Institute of Computer Science
Georg-August University of Göttingen, Germany

# Lawful Interception vs. Privacy in Online Communications

Tobias-André Staub
Flachsbachstr. 9, 37242 Bad Sooden-Allendorf
Matrikelnummer: 20213734

Seminar on Internet Technologies
Prof. Dr. Xiaoming Fu
SS 2008

## Table of Content

# 1 Introduction

In the last decades the internet became a popular and easy to use medium that offers a lot of advantages compared with other media. Once connected to the global network you can start investigations by accessing a large pool of information, you can buy products and order different services without going to a market or supplier. But what is more important, you can communicate in a comfortable way by writing emails or sending instant messages and your partner can answer just in time or even delayed in time. 68% of the german population used the internet in the first quarter of 2007, whereas 86% of them used it for email [1].

## 1.1 Types of Online Communications

There are different types of communications when using the internet. The most popular form is to contact your friends and partners by sending and receiving electronic mails. This way information can be delivered very quickly and for free. With an attachment you can transmit other electronic documents like pdf-files, pictures, movies etc. Another popular form of communication is instant messaging, what is similar to email but you can easily write real-time messages, which are transmitted instantly. Actually you can see whether your communication partner is online or not. There are different clients like AIM, ICQ, Windows Messenger, Skype etc. and they use different protocols. A real-time form of communication is the chat. On the technical level there are internet relay chat (IRC), webchat and instant messaging, too. The users sign on and meet in a virtual room, where they can talk to all participants on the one hand or to selected persons on the other hand. IRC requires a client software, whereas webchat can be used within a browser. In the web you can exchange information in public, what is relevant when you want to address a large range of people. You can write in forums and newsgroups pseudonymously without revealing your identity. The other way round you can hide your personal information by giving yourself a pseudonym or try to surf anonymously with purpose-built tools. Of course you can have your phone calls over the internet instead of the public switched telephone network. This process is called Voice over Internet Protocol (VoIP). In the most cases outgoing calls are much cheaper and even for free, when calling members that are registered at the same service. Technically the

voice stream is digitized and wrapped into packets, so there is no real connection between the communication partners.

# 2 Definition and Motivation for Lawful Interception

Lawful Interception means legal and authorized interception of telecommunications by law enforcement agencies (LEA) and intelligent services. Those measures are based on national laws and regulations. For Europe there is a directive called “Convention on cybercrime".

The goal is to get information about criminals and their activities, especially to identify networks of relationships between suspected criminals. Mostly persons in the scope of terrorism, pedophilia rings, cyber stalking, data theft and drug dealing are targeted [2]. It is hard to catch those criminals red-handed, an unequivocal evidence is necessary. Therefore the focus will be on an account, e.g. DSL, email, SIP etc, to detect projected activities [3].

There are statistical information about interceptions in Germany for the year 2005. The government confirmed 4925 criminal proceedings with 12606 persons affected [4,5]. 279 email accounts were intercepted; we talk about 216 more than just one year before. At all the number of interceptions related to the internet access increased to 193, so there are 101 more cases compared to 2004.

# 3 The European Telecommunications Standards Institute (ETSI) serving as example for the implementation of Lawful Interception

## 3.1 Requirements of Lawful Interception

It is up to the network operator, access provider and service provider to ensure the feasibility of an interception by providing ordained interfaces. On the other side they are not allowed to monitor results. In case of a network internal encryption they have to remove it for the interception. The integrity and confidentiality of information must be guaranteed. When intercepting a target, all communication has to be considered that means twenty four hours and seven days a week. It is an expensive operation for the commissaries and so they let the customer pay for that in form of general price adjustments. Only authorized personnel, from the LEA for instance, can initiate an

interception and has to do it in a transparent way and for the specified traffic only. Therefore every use of the Lawful Interception equipment has to be logged. The most important thing is that an interception has to undetectable that means the subject must not be aware of such a measure [6].

### 3.2 The ETSI Reference model

Almost all countries have adopted global Lawful Interception requirements and standards from the European Telecommunications Standards Institute (ETSI) [7]. Their lawful interception standards are used throughout Europe, much of Asia and soon in Australia.

The ETSI reference model for IP networks is described in the technical report TR 102 528 [8] and shown in figure 1. The idea is to separate the function of interception at network elements from delivery of the information to the LEA. We can see that the system consists of two domains, one for the communications service provider (CSP) and one for the law enforcement agency (LEA). Both parts are interacting via the handover interfaces HI1, HI2 and HI3, so there is no direct access to the CSP domain.

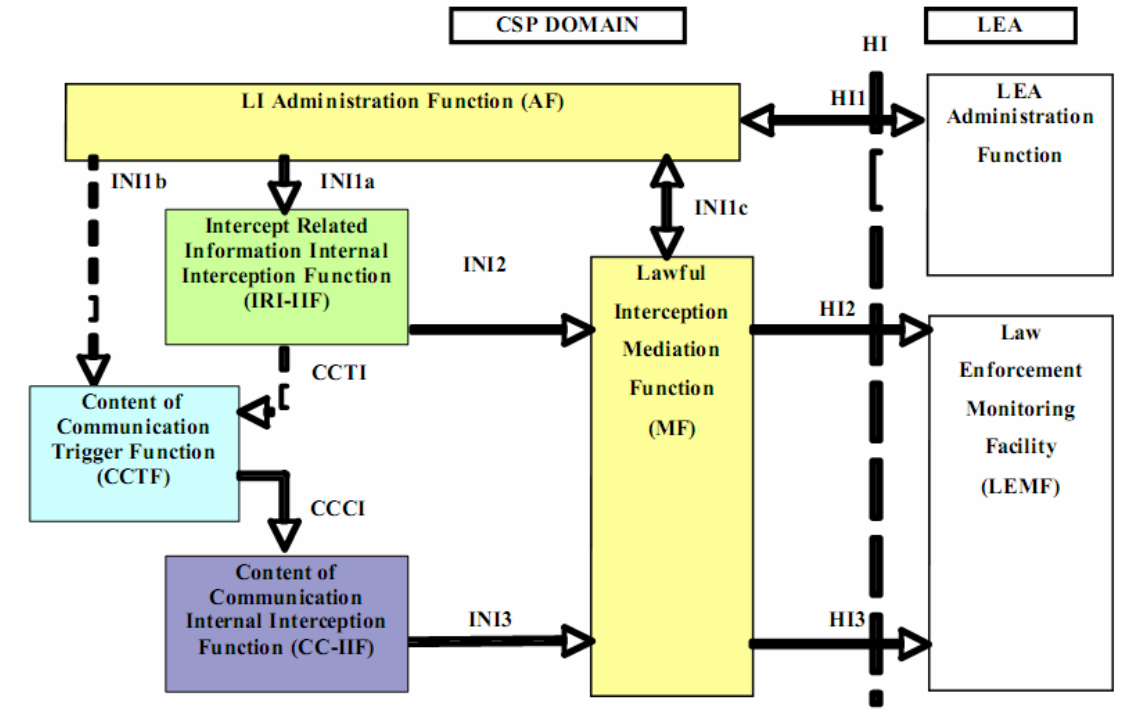


**Figure 1: Reference model for Lawful Interception in IP networks.**

There are three different functions that have to be explained, the Administration Function, the Mediation Function and the Access Function.

The LEA sends a warrant to the LI Administration Function (AF) over the interface HI1. The AF is a user interface to administrate the components and interception measures. It should exist in each service provider network; so that the LEA can send intercept requests. There are information about the warrant available, e.g. identification of the intercepted subject, start, end and duration of the measure, type of gathered information (signalling information or content) etc. The AF provisions the Mediation Function over the Internal Network Interface 1c (INI1c).

The Mediation Function (MF) communicates with the Intercept Related Information Internal Interception Function (IRI-IIF) and the Content of Communication Internal Interception Function (CC-IIF). The MF receives information about active intercepts on the one hand and it correlates and formats that information for delivery to the Law Enforcement Monitoring Facility (LEMF). Therefore it uses the HI2 and HI3 interfaces, whereas HI2 is used for Intercept Related Information (signalling) and HI3 is used for content.

The Intercept Related Information Internal Interception Function (IRI-IIF) generates the information associated with sessions, calls, connections and so on. The data will be sent to the Content of Communication Trigger Function (CCTF) over the Content of Communication Trigger Interface (CCTI) and to the MF over the Internal Network Interface 2 (INI2).

The Content of Communication Trigger Function (CCTF) determines the location of the intercepted device. It is dynamically controlled by the IRI-IIF using the CCTI. Over the Content of Communication Control Interface (CCCI) the CCTF has influence on the Content of Communication Internal Interception Function (CC-IIF).

The CC-IIF duplicates the content and sends it to the MF via the Internal Network Interface 3 (INI3). It can be delivered as a stream of IP packets with a special correlation header or as files over FTP [9]. While copying the parties' traffic, there will be no retransmission, except one member will retransmit due to transmission problems.

The Lawful Interception system prevents detection by unauthorized entities. Therefore they are able to check the IP addresses via traceroute and the measurement of rount trip delay etc., to check if any unusual signalling is occurring and to detect degradation or interruptions in service.

### 3.3 The difference between PSTN and IP networks

In contrast to PSTN with its circuit switching IP is a connectionless protocol based on packets and that means there is no call setup process at all. The path of the packets varies and whereas one passes the direct way to the destination another one uses a different route. The signalling information is tightly bound to the content of the communication. So you cannot intercept one single line like in the PSTN, you have to examine each single packet [10].

“Tunneling” seems to be a problem, because in this case an IP packet is encapsulated into another IP packet. A test will not find the “hidden” information, thus the LI equipment has to recognize tunneling in order to extract the contained message.

Another problem is encryption. The ISP has to remove the network internal encryption, but if the user ciphers its information the LEMF will get useless content, because it is ciphered.

To analyse the IP packets of a target so called “sniffers” are used. The underlying idea of such hardware was to diagnose network faults, now the job is to capture traffic of interest by listening to specific IP addresses. Therefore a sniffer is installed on key points in the network and it monitors logins, which are messages handled by RADIUS daemons.

### 3.4 An example for Lawful Interception of VoIP

Figure 2 shows that VoIP distinguishes between signalling (call setup and control) and content (data stream containing voice) [11]. When the user wants to initiate a call, he has to contact the Signalling provider to determine the position (IP address) of the interlocutor. At the same time, the signalling server knows the position of the caller. The communication partner can now get informed about the phone call. After setting up a connection both persons are talking with each other using their own P2P connection over an Access-Provider. The signalling server is not involved in the transmission of content.

To intercept the VoIP data stream an Administration Function has to be implemented at the Signalling provider. Under the premise that the AF has got a warrant, the Signalling server awaits the login of a specific account. When the user tries to contact the server, the AF gets informed about this progress. Consequently the AF will instruct the Access-Provider to intercept the content of communication. The LEA receives the Intercept

Related Information over the HI2 interface and the content of the communication over the HI3 interface.

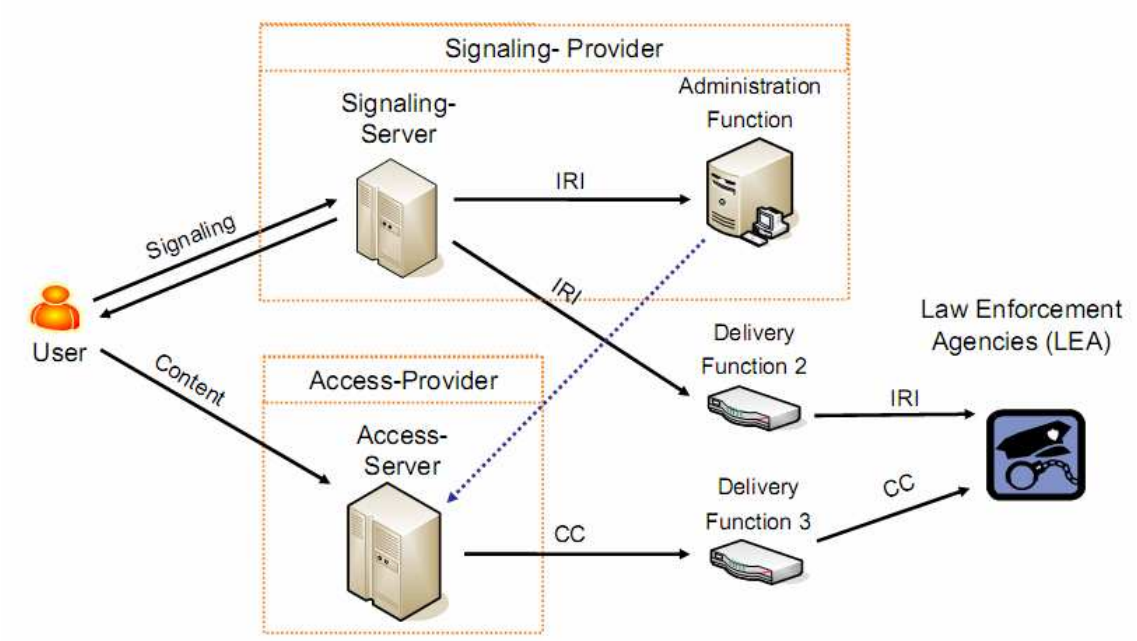


**Figure 2: Example for the interception of VoIP traffic**

# 4 Online Privacy

## 4.1 The need of privacy

Due to the important role of online communication it is obvious that the exchange of private or business information (especially of lawyers, physicians etc.) has to be protected in general. Systems for Lawful Interception can have flaws in security, so that there is a chance for illegal operations. They are objectives for “hackers”, because accessing the list of warrants, in particular to add, modify or delete entries, can be attractive. On the other side it is also very interesting to use such a system for monitoring the traffic of other users.

## 4.2 Technical measures to protect privacy

In the following subchapters some technical measures to thwart interceptions are described. Either you encrypt the content of your communication or you try to hide your

identity by ensconcing the IP address. There are many interesting projects that deal with data privacy.

### 4.2.1 HTTPS / SSL /TLS

The Hypertext Transfer Protocol over Secure Socket Layer was originally developed by Netscape in 1994. The company was taken over by AOL [12] and the Netscape browser became open source and was refined by the Mozilla project [13]. With the help of Secure Socket Layer or Transport Layer Security the protocol establishes a secure HTTP connection. There is an additional encryption and authentication layer between HTTP and TCP.

The Server sends a certificate, which contains the name, the public key, the period of validity and so on. Now the client can randomly generate a key, so that both partners can communicate with each other and nobody can spy them or manipulate the sent data. This method works with websites and email servers (pop3 and smtp) [14]. The problem is that only the content is safe from interception, but a server administrator can be required to hand out logfiles or even to intercept on serverside.

### 4.2.2 Pretty Good Privacy (PGP) / GnuPG / OpenPGP

In 1991 Philip Zimmermann created a computer program to increase the security of email communication. The objective of Pretty Good Privacy [15,16] or GnuPG [17] is to sign, encrypt and decrypt emails. Therefore it uses public key cryptography with an asymmetric encryption. The user has got both, a private and a public key. The public key is uncritically and can be shared with all partners, so that they can encrypt the emails with this signature. The decryption requires the corresponding private key, which belongs to the recipient. An interception will only discover who is communicating with whom, but the content is a secret and not readable.

Enigmail [18] is an OpenPGP plugin for the open source mail client Mozilla Thunderbird (thunderbird), so it gets very simple to send encrypted and digitally signed emails.

### 4.2.3 ZFone / PGPfone

Philip Zimmermann also created with PGPfone an application to encrypt VoIP traffic. The current software is called ZFone [19] and supports all VoIP protocols like SIP and RTP. Furthermore it can be used with different softphones, e.g. X-Lite, Gizmo,

Xmeeting, Google Talk or SJphone. The problem of classic VoIP encryption can be found in the negotiation of session keys. Skype for instance involves the SIP server in the negotiation process, so there is a chance to intercept the session keys at the server. ZFone implements an own ZRTP protocol and uses Diffie-Hellmann for the negotiation, so both communication partners compound with each other and in this case there is no need of a server. Eavesdropping can be impeded successfully, because the keys are not transmitted over the network. Then the complete communication will be done over an encrypted SRTP session.

Ed Felten, a professor at the Princeton University, sees ZFone to be vulnerable to spyware [20]. In his opinion the unciphered data sream can be captured by tapping the communication between the softphone and ZFone. That will be the only way to confound encryption, but at the moment he denotes it as future prospects.

### 4.2.4 JonDonym / AnOn / JAP

The University of Dresden developed the Java Anon Proxy (JAP) software and the AN.ON service [21] in form of a research project. To improve anonymity, the user has to install the java based software which works as a proxy. The browser will now send the messages to JAP, where they will be encrypted and forwarded to the MIX cascade of the AN.ON service that consists of three fixed nodes. The last node of the internal network decrypts the messages and delivers them to the destination. This way the address of the sender is even for the MIX cascade unknown.

Since 2006 no more subsidies are given to the project, so the service became a commercial product and is now called JonDonym [22]. You have to pay for the MIX cascades and the premium service, whereas AN.ON is at the moment still free of charge but it will be a commercial service in the future. JAP in general is supported by essential institutions like the “Chaos Computer Club Berlin” or the “Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein”. The chargeable JonDonym offers different rates and prices to provide some features like high availability, good performance, high security and support of all internet ports.

### 4.2.5 The Onion Router (TOR)

The Onion Router [23] is a software project recommended by the Electronic Frontier Foundation [24]. The goal is to thwart traffic analysis and to improve privacy and security of the internet. The software gives you access to a distributed and anonymous network that works like a virtual tunnel and can handle TCP connections. The idea is

similar to JonDonym and AN.ON, but the messages take a random pathway through the worldwide TOR network and the service is for free. There is no static MIX cascade like in JonDonym or AN.ON. The messages are encrypted and forwarded by three different nodes before they are decrypted and leave the internal network. This way the address of the sender is even for the TOR network unknown. You can easily integrate TOR into Firefox.

The only disadvantage is that in contrast to other MIX cascades only TCP communication is handled. The most critical aspect of TOR is that the last node can be compromised is able to analyse the complete traffic that leaves the network. Dan Egerstad has shown that illegal abuse in this form is possible [25].

### 4.2.6 Virtual Private Network (VPN)

A Virtual Private Network is a network which is not carried by physical wires, but it reverts to existing infrastructure e.g. the public internet. It allows accessing the internal network, because IP packets with a different address (often private addresses like 10.40…) are encapsulated into routable packets. To ensure privacy all data between two communicating partners will be encrypted, that is why we talk of a "Tunnel" [26]. For this kind of communication you can use different protocols like IPSec or the Point-to-Point Tunnelling Protocol. In the past the setup of a VPN was a little bit complicated, but nowadays there are comfortable tools like OpenVPN [27] for an end-to-end connection or CyberGhostVPN [28] for internet access.

OpenVPN is an open source alternative to a lot of commercial products and among other things it offers web-based management and simplified configuration. The software generates a VPN over an encrypted TLS connection. Therefore it uses OpenSSL libraries. For the transport TCP as well as UDP are supported. We decide two forms of authentication, pre-shared-key on the one side and certificates on the other.

CyberGhostVPN is a commercial service maintained by S.A.D. [29]. The company also offers a limited basic version for free. All you need is client software that establishes a connection to the CyberGhostVPN server and the data stream over the public internet will be encrypted with 128 bit AES. Furthermore like using a proxy your IP address will be hidden, so you can surf anonymously.

### 4.2.7 Invisible Internet Project (I2P)

In 2003 the Invisible Internet Project [30] was founded as an open source project. The aim is to build an anonymizing network with low latency. Until now there is only a

version for testing and it seems that the stable release of version 1.0 will take a while. In contrast to other projects like JonDonym/AN.ON or TOR not only the request of clients are veiled, moreover the complete internet should be masked. That is why I2P is something like an “internet in the internet”. You can also access the “normal” internet by using so called Out-proxies, which are apparently overwhelmed with work. However the idea is to provide a full range of internal services. The application Syndie offers you anonymous web browsing, anonymous web hosting, anonymous blogging and content syndication. I2PSnark is an anonymous file sharing tool, I2Pmail and susimail are anonymous email services and there are a lot of other anonymous activities like newsgroups, chat etc.

The Semireliable Secure UDP (SSU) is a protocol for the communication over several nodes on which the software runs. Within the network there is a peripheral database, where all routers gather information about the network autonomously. The path between the user and a destination (website or other services) is called “tunnel”, because the information are signed with a 1024 bit DSA key and encrypted via 256 bits AES [31]. In general all messages are encrypted more than once. This is done with the “garlic” method which is an extension of the more common “onion” encryption. Multiple messages are wrapped up into a “garlic message”, which will be encrypted with a public key, so nobody can determine how many items are contained.

### 4.2.8 Freenet Project

The Freenet Project [32] is based on the idea of Ian Clarke, who was a student at the University of Edinburgh and wanted to build an anonymous system which is not a subject of censorship. In cooperation with volunteers, among others Matthew Toseland, he created a P2P software to distribute information within a network [33]. Their goal was to split the file into fragments which are encrypted and distributed over multiple clients. So there is no central location for the file and no user can determine, who has published it. On the other side an already published file cannot be removed from the network. The user is not responsible for copyrighted content, because the “splitfiles” on the hard disc are encrypted.

You can use Freenet with any browser. There is no special tool for searching; the content will be listed and linked on websites, so called “freesites”. Like in other P2P networks the request of a client will be passed from one node to another in an encrypted form. In case of a finding the requested fragments are handled the same way. That is also an aspect of anonymity, because the receiver of a fragment could be the final

recipient or just a transfer hatch. A disadvantage of this method is the permanent traffic that causes a deceleration of the network.

## 5 Discussion

Lawful Interception is a polarizing topic and can be reduced to the fact that it is always a compromise between security and people's freedom. On the one side everybody wants to be protected and secure, but on the other side people long for freedom and do not want to be under police surveillance. These different interests can hardly be combined.

There is a report about a sniffer which was installed at the internet service provider by the Law Enforcement Agency [10]. They did this action on their own and started their interceptions. After the surveillance they took the sniffer and examined the captured traffic. In this case there is no separation of responsibility between the LEA and the ISP.

We have seen that encryption successfully protects the content of a communication. Criminals could have the chance to hide behind ciphered data streams, but the most important part of an interception is the Intercept Related Information. The motivation is primarily to reveal networks of relationships. There is also research in doing interception on the application level, so special spyware will send the desired information to the LEMF before it is encoded.

In 2004 there was the "Unlawful interception" scandal in Greece [34]. More than 100 mobile phone numbers were wrongfully under surveillance for 11 months. The offenders accessed the LI subsystems by passing the authorization mechanism and got the chance for an abuse. Vodafone noticed the incursion one year later during a routine examination. It is a negative example that shows how dangerous the security leaks of LI systems can be.

## 6 Conclusions

Lawful Interception is a powerful tool to locate criminals and get informed about their (planned) activities. It should be used in exceptional cases, where other actions fail. How far those measures against criminals are successful is still not clear, because content encryption is still a problem and hinders the investigations.

At the present moment people have the right to encrypt their online communication, to use pseudonyms and to surf anonymously. In Germany the federal data protection act

strongly encourages to those measures. The “Federal Ministry for Security in Informational Technology” also provides software downloads and manuals to the in chapter 4.2 mentioned security tools.

## Abbreviations

| | |
|---|---|
| AES | Advanced Encryption Standard |
| AF | Administration Function |
| CC-IIF | Content of Communication Internal Interception Function |
| CCCI | Content of Communication Control Interface |
| CCTI | Content of Communication Trigger Interface |
| CCTF | Content of Communication Trigger Function |
| CSP | Communication Service Provider |
| EFF | Electronic Frontier Foundation |
| HTTP | Hyper Text Transport Protocol |
| INI | Internal Network Interface |
| IRI | Intercept Related Information |
| IRI-IIF | Intercept Related Information Internal Interception Function |
| ISP | Internet Service Provider |
| LEA | Law Enforcement Agency |
| LEMF | Law Enforcement Monitoring Facility |
| LI | Lawful Interception |
| P2P | Peer to peer |
| POP3 | Post Office Protocol Version 3 |
| PSTN | Public Switched Telephone Network |
| RTP | Realtime Transport Protocol |
| SIP | Session Initiation Protocol |
| SMTP | Simple Mail Transfer Protocol |
| SRTP | Secure Realtime Transport Protocol |
| SSL | Secure Socket Layer |

| | |
|---|---|
| TCP | Transport Control Protocol |
| TLS | Transport Layer Security |
| TOR | The Onion Router |
| UDP | User Datagram Protocol |
| VoIP | Voice over Internet Protocol |

## Figures

## References


[1] “Statistisches Bundesamt Deutschland - Private Nutzung von Informations- und Kommunikationstechnologien”; http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Statistiken/Informationsgesellschaft/PrivateHaushalte/Tabellen/Content75/ZeitvergleichComputernutzung,templateId=renderPrint.psml.

[2] Datenschutzgruppe der Roten Hilfe Heidelberg, “Lawful Interception (rechtmäßiges Abhören) von IP-Datenverkehr”; http://gipfelsoli.org/rcms_repos/Antirepression/lawful_interception.pdf.

[3] H. Scholz, “Lawful Interception in German VoIPNetworks”; http://events.ccc.de/congress/2005/fahrplan/attachments/617-slides-voip-lawful-interception.pdf.

[4] “LawfulInterception - Datenschmutz Wiki”; http://www.datenschmutz.de/cgi-bin/moin.cgi/LawfulInterception.

[5] Deutscher Bundestag, “Schriftliche Fragen mit den in der Woche vom 16. Oktober 2006 eingegangenen Antworten der Bundesregierung,” Nov. 2006; http://dip.bundestag.de/btd/16/030/1603054.pdf.

[6] ETSI, “Lawful Interception (LI); Requirements of Law Enforcement Agencies”; http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=22450&curItemNr=1&totalNrItems=1&optDisplay=10&titleType=all&qSORT=HIGHVERSION&qETSI_ALL=&SearchPage=TRUE&qETSI_STANDARD_TYPE=%27TS%27&qETSI_NUMBER=101+331&qINCLUDE_SUB_TB=True&qINCLUDE_MOVED_ON=&qSTOP_FLG=N&qKEYWORD_BOOLEAN=OR&qSTOPPING_OUTDATED=&butExpertSearch=Search&includeNonActiveTB=FALSE&includeSubProjectCode=FALSE&qREPORT_TYPE=SUMMARY.

[7] “ETSI”; http://www.etsi.org/WebSite/homepage.aspx.

[8] ETSI, “Lawful Interception (LI); Interception domain Architecture for IP networks”; http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=23389&curItemNr=1&totalNrItems=1&optDisplay=10&titleType=all&qSORT=HIGHVERSION&qETSI_ALL=&SearchPage=TRUE&qETSI_STANDARD_TYPE=%27TR%27&qETSI_NUMBER=102+528&qINCLUDE_SUB_TB=True&qINCLUDE_MOVED_ON=&qSTOP_FLG=N&qKEYWORD_BOOLEAN=OR&qSTOPPING_

OUTDATED=&butExpertSearch=Search&includeNonActiveTB=FALSE&includeSubProjectCode=FALSE&qREPORT_TYPE=SUMMARY.

[9] ETSI, “Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture ”; http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=25247&curItemNr=1&totalNrItems=2&optDisplay=10&titleType=all&qSORT=HIGHVERSION&qETSI_ALL=&SearchPage=TRUE&qETSI_STANDARD_TYPE=%27TR%27&qETSI_NUMBER=101943&qINCLUDE_SUB_TB=True&qINCLUDE_MOVED_ON=&qSTOP_FLG=N&qKEYWORD_BOOLEAN=OR&qSTOPPING_OUTDATED=&butExpertSearch=Search&includeNonActiveTB=FALSE&includeSubProjectCode=FALSE&qREPORT_TYPE=SUMMARY.

[10] P. Branch, “Lawful Interception of IP Traffic ”; http://caia.swin.edu.au/pubs/ATNAC03/branch-ATNAC2003.pdf.

[11] R. Winschuh, “Lawful Interception of VoIP”; http://iptel.org/voipsecurity/doc/06%20-%20Winschuh%20-%20Lawful%20Interception%20of%20VoIP.pdf.

[12] “AOL.de | Kostenlose Email, Nachrichten & Wetter, Sport, Shopping und Star-News auf AOL.de”; http://www.aol.de/.

[13] “Mozilla.org - Home of the Mozilla Project”; http://www.mozilla.org/.

[14] “Einen Blick in die schwarze Kiste wagen - Anregungen zu einem kritischen Umgang mit dem Internet,” Juni. 2007; http://www.offene-uni.org/_media/offene-uni2/workshops/fertig.pdf?id=offene-uni2%3Aworkshops%3Adatenschutz&cache=cache.

[15] “PGP Corporation - Startseite”; http://www.pgp.com/de/.

[16] “The International PGP Home Page”; http://www.pgpi.org/.

[17] “The GNU Privacy Guard - GnuPG.org”; http://www.gnupg.org/.

[18] “Enigmail: A simple interface for OpenPGP email security”; http://enigmail.mozdev.org/home/index.php.

[19] “Zfone Project Home Page”; http://zfoneproject.com/.

[20] “gulli: ZFone: Verschlüsseltes Telefonieren via VoIP auch für Windows”; http://www.gulli.com/news/zfone-verschl-sseltes-2006-05-23/.

[21] “JAP -- ANONYMITY & PRIVACY”; http://anon.inf.tu-dresden.de/index.html.

[22] “JonDonym - der Internet-Anonymisierungsdienst | JonDos GmbH”; https://www.jondos.de/de/.

[23] “Tor: Anonymität online”; http://www.torproject.org/index.html.de.

[24] “Electronic Frontier Foundation | Defending Freedom in the Digital World”; http://www.eff.org/.

[25] “heise Security - 31.08.07 - Zugangsdaten für Regierungs-Mail-Accounts veröffentlicht”; http://www.heise.de/security/Zugangsdaten-fuer-Regierungs-Mail-Accounts-veroeffentlicht--/news/meldung/95262.

[26] “VPN - Wissen - Meyers Lexikon online”; http://lexikon.meyers.de/wissen/VPN.

[27] “Welcome to OpenVPN”; http://www.openvpn.net/.

[28] “CyberGhost VPN - Anonym surfen im Internet”; http://www.cyberghostvpn.com/anonym_surfen.php.

[29] “S.A.D.de - Things are different”; http://www.my-sad.com/.

[30] “I2P Anonymous Network - I2P”; http://www.i2p2.de/.

[31] “TP: Anonyme Internetnutzung mit dem Invisible Internet Project (I2P)”; http://www.heise.de/tp/r4/artikel/25/25273/1.html.

[32] “The Freenet Project - /index”; http://freenetproject.org/.

[33] “Anonym im Netz: EFF-Gründer unterstützt Freenet Project - Golem.de”; http://www.golem.de/0608/47274.html.

[34] “Abhörskandal: Vodafone droht 170-Millionen-Bußgeld - Netzwelt - SPIEGEL ONLINE - Nachrichten”; http://www.spiegel.de/netzwelt/mobil/0,1518,438072,00.html.