

# Developing a Legally Compliant Reachability Management System as a Countermeasure against SPIT<sup>1</sup>

Markus Hansen, Marit Hansen, Jan Möller,<sup>2</sup>  
Thomas Rohwer, Carsten Tolkmit,<sup>3</sup>  
Henning Waack<sup>4</sup>

## **Abstract:**

*This paper explains why SPIT (Spam over Internet Telephony) is harder to filter than conventional e-mail spam, lists scenarios, possible countermeasures, and presents a prototype for a legally compliant and privacy-friendly SPIT-filtering reachability management system that is currently in development within the SPIT-AL project.*

## **Keywords:**

*spam, spit, spam over internet telephony, internet telephony, voip, voice-over-ip, privacy, reachability management*

## **1. Introduction**

Internet Telephony has developed to a degree that allows a cost-saving use of VoIP technology [1], meets professional needs, and does not require detailed technical knowledge.

It can reasonably be assumed that VoIP will unfold the same effects on telephony that e-mail did with respect to written communication. One of these effects will be unsolicited advertising calls, or SPIT (Spam over Internet Telephony) [11][13]. SPIT calls can originate from both humans (e.g., in call centres) or automated devices, and legislation prohibiting such calls is most often effectless against calls from other countries [4]. Therefore, as with e-mail, there will be a growing demand for SPIT-filtering applications.

E-mail as asynchronous communication allows for several filtering mechanisms to be applied to the full content of the communication before being presented to the user (or marked as SPAM or even deleted). Telephony in contrast is synchronous communication and therefore does not provide much information prior to the transmission of the content, making it both harder to filter and more annoying to users.

As telecommunication (at least in Germany) is protected by several laws, instances filtering mails or calls face several legal consequences (e.g., imprisonment). Therefore, it is mandatory not only to construct technical filtering mechanisms, but also to consider implications from telecommunication or privacy protection laws and regulation [2].

This article is mainly based on a white paper on SPIT filtering [12] that has been created within the SPIT-AL project, which aims to develop an open source SPIT filter that is effective, legally compliant, and

privacy-friendly. The approach incorporates aspects of reputation systems [8] to implement a reachability management system [7]. The SPIT-AL project is sponsored by the European Regional Development Fund within the "e-Region PLUS" programme of Schleswig-Holstein and by funds of the Land (federal state) Schleswig-Holstein.

## **2. SPIT Scenarios and Possible Countermeasures**

The following scenarios are not necessarily limited to Internet telephony, but their realisation in the near future is likely to happen within this context.

Telephony protocols of modern technology platforms (e.g., Internet telephony) often contain mechanisms to request context information. E.g., it is possible to request the reachability status of the other party or to transmit a short message that could also be used for advertising. It is also possible to submit instant messages that could be used as a transport channel for unsolicited advertisement.

Of course, it is also possible to use the telephony functionality to transmit advertising audio messages or simply advertising calls.

### **2.1 SPIT Scenarios**

#### **2.1.1 Call Centres**

In call centres, call centre agents conduct advertising calls. A computer systematically or at random selects a party to call. In case a party responds to a call, it is dispatched to an available agent.

The operator of such a call centre has to cover the costs for his employees, for computer hardware, and for established calls, whereas the latter is expected to be negligible within the context of Internet telephony.

<sup>1</sup> This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 2.5 License. <http://creativecommons.org/licenses/by-nc-nd/2.5/> - If you like to contribute, please contact the authors.

<sup>2</sup> Independent Centre for Privacy Protection Schleswig-Holstein, Kiel, Germany, <http://www.datenschutzzentrum.de/>

<sup>3</sup> TNG – The Net Generation AG, Kiel, Germany, <http://www.tng.de/>

<sup>4</sup> Dresden University of Technology, Dresden, Germany, <http://www.inf.tu-dresden.de/>

The number of possible simultaneous calls – and therefore the spam impact – primarily depends on the number of employees.

### **2.1.2 Calling Bots**

Internet telephony is a communication platform strongly dependent on computers. It is therefore likely that the same computers – systematically or at random – select a party to call and transmit a prerecorded advertising message once the call is accepted.

### **2.1.3 Ringtone SPIT**

Some VoIP telephones come pre-configured in a way that they accept a special SIP header information called "Alert-info" which may contain an URL pointing to a prerecorded audio file somewhere on the Internet. Obviously, this can be used to play advertising messages before the call has even been accepted by the user just as the phone is ringing. Proper configuration, i.e., not allow downloading ringtones from the Internet, should solve the problem.

### **2.1.4 Combinations**

Combinations of the predescribed scenarios are thinkable and likely to occur. Costs for the initiator will be in between those for the single scenarios.

## **2.2 Approaches for Countermeasures**

Depending of the kind of spam, there are different possible approaches to counter it. Below, several countermeasures will be discussed.

Protocol spam (e.g., by exploiting VoIP protocol functionality such as requests for reachability) will presumably not result into a high amount of spam, as the message content that can be send is rather limited in both length and presentation options. Thus the advertising potential is as limited. We therefore are not discussing protocol spam in the following.

Effective countermeasures for instant message spam already exist, e.g., the usage of buddylists. As it can be assumed that this kind of communication will be performed with communication partners rated as 'friendly' only, this countermeasure will still be available in the future. Sending instant messages however is not directly inherent to telephony, so we will not discuss this kind of advertising.

For actual SPIT at the moment there are only few to none countermeasures, and the amount of this kind of spam will increase in the future. The concept discussed in this article focuses on countering advertising using telephony. We have found the following approaches for countermeasures. Using several approaches in combination is also possible.

### **2.2.1 Costs for Telephony**

A common approach to protect against unwanted advertising calls is to increase the costs for the caller. This is of course in contradiction to the decrease of costs expected from Internet telephony. Nevertheless, this approach can still be useful to allow an initial contact at higher costs by unknown callers that would otherwise get rejected, e.g., by pointing them to PSTN<sup>5</sup> or letting him perform a task (see below) to identify.

### **2.2.3 Buddylists / Whitelists**

Each subscriber to the telephony service is maintaining a list of other subscribers he is willing to accept calls from unlisted third-party subscribers cannot call the first. This results into problems regarding initial contact. While this mechanism is good to prevent SPIT calls, it would also reject otherwise welcome callers. As a result of an exclusive use of whitelists, telephony would not allow initial contact anymore. For the realisation of the SPIT-AL concept, a rather similar mechanism might be of use.

### **2.2.4 Extended Whitelist with Web of Trust**

To allow calls from callers not listed on the personal whitelist, it could be helpful to access a web of trust. Each subscriber grants his trust to several other subscribers, thus benefitting from their whitelists by directly accepting calls from callers listed there. If these lists got transmitted from trusted parties to trusted parties of trusted parties, a significantly higher number of callers could reach the subscriber without facing problems [9]. The basic problem of a caller still exists though, i.e., at least one entry in one of the lists within the trusted circle has to exist beforehand.

### **2.2.5 Blacklists**

Blacklist can either be maintained by the subscriber himself or there may exist one or several central blacklists. Callers disseminating SPIT get listed on those blacklists, thus preventing further calls from these originators. The subscriber will then only accept calls from people not listed on any of the blacklists. This approach is limited to denying calls from known spammers. In case each subscriber is maintaining his own list and therefore can only access his own data, it is very likely that the recognition rate of SPIT will stay low. A central blacklist would be more effective, but cannot deny calls from unidentified spammers either.

### **2.2.6 Statistical Blacklists**

Telephony providers and carriers can analyse certain traffic data and, using statistical methods, conclude on the nature of the calls. E.g., in case the same caller is calling several hundred different numbers within a

---

5 Public Switched Telephone Network, also known as Plain Old Telephone System (POTS)

certain time interval and the resulting connections are rather short, there is a certain probability the caller is a spammer. The caller can then be added to a blacklist subscribers can benefit from as further calls from the same caller can then be rejected. Entries on statistical blacklists could have properties like a fade-out time, so that honest users can "redeem" themselves by good behaviour.

### 2.2.7 Voice Menu Interaction

Before being connected to the subscriber, the caller will be directed to an automated voice menu and will have to perform a task, e.g., 'Please press 635#\*' to be connected to the subscriber'. Only after correctly completing the given task, the connection to the subscriber gets established. Thus, the task functions as an audio captcha.

Provided the code to enter is random, this approach can effectively block spit calls from calling bots as most computers will now and in the near future be unable to perform the tasks. SPIT originating from call centres can not be blocked, but as it will take a call centre agent more time to complete the task, it will produce higher costs (connection and salary) for the call centre. This approach can be implemented within the SPIT-AL prototype.

### 2.2.8 Greylists

A greylist is a kind of 'blurred' black- or whitelist. Its behaviour depends on the circumstances of the calls: On first call attempt, the caller will receive a 'line busy' signalling, the phone of the callee will not ring. Only in case the caller is reattempting to reach the subscriber he will get patched through to the subscriber as it is likely that a human is actually interested in talking to the subscriber.

This approach is in risk of calling bots adapting their behaviour. Still they will be limited to fewer calls per time. Greylists could be a component of the SPT-AL prototype.

### 2.2.9 Simulated Conversation

Similar to a voice menu, the caller is presented a human voice. Prerecorded audio files simulate that an actual subscriber has accepted the call.<sup>6</sup> Depending on silence on the line (i.e. the caller is not talking and likely to expect a reply), further audio files with more or less interrelated content will be played.

This concept aims at binding a spammer to a call for a preferably long time without being successful regarding the commercial intent. Resources of the caller get bound and the business model gets less profitable. However, this approach also binds

resources of the subscriber. An implementation within the SPIT-AL prototype is not planned.

### 2.2.10 Honeyphones

The Simulated Conversation approach can also be used to implement honeyphones<sup>7</sup>, i.e. dedicated lines always answering as described above. As the line is not linked to any actual human subscriber, callers are most likely spammers calling random numbers. They can then be added to a central blacklist.

It is still possible that non-spammers accidentally call a honeyphone. Human analysis of recorded conversations might help sorting out such occurrences. An implementation is not planned for the SPIT-AL prototype.

## 3. The SPIT-AL Project and Its Technical Structure

The following technical structure for an implementation of a SPIT countering solution, its features, architecture and the context it can be used in, are a result from the approaches described above.

### 3.1 Basic Functionality

SPIT-AL is accepting calls as a proxy for the called subscriber. According to the meta-data of the call (caller identity, call origin, time if applicable) and the preferences of the subscriber, the call gets rated. An evaluation of the voice stream and therefore of the communication content does not take place as the classification of the call has to happen fast, i.e. before a potential annoyance. Depending on the rating of the call, the system decides which action to take on it.

### 3.2 System Architecture

SPIT-AL should possibly be designed in way that it can be integrated into an existing telecommunication infrastructure. The used devices for linking to PSTN/ISDN and Internet telephony services are not developed within the project. The operator of the telephone system (or the voice switch) at which the calls are terminating, is responsible for directing calls for participating subscribers to the SPIT-AL system first. This way SPIT-AL can be used for different categories of telephony (VoIP, PSTN, or even mobile). Certain functionality such as statistical filtering require a tighter integration into the infrastructure of the operator.

The architecture of SPIT-AL is functionally divided into several subsystems.

The *Application Softswitch* handles routing of calls between the components that implement the various graded actions. The calls of participating subscribers must initially be routed to this system.

<sup>6</sup> A model implementation is the Telecrapper 2000, <http://www.pagerealm.com/tc2k/>

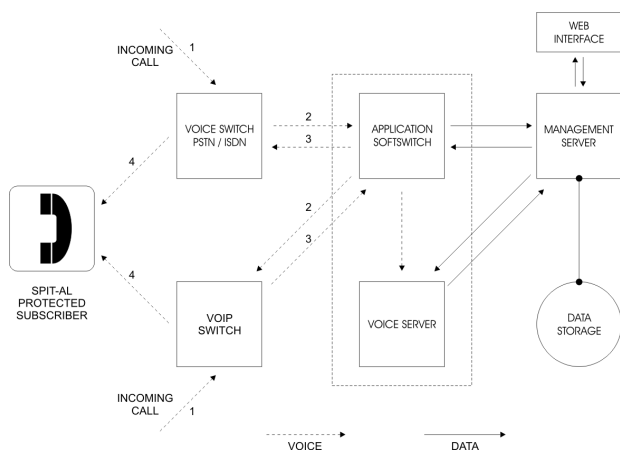
<sup>7</sup> Named in analogy to honeypots and honeynets, c.f. <http://project.honeynet.org/papers/honeynet/>

For the implementation of several possible features within SPIT-AL, the application softswitch gets assistance from a *Voice Server*. The voice server provides for voice boxes, voice menus, or simple announcements.

The application softswitch itself does not make decisions about the routing of calls, but delegates the decisions to a *Management Server*. The management server receives call meta-data from the application softswitch and responds to it with a decision where to route the call. The management server also manages the user-specific configuration data (setting, preferences) and data for the certain mechanisms (see below).

The management server stores all data relevant to the system in a *Data Storage*.

A *Web Interface* enables subscribers to manage his data (personal preferences, white- and blacklists (see below) and voice box content if applicable) via the management server.



As a basis for the application softswitch and the voice server the open source software Asterisk<sup>8</sup> could be used.

The subsystems can be implemented on distributed systems as well as a single computer. This way SPIT-AL can be used by telephony providers as well as an additional service within companies, authorities, or small private networks.

### 3.3 Features and Details of Functionality

Each subscriber and user of SPIT-AL will select his personal preferences using the web interface. The single options will be described in detail later.

The management server calculates a score from the known call meta-data such as caller identity, call origin (PSTN, VoIP, perhaps operator of caller's network), time, etc. The user's preferences mentioned above can influence the assessment. For certain

<sup>8</sup> <http://www.asterisk.org/>

ranges of score points the individual users select an appropriate action. Because of privacy reasons (possibly enforced by law), the users must have complete supervision over all available preferences.

#### 3.3.1 Assessment Criteria

The following presents a list of assessment criteria that influence the rating of calls as SPIT. Some of them will be implemented into SPIT-AL. To calculate the aforementioned score, several criteria will be taken into account by combining the results (e.g., adding or weighting them).

Not all of the presented criteria will be implemented into the SPIT-AL prototype. Within the project, initially the "private whitelist" and "private blacklist" criteria will be implemented.

##### 3.3.1.1 Call Origin

A call can be rated according to its origin. E.g., in case it originates from PSTN, this can lead to a positive rating, as it can be assumed, that calls cause higher costs there and therefore the probability of being SPIT is lower.

Also calls originating from bigger VoIP providers with regulated VoIP infrastructure (e.g., strong user authentication, business terms and conditions outruling advertising calls) could be identified as such and receive a positive rating. In contrast, calls directly originating from dial-in or DSL Internet connections could receive a negative rating.

##### 3.3.1.2 Private Whitelist

Each user of SPIT-AL is maintaining within his preferences a list of known and trusted caller identities. If a caller is on the list with his caller identity, the call gets ranked positively.

##### 3.3.1.3 Imported Whitelists

Each user of SPIT-AL may publish his personal whitelist, the decision gets stored with the preferences. Additionally, he can select from which other users he is willing to receive their published whitelists and how to weight them when importing them into his personal list set. In case the caller identity of an incoming call is not on the personal whitelist, the other (imported) lists are queried. The outcome in combination with the weighting of the imported list results in a rating. This procedure can be conducted recursively. This way, a query gets sent to (trusted) peers and (via a limited number of levels) to peers of peers and so on.<sup>9</sup>

For reasons of privacy it is possible to enhance this feature by one or more central servers where callers

<sup>9</sup> Concept and design of a distributed lists feature as an enhancement to SPIT-AL are subject to a computer science diploma thesis.

have to initially explicitly agree to this transfer of their personal information. Information on users not listed on these servers will not be transferred between peers.

#### **3.3.1.4 Private Blacklist**

Each user of SPIT-AL is maintaining within his preferences a list of known caller identities marked as spammers. If a caller can be matched by the given caller identity, the call gets ranked strongly negative.

#### **3.3.1.5 Imported Blacklists**

Each user of SPIT-AL can select within his personal preferences if he is willing to publish his blacklist. Additionally, he can select from which other (trusted) users he wants to import their published blacklists and how to weight their content. In case the caller identity of an incoming call is not on the personal blacklist, the other (imported) lists are queried, resulting in a weighted rating. This procedure can be conducted recursively. This way, a query gets sent to (trusted) peers and (via a limited number of levels) to peers of peers and so on.

#### **3.3.1.6 Statistical Blacklist**

SPIT-AL can compile statistics regarding a certain caller identification based on the meta-data of all calls routed through it, e.g., caller identifier, called subscriber, time, duration, etc. In case a caller is initiating connections to a high number of subscribers in a short period of time and most of the calls are rather short, it can be assumed that the caller is a spammer. This information can be published in a blacklist that SPIT-AL users can import and weight.

### **3.3.2 Actions**

After the management server has rated the call with a certain rating, the subscriber's preferences get queried for the action to take on it. The following presents several possible actions. Not all of them will be implemented right from the beginning within the SPIT-AL prototype. Within the prototype, the actions 'accept', 'reject', and 'route to third line' will be implemented.

#### **3.3.2.1 Accept**

A call resulting into this action will be routed to the called subscriber directly. The communication will therefore be established without delay in case of a high positive ranking, e.g., because the caller is listed on the subscriber's personal whitelist.

#### **3.3.2.2 Reject**

The caller will receive a ringing signal (or a line not available or busy signal), but the telephone of the called subscriber will not ring. In case of a strong negative rating, e.g., as a result from the caller being listed on the personal blacklist, the caller will never

reach the subscriber and can also never conclude on his actual reachability.

#### **3.3.2.3 Route to Third Line**

The call gets routed to a third line defined by the called subscriber within his SPIT-AL preferences. There the subscriber can operate an answering machine or implement further mechanisms.

#### **3.3.2.4 Reject Temporarily / Greylisting**

The caller will receive a 'busy' signal. In case he is calling again within a short period of time, he will be routed to the subscriber. In case he is calling again within a longer period of time, another action is taken.

#### **3.3.2.5 Announcement of Alternative Reachability**

The call gets routed to the voice server, where the caller can receive a prerecorded message explaining how he can contact the subscriber, e.g., by a more cost-intensive PSTN line.

#### **3.3.2.6 Voice Menu**

The call gets routed to the voice server, where the caller is confronted with a voice menu, where he has to listen to a (perhaps longer) announcement and then to perform a task, e.g., press a certain sequence of digits on his phone keyboard. After passing the test, he gets routed to the subscriber or a voice box (see below) according to the subscriber's preferences.

#### **3.3.2.7 Voice Box**

The call gets routed to the voice server where the caller can leave a message for the subscriber on a voice box. If required by the subscriber's preferences, a task has to be performed beforehand (see above).

### **3.3.3 Further Features**

To allow subscribers to use SPIT-AL as easily as possible, further features for an implementation are possible.

#### **3.3.3.1 Adding Called Communication Partners Automatically to Personal Whitelist**

In case a subscriber is directly calling another party, the caller identity of the called party can be added to the subscriber's personal whitelist as it can be assumed that he is willing to also accept calls from that party, too.

#### **3.3.3.2 Logging of Connection and Decision Data**

In case a user of SPIT-AL receives a call, connection data such as time and caller identity as well as the score calculated by the management server (together with a short description how the score was calculated) will be written to a logfile (or database).

Via the web interface where a user maintains his personal white- and blacklists, the user can review the

connection and decision log and mark callers as spammers or peers with a single mouse click, adding them to his black- or whitelist.

### 3.3.3.3 Marking Proceeding Calls Using Dialtones

In case a subscriber is talking to a communication partner via telephone, he can add the communication partner to his white- or blacklist by typing certain sequences of digits on his telephone keyboard.

## 3.4 Basic Technical Problems

### 3.4.1 Suppression of Identity

Telephony is required by law<sup>10</sup> to have the feature to suppress the caller's identity. Mechanisms to protect the caller's privacy also in Internet telephony are currently in development [10][14].

The called subscriber is then unable to detect the caller's identity or conclude from it whether he wants to accept the call or not. This significantly reduces the efficiency of white- or blacklists.

### 3.4.2 Identity Verification

Using Internet telephony, as of today it is fairly easy to forge a certain caller identity, as no authoritative and binding standards on end-to-end identity verification and caller authentication exist. While there are mechanisms for inter-domain authenticated identity, they are rather seldomly used and it remains cheap to obtain a nearly infinite supply of addresses [13].

## 4. Legal Aspects<sup>11</sup>

Filtering telephone calls as described above raises a lot of legal questions that have to be taken into account when designing a technical solution against unwanted telephone calls. As SPIT-AL is developed in Germany, the following overview is based on German law. Similar regulation should apply at least within the European Union [5]. A more detailed analysis focusing on German regulation can be found within the SPIT-AL white paper, while this article covers basic principles.

### 4.1 Legal Foundations

Various legal norms from several fields of law can take regulating effect on processes to be used within the context of SPIT filtering such as constitutional law, data protection law, telecommunication law, teleservices law, criminal law, and possibly administrative law [3][6]. Different types of users,

<sup>10</sup> At least in Europe, Art. 8 Dir. 2002/58/EC (European Data Protection Directive).

<sup>11</sup> For the first drafts of the SPIT-AL white paper, a basic legal analysis has been conducted. During further conceptualisation of the prototype a more in-depth analysis will follow.

e.g., individuals, companies, or administrations, will face slightly different legal positions regarding details due to different applicable regulation, whereas other more fundamental principles will be the same in all cases. As an example, an analysis of call content would breach secrecy of telecommunications and be sanctioned by up to five years in prison according to German telecommunication and criminal law.

## 4.2 Main Legal Requirements

### 4.2.1 User-Controlled Filtering

For reasons of constitutional, data protection, and telecommunication law, it is mandatory to pass full control of the if and how of a SPIT filter into the subscriber's hands, as this minimises legal problems regarding secrecy of telecommunications and privacy in cases of private use of the filter. This way, the subscriber's rights of unobserved telecommunication and privacy protection lies within the best hands – his own.

The complexity of the concepts designed within the SPIT-AL project as an effect will unfold problems regarding practical use as well as the ability to secure and exercise own rights and interests. Therefore the precautions listed below can be of help.

### 4.2.2 Transparency and Control of Data Processing

Subscribers have to be explained the single mechanisms of identification, classification, and treatment of incoming calls. This should enable them to take note of SPIT-AL's basic functionality as well as the underlying database and the purpose of data transfer.

In case of transfers of personal data belonging to third parties from within a subscriber's sphere, it is mandatory to inform the affected persons about purpose, further use, and possibilities to exercise users' rights. A central infrastructure for giving (or withdrawing) consent or objecting as well as an enforcing mechanism for SPIT-AL could help securing the rights of data subjects<sup>12</sup>.

As a matter of principle, each mechanism has to be explicitly activated by the subscriber as this requires at least a minimum notice of basic paradigms.

### 4.2.3 Presets for Different User Types

In order to facilitate the process of configuration and to direct use into a principally legal direction, different presets for certain types of users are a practical option. The presets have to be activated on initial use and can be changed thereafter if desired.

Due to different legal positions for individuals, companies, and administrations, it seems reasonable to

<sup>12</sup> Person whose data is being processed, Art. 2 Dir. 2002/58/EC, Art. 2 a) Dir. 95/46/EC.

establish three presets for the SPIT-AL prototype. They differ from each other especially in the combinations of applicable mechanisms for identification, classification, and treatment of incoming calls. In addition, a user-focused documentation of the configuration has to point out the specific characteristics of the user types.

## 5. Conclusion

This article explained that SPIT filtering mechanisms will be required in the future. As they have to take effect before a call is accepted and therefore can therefore not rely on content analysis (as opposed to e-mail spam), in SPIT-AL, caller identity will be matched against white- and blacklists within a distributed environment, a peer-to-peer web of trust. In addition, information from further meta-data and statistical analysis might be used. According to the classification of a call and the subscriber's preferences, different approaches to treat the call are possible, e.g., 'accept', 'reject', 'redirect to voice box', 'point to alternative reachability', etc. Computer-generated SPIT can be filtered by adding mechanisms requiring caller interaction such as a voice menu.

For a legal overview, different fields of German law have been taken into account, especially telecommunication and data protection law, but also teleservices, criminal, and administrative law. The realisation of white- and blacklists with a focus transparency and user control is of high importance. This also addresses the approach of distributing and importing lists to and from third parties.

The concept favoured by the SPIT-AL project contains central as well as decentral (implemented at certain users) components. The approaches discussed will be further refined as the project progresses. The SPIT-AL open source prototype will cover basic functionality of a legally compliant reachability management system as a countermeasure against SPIT. Further functionality will be added later.

## 6. References

- [1] Bundesamt für Sicherheit in der Informationstechnik: VoIPSEC – Studie zur Sicherheit von Voice over Internet Protocol, October 2005, <http://www.bsi.de/literat/studien/VoIP/>
- [2] Bundesnetzagentur: Anhörung zu Voice over IP (VoIP) – Themenweise Auswertung der Anhörung zu Voice over IP, October 2005, <http://www.bundesnetzagentur.de/media/archive/3173.pdf>
- [3] Bundesnetzagentur: Eckpunkte der regulatorischen Behandlung von Voice over IP (VoIP), 9 September 2005, <http://www.bundesnetzagentur.de/media/archive/3186.pdf>
- [4] Center for Democracy & Technology: Spam 2005: Technology, Law and Policy, Washington D.C., March 2005, <http://www.cdt.org/speech/spam/spam2005/>
- [5] Commission of the European Union: Commission Staff Working Document: The treatment of Voice over Internet Protocol (VoIP) under the EU Regulatory Framework, 14 June 2004, [http://europa.eu.int/information\\_society/policy/ecom/doc/info\\_centre/commiss\\_serv\\_doc/406\\_14\\_voip\\_consult\\_aper\\_v2\\_1.pdf](http://europa.eu.int/information_society/policy/ecom/doc/info_centre/commiss_serv_doc/406_14_voip_consult_aper_v2_1.pdf)
- [6] 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Entschließung Telefonieren mit Internettechnologie (Voice over IP – VoIP), 28. Oktober 2005, [http://www.datenschutzzentrum.de/material/themen/press\\_e/20051028-dsbk-voip.htm](http://www.datenschutzzentrum.de/material/themen/press_e/20051028-dsbk-voip.htm)
- [7] Herbert Damker, Kai Rannenberg, Günter Müller: Erreichbarkeitsmanagement und mehrseitige Sicherheit aus Benutzersicht, Fachvorträge auf dem 4. Deutschen IT-Sicherheitskongress des Bundesamtes für Sicherheit in der Informationstechnik, Bonn, May 1995, <http://www.wiiw.de/publikationen/Erreichbarkeitsmanagementundme.pdf>
- [8] Tobias Mahler, Thomas Olsen: Reputation Systems and Data Protection Law, Paul Cunningham, Miriam Cunningham (eds), eAdoption and the Knowledge Economy: Issues, Applications, Case Studies, IOS Press 2004, p. 180-188, <http://www.afin.uio.no/forskning/notater/Reputation%20Systems%20and%20Data%20Protection%20Law.pdf>
- [9] Stanley Milgram: The Small World Problem, Psychology Today, Mai 1967, p. 60-67
- [10] Jon Peterson: A Privacy Mechanism for the Session Initiation Protocol (SIP), RFC 3323, November 2002, <http://www.jdrosen.net/papers/rfc3323.txt>
- [11] R. Pierce Reid: Voice Spam Spam, Spamity Spam – White Paper, July 2004, [http://www.qovia.com/resources/pdfs/white%20papers/qovia\\_spit\\_wpaper.doc](http://www.qovia.com/resources/pdfs/white%20papers/qovia_spit_wpaper.doc)
- [12] Thomas Rohwer, Carsten Tolkmit, Markus Hansen, Marit Hansen, Jan Möller, Henning Waack: White Paper: Abwehr von "Spam over Internet Telephony" (SPIT-AL), March 2006, [http://www.spit-filter.com/Whitepaper\\_SPITAL\\_20060310.pdf](http://www.spit-filter.com/Whitepaper_SPITAL_20060310.pdf)
- [13] Jonathan Rosenberg, Cullen Jennings, Jon Peterson: The Session Initiation Protocol (SIP) and Spam, draft-ietf-sipping-spam-01, SIPPING Internet-Draft, 17 July 2005, <http://www.ietf.org/internet-drafts/draft-ietf-sipping-spam-02.txt>
- [14] Jonathan Rosenberg, Cullen Jennings, Jon Peterson: Identity Privacy in the Session Initiation Protocol (SIP), draft-rosenberg-sip-identity-privacy-00, SIP Internet-Draft, 11 July 2005, <http://www.ietf.org/internet-drafts/draft-rosenberg-sip-identity-privacy-00.txt>