon. The EU security-industrial complex*. Amsterdam: Transnational Institute/Statewatch. http://www.statewatch.org/analyses/neoconopticon-report.pdf

Hayes, Ben. 2010. "Full spectrum dominance" as European Union security policy. On the trail of the "NeoConOpticon". In *Surveillance and democracy*, ed. Kevin D. Haggerty and Minas Samatas, 148-169. Oxon: Routledge.

Information and Privacy Commissioner of Ontario. 2009. *Creation of a Global Privacy Standard.* http://www.ipc.on.ca/images/Resources/gps.pdf

Jason, Andreas. 2011. *The basics of information security*. Waltham, MA: Syngress.

Jewkes, Yvonne. 2011. *Media & crime*. London: SAGE. Second edition.

Kling, Rob, Howard Rosenbaum and Steve Sawyer. 2005. *Understanding and communicating social informatics*. Medford, NJ: Information Today.

Landau, Susan. 2010. *Surveillance or security? The risks posed by new wiretapping technologies*. Cambridge, MA: MIT Press.

Lister, Martin, Jon Dovey, Seth Giddings, Iain Grant and Kieran Kelly. 2003. *New media: a critical introduction*. New York: Routledge.

Lyon, David. 1994. *The electronic eye. The rise of surveillance society*. Cambridge: Polity.

Lyon, David. 1998. The world wide web of surveillance. The Internet and off-world power-flows. *Information, Communication & Society* 1 (1): 91-105.

Lyon, David. 2001. *Surveillance society: monitoring everyday life*. Buckingham: Open University Press.

Lyon, David. 2003a. *Surveillance after September 11*. Cambridge: Polity.

Lyon, David. 2003b. Surveillance after September 11, 2011. In *The intensification of surveillance. Crime, terrorism and warfare in the information age*, ed. Kirstie Ball and Frank Webster, 16-25. London: Pluto Press.

Lyon, David. 2003c. Surveillance as social sorting: computer codes and mobile bodies. In *Surveillance as social sorting*, ed. David Lyon, 13-30. New York: Routledge.

Lyon, David, ed. 2006. *Theorizing surveillance*, ed. David Lyon, 23-45. Portland, OR: Willan.

Lyon, David. 2007. *Surveillance studies. An overview*. Cambridge, UK: Polity.

MacKenzie, Donald and Judy Wajcman. 1999a. Introductory essay: the social shaping of technology. In *The social shaping of technology*, ed. Donald MacKenzie and Judy Wajcman, 3-27. Maidenhead: Open University Press.

MacKenzie, Donald and Judy Wajcman. 1999b. Preface to the second edition. In *The social shaping of technology*, ed. Donald MacKenzie and Judy Wajcman, xiv-xvii. Maidenhead: Open University Press.

Marx, Gary T. 1988. *Undercover. Police surveillance in America*. Berkeley, CA: University of California Press.

McStay, Andrew. 2011. Profiling Phorm. An autopoietic approach to the audience-as-commodity. *Surveillance & Society* 8 (3): 310-322.

Monahan, Torin. 2010. *Surveillance in the time of insecurity*. New Brunswick: Rutgers University Press.

Nagenborg, Michael and Rafael Capurro. 2010. *Ethical evaluation*. EU FP7 ETICA Project – Ethical Issues of Emerging ICT Applications, Deliverable 3.2.2.

Parsons, Christopher. 2008. *Deep packet inspection in perspective: tracing its lineage and surveillance potentials. Version 1.2.* http://www.sscqueens.org/sites/default/files/WP_Deep_Packet_Inspection_Parsons_Jan_2008.pdf

Posner, Richard A. 1978/1984. An economic theory of privacy. In *Philosophical dimensions of privacy*, ed. Ferdinand David Schoeman, 333-345. Cambridge, MA: Cambridge University Press.

Poster, Mark. 1990. *The mode of information*. Cambridge: Polity.

Raab, Charles and David Wright. 2012. Surveillance. Extending the limits of privacy impact assessment. In *Privacy impact assessment,* ed. David Wright and Paul De Hert, 363-383. New York: Springer.

Ramos, Anderson. 2007. Deep packet inspection technologies. In *Information security management handbook*, ed. Harald F. Tipton and Micki Krause, 2195-2202. Sixth edition. Boca Raton, FL: Auerbach.

Riley, Chris M. and Ben Scott. 2009. *Deep packet inspection. The end of the Internet as we know it?* Florence, MA: Free Press. http://www.freepress.net/files/Deep_Packet_Inspection_The_End_of_the_Internet_As_We_Know_It.pdf

Quinn, Michael. 2006. *Ethics for the information age*. Boston: Pearson.

Shade, Leslie Regan. 2003. Technological determinism. In *Encyclopedia of new media*, ed. Steve Jones, 433-434. Thousand Oaks, CA: Sage.

Smith, Gavin. 2004. Behind the screens: Examining constructions of deviance and informal practices among CCTV control room operators in the UK. *Surveillance & Society* 2 (2/3): 376-395.

Stahl, Bernd Carsten. 2011. IT for a better future. How to integrate ethics, politics and innovation. *Journal of Information, Communication and Ethics in Society* 9 (3): 140-156.

Stallings, William. 2006. *Data and computer communications*. Eaglewood Cliffs, NJ: Prentice-Hall.

Stallings, William. 1995. *Operating systems*. Eaglewood Cliffs, NJ: Prentice-Hall. Second edition.

Stengel, Lisa and Michael Nagenborg. 2010. *Reconstructing European ethics*. EU FP7 ETICA Project – Ethical Issues of Emerging ICT Applications, Annex I to deliverable D.3.2.2.

Surveillance Studies Network. 2006. *A report on the surveillance society*. Wilmslow: Office of the Information Commissioner.

Surveillance Studies Network. 2010. *The surveillance society. An update report on developments since the 2006 Report on the Surveillance Society*. Wilmslow: Office of the Information Commissioner.

Turow, Joseph. 2008. *Niche envy. Marketing discrimination in the digital age*. Cambridge, MA: MIT Press.

Webb, Maureen. 2007. *Illusions of security. Global surveillance and democracy in the post-9/11 world*. San Franciso, CA: City Lights.

Wright, David. 2011. Should privacy impact assessments be mandatory? *Communications of the ACM* 54 (8): 121-131.

Wright, David and Emilio Mordini. 2012. Privacy and ethical impact assessment. In *Privacy impact assessment,* ed. David Wright and Paul De Hert, 397-418. New York: Springer.

Reports, Interviews, News Articles and other Documents

80/20 Thinking, *Privacy Impact Assessment for Phorm*. http://www.phorm.com/assets/reports/Phorm_PIA_Final.pdf

Amesys, Press release. September 1, 2011. http://www.wcm.bull.com/internet/pr/new_rend.jsp?DocId=673289&lang=en

ArabianBusiness, Western Spy Tools Aid in Crackdown on Arab Dissent. August 28, 2011.

ARD Tagesthemen, Siemens-Nokia Überwachungstechnik im Iran. June 24, 2009. http://www.youtube.com/watch?v=8JbydEFBx5E

BBC Monitoring World Media, Prominent Iranian Journalist Jailed for Three Years. September 30, 2010.

BBC Monitoring Europe, Italian Software Company Denies Complicity in Syrian President's Repression. November 9, 2011

Berners-Lee, Tim. 2009. *No Snooping*. http://www.w3.org/DesignIssues/NoSnooping.html

Bloomberg, Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear. November 4, 2011. http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html

Bloomberg, Iranian Police Seizing Dissidents Get Aid of Western Companies. October 30, 2011. http://www.bloomberg.com/news/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies.html

Bloomberg, Torture in Bahrain Becomes Routine With Help From Nokia Siemens. August 23, 2011. http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html

Brand Republic News Releases, EU to Take UK to Court over Internet Privacy Rules. October 4, 2010.

Bundesverfassungsgericht, Leitsätze zum Urteil des Ersten Senats vom 27. Februar 2008. http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html

*change.*org. How We Won. December 1, 2011. http://www.change.org/petitions/demand-us-and-european-cos-stop-supporting-deadly-syria-net-surveillance

Charter of Fundamental Rights of the European Union. http://www.europarl.europa.eu/charter/pdf/text_en.pdf

CNET UK, Virgin Media and CView to Rifle Through Your Packets. November 27, 2009. http://crave.cnet.co.uk/software/virgin-media-and-cview-to-rifle-through-your-packets-49304424

CNN Online, Cyberwar Explodes in Syria. November 20, 2011.

Council of Europe. *The European Convention on Human Rights.* http://www.hri.org/docs/ECHR50.html

Data Protection Commissioner of Ireland. 2011. *Facebook Ireland Ltd. Report of Audit*. 21 December 2011. http://dataprotection.ie/viewdoc.asp?m=f&fn=/documents/Facebook%20Report/final%20report/report.pdf

Electronic Frontier Foundation (EFF), *Anti-Counterfeiting Trade Agreement. What is ACTA?* https://www.eff.org/issues/acta

Electronic Privacy Information Center (EPIC), *Deep Packet Inspection and Privacy*. http://epic.org/privacy/dpi/

EU Regulation No. 961/2010 of 25 October 2010 on Restrictive Measures against Iran and Repealing Regulation (EC) No. 423/2007. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:281:0001:0077:EN:PDF

EU Regulation No. 1232/2011 of the European Parliament and the European Council of Amending Council Regulation (EC) No 428/2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-Use items. http://trade.ec.europa.eu/doclib/docs/2011/december/tradoc_148465.pdf

EU Regulation No. 267/2012 of 23 March 2012 Concerning Restrictive Measures Against Iran. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:088:0001:0112:EN:PDF

EUobserver.com, EU Companies Banned from Selling Spyware to Repressive Regimes. October 11, 2011. http://euobserver.com/1018/113791

EUobserver.com, EU to Press for 'Right To Be Forgotten' Online. November 4, 2010. http://euobserver.com/851/31200

EUobserver.com, New EU Laws to Target Facebook. January 28, 2010. http://euobserver.com/871/29367

European Commission, Telecoms: Commission Launches Case against UK over Privacy and Personal Data Protection. Press release. April 14, 2009. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570

European Parliament News, Controlling Dual-Use Exports. September 27th, 2011. http://www.europarl.europa.eu/news/en/pressroom/content/20110927IPR27586/html/Controlling-dual-use-exports

European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Directive 95/46/EC). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Eurostat. http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home/

FAKT, Syrien überwacht mit Siemens-Technik. April 10, 2012. http://www.mdr.de/fakt/siemens106.html

FCC (Federal Communications Commission). 2010. *Report and Order in the Matter of Preserving the Open Internet*. Adopted on December 21, 2010.

FIDH (International Federation for Human Rights), FIDH and LDH File a Complaint Concerning the Responsibility of the Company AMESYS in Relation to Acts of Torture, October 19, 2011. http://www.fidh.org/FIDH-and-LDH-file-a-complaintLDH

Free Press, Consumer Federation of American and Consumers Union. 2006. Why Consumers Demand Internet Freedom. Network Neutrality: Fact vs. Fiction. *http://www.freepress.net/files/nn_fact_v_fiction_final.pdf*

Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt. *http://www.buzer.de/gesetz/8578/index.htm*

Heise Online, Datenschützer prüft alle 22 Trojanereinsätze in Bayern. November 24, 2011. http://www.heise.de/newsticker/meldung/Datenschuetzer-prueft-alle-22-Trojanereinsaetze-in-Bayern-1384410.html

Heise Online, Ein "Bayerntrojaner" zum Abhören von Internet-Telefonie? January 24, 2008. http://www.heise.de/newsticker/meldung/Ein-Bayerntrojaner-zum-Abhoeren-von-Internet-Telefonie-182553.html

Heise Online, Einsatz des Staatstrojaners: Zwischen fehlendem Rechtsrahmen und Verfassungswidrigkeit. October 11, 2011. http://www.heise.de/newsticker/meldung/Einsatz-des-Staatstrojaners-Zwischen-fehlendem-Rechtsrahmen-und-Verfassungswidrigkeit-1358601.html

Hildebrand Interactive, About Us. http://www.hildebrandinteractive.com/aboutus.html

Hidebrand Initiative, Eliminating Digital Exclusion. http://www.hildebrand.co.uk/ourwork/digitalbridge.html

Lessig, Lawrence and Robert W. McChesney, No Tolls on the Internet. *The Washington Post*. June 8, 2006.

Maghreb Confidential. Alcatel-Lucent. May 9, 2008.

Möchel, Erich. *Datenjagd auf Dissidenten.* April 7, 2008. http://www.fuzo-archiv.at/artikel/268868v2/).

Morozov, Evgeny. Political Repression 2.0. *New York Times*. September 1, 2011.

NDR (Norddeutscher Rundfunk). ZAPP: Germany Spyware for Dictators. December 7, 2011. http://www.ndr.de/fernsehen/sendungen/zapp/media/zapp4923.html

NDR (Norddeutscher Rundfunk). ZAPP: Interview mit Erich Möchel. December 7, 2011. http://www.ndr.de/fernsehen/sendungen/zapp/media/moechel103.html

New York Times Online, U.S. Approval of Killing of Cleric Causes Unease. May 13, 2010. http://www.nytimes.com/2010/05/14/world/14awlaki.html

New York Times Online, E.U. to Tighten Web Privacy Law, Risking Trans-Atlantic Dispute. November 9, 2011. http://www.nytimes.com/2011/11/10/technology/eu-to-tighten-web-privacy-law-risking-trans-atlantic-dispute.html?pagewanted=all

Nokia Siemens Networks. 2009. Corporate Responsibility 2009. Espoo: NSN. http://www.nokiasiemensnetworks.com/file/12186/corporate-responsibility-2009?download

Nokia Siemens Networks, Provision of Lawful Intercept Capacity in Iran. June 22, 2009. http://www.nokiasiemensnetworks.com/news-events/press-room/press-releases/provision-of-lawful-intercept-capability-in-iran

Office of the Privacy Commissioner of Canada, Review of the Internet Traffic Management Practices of Internet Service Providers. February 18, 2009. http://www.priv.gc.ca/information/pub/sub_crtc_090728_e.cfm

Privacy International, *Online Behavioural Targeted Advertising – Privacy International's Position*. April 19, 2009. https://www.privacyinternational.org/article/online-behavioural-targeted-advertising-%E2%80%93-privacy-international%E2%80%99s-position

Privacy International, *PI Warns that New ISP Interception Plans Will Be Illegal*. November 26, 2009. https://www.privacyinternational.org/article/pi-warns-new-isp-interception-plans-will-be-illegal

Privacy International, Surveillance Who's Who. https://www.privacyinternational.org/big-brother-incorporated/countries

Profil, Trojanische Sitten. Der Bundestrojaner wurde ohne rechtliche Grundlage eingesetzt. October 22, 2010. http://www.profil.at/articles/1142/560/310153/bundestrojaner-trojanische-sitten

Proposal of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Qosmos, Qosmos Statement about Recent Media Reporting. November 22, 2011. http://www.qosmos.com/news-events/qosmos-statement-about-recent-media-reporting

ReadWriteWeb, Facebook's Zuckerberg Says the Age of Privacy is Over. January 9, 2010. http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php

Spiegel Online, Digitask: Trojaner-Hersteller beliefert etliche Behörden und Bundesländer. October 11, 2011. http://www.spiegel.de/netzwelt/netzpolitik/0,1518,791112,00.html

Spiegel Online, Fahnder: Massiver Eingriff. February 28, 2011. http://www.spiegel.de/spiegel/0,1518,748110,00.html

Spiegel Online, Innere Sicherheit: Trojaner im Abo. October 17, 2011. http://www.spiegel.de/spiegel/print/d-81015404.html

Spiegel Online, Schnüffel-Software: Bayerns Innenminister stoppt Trojaner-Einsatz. October 11, 2011. http://www.spiegel.de/netzwelt/netzpolitik/0,1518,791193,00.html

Spiegel Online, Staatstrojaner: Digitask wehrt sich gegen Inkompetenz-Vorwurf. October 12, 2011. http://www.spiegel.de/netzwelt/netzpolitik/0,1518,791251,00.html

Spiegel Online International, Is Syria Monitoring Protesters with German Technology? November 8, 2011.

Spiegel Online International, Western Surveillance Technology in the Hands of Despots. December 8, 2011.

Spiegel Online International, Monitoring the Opposition: Siemens Allegedly Sold Surveillance Gear to Syria. April 11th, 2012. http://www.spiegel.de/international/business/0,1518,826860,00.html

Techopedia. *Deep Packet Inspection (DPI).* http://www.techopedia.com/definition/24973/deep-packet-inspection-dpi

Telecom Worldwide. Alcatel-Lucent to Provide Fibre-Optic Backbone Network Contract for Libya. July 12, 2007.

The Calgary Herald, Italian Firm Helping Syria Spy on E-Mails. System Made for Repression, says Think-Tank. November 5, 2011).

The Huffington Post, Google CEO on Privacy. March 18, 2010. http://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if_n_383105.html

The Huffington Post, Eric Schmidt Dreams of a Future Where You're Never Lonely, Bored, or Out of Ideas. September 28, 2010 http://www.huffingtonpost.com/2010/09/28/eric-schmidt-techcrunch-disrupt_n_742034.html

The Local, Ericsson Rejects Claims of Aiding Iran. November 11, 2011. http://www.thelocal.se/37098/20111101

The Local, Pirate Bay to Launch Fleet of "Aerial Server Drones". March 21, 2012. http://www.thelocal.se/39796/20120321/

The Register, London Estate Broadband Offers 'Spot the ASBO Suspect' TV Channel. December 30, 2005. http://www.theregister.co.uk/2005/12/30/shoreditch_digital_bridge/

The Times, West Tries to Cover Up Libya Deals: The Race is On to Seek Out and Destroy Any Incriminating Evidence. October 7, 2011.

Wall Street Journal Online, Firms Aided Libyan Spies. First Look Inside Security Unit Shows How Citizens Were Tracked. August 30, 2011. http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html

Wall Street Journal Online, Iran's Web Spying Aided by Western Technology. June 22, 2009, http://online.wsj.com/article/SB124562668777335653.html

Washington Times, Fed Contractor, Cell Phone Maker Sold Spy System to Iran. April 13, 2009. http://www.washingtontimes.com/news/2009/apr/13/europe39s-telecoms-aid-with-spy-tech/?page=all

Washington Times, British Firm Offered Spy Software to Egypt: Activists Say They Were the Targets. April 26, 2011.

Wired Magazine Online, EU Court Rules that Content Owners Can't Force Web Filters on ISPs. November 24, 2011. http://www.wired.co.uk/news/archive/2011-11/24/eu-rules-on-filtering

Wired Magazine Online, Social Networks Don't Have to Police Copyright, Rules EU. February 16, 2012. http://www.wired.co.uk/news/archive/2012-02/16/eu-social-networks-copyright

ZDF Frontal21, Nokia-Siemens-Networks im Iran. January 26, 2010. http://www.youtube.com/watch?v=oHqyKYa6Ffw

ZDNet UK, Virgin Media Puts CView Packet Sniffing Trial on Hold. September 30, 2010. http://www.zdnet.co.uk/news/security-threats/2010/09/30/virgin-media-puts-cview-packet-sniffing-trial-on-hold-40090353/