

Facilitating the Adoption of Tor by Focusing on a Promising Target Group

Heiko Roßnagel¹, Jan Zibuschka¹, Lexi Pimenides², Thomas Deselaers²

¹Fraunhofer Institute for Industrial Engineering (IAO),
Nobelstr. 12,
70569 Stuttgart, Germany

²Computer Science Department,
RWTH Aachen University,
Aachen, Germany

Heiko.Rossnagel@iao.fraunhofer.de
Jan.Zibuschka@iao.fraunhofer.de
lexi@pimenidis.org
deselaers@vision.ee.ethz.ch

Abstract. The technology for anonymous communication has been thoroughly researched. But despite the existence of several protection services, a business model for anonymous web surfing has not emerged as of today. One possibility to stimulate adoption is to facilitate it in a specific subnet. The idea is to identify a promising target group which has a substantial benefit from adopting the technology and to facilitate the adoption within that target group. We examine the feasibility of this approach for anonymity services. We identify a potential target group – consumers of pornographic online material – and empirically validate their suitability by conducting a traffic analysis. We also discuss several business models for anonymity services. We argue that providers of anonymity services should try to generate revenue from content providers like adult entertainment distributors. The latter could benefit from offering anonymous access to their products by differentiating against competitors or by selling their products at a higher price over the anonymous channel.

Keywords: Adoption, privacy, business models, anonymity services.

1 Introduction

Since Chaum proposed a method for anonymous and unobservable delivery of electronic messages [16] technologies for anonymous communication have been thoroughly researched. The concept has been adapted to internet data traffic [38], ISDN call routing [37] or mobile technology [24].

Despite their excessive needs for computational power and bandwidth, several protection services that provide anonymous communications such as Tor [21] or

AN.ON [9] are offered without financial charges. However, the deployment of such technology and services has not yet reached the mass market of end users. So far only a small fraction of users are using these privacy enhancing technologies (PET) [33] and early adopters, which are necessary to reach a critical mass of adopters, have not been attracted [26]. Consequently, there is no beneficial market today for providers of anonymization services.

Also, evidence has been provided that users of anonymity services have a low willingness to pay for these services [46]. Consequently, no working business model for anonymity services has been developed so far.

While it may be argued that the intrinsic motivation of node operators to communicate anonymously themselves is enough to keep the network up and running in its initial phases, it may be doubted that the growth might continue without proper remuneration. This problem is currently seen and discussed in the Tor network [34].

In [41] several possibilities to stimulate the adoption of anonymity services have been discussed, ranging from information provisioning about the risks of unprotected online access to very invasive methods like mandatory adoption.

While most of these possibilities have to be undertaken by policy makers, some of them (i.e. bundling with complementary goods) can be applied by vendors of privacy enhancing products. One such approach is to facilitate the adoption in a specific subnet. The idea is to identify a promising target group which has a substantial benefit from adopting the technology and to facilitate the adoption within that target group. If this group is large enough, demographically spread and well coordinated this could lead to natural adoption [36]. Anonymity services could therefore be selectively offered to users of services which have a more obvious demand for anonymity and a high willingness to pay for them [41].

In this contribution we examine the feasibility of this approach. We first identify a potential target group – consumers of pornographic online material – and then empirically validate their suitability for facilitating adoption of anonymity services, by conducting a traffic analysis. We also discuss different business models and possible approaches for revenue generation.

2 Related Work

In recent years there has been a growing body of research on the economics of privacy and privacy enhancing technologies. Most of the work is concerned with the determination or measurement of the value of privacy for individuals [47]. Huberman et al. [30] used reverse-prize auctions to identify the monetary value of private information to individuals. Their results show that a trait's desirability in relation to the group impacts the amount people demand for revealing this information. For example individuals weighing slightly below average required little compensation to publicize this fact. In contrast, those who weighed more and might therefore fear embarrassment or stigmatization demanded relatively high compensation [30].

Other studies examined the circumstances under which users are willing to disclose private information [3] [1] [8]. Their results show that individuals who genuinely would like to protect their privacy may not do so because of psychological distortions

such as hyperbolic discounting, under insurance, self-control problems and immediate gratification [3] [1]. This demonstrates discrepancies between attitudes towards privacy and actual behaviour [8].

The results of [7] show that perceptions of a web merchant's trustworthiness can be high even when privacy and security features are weak. As a possible explanation for this result they suggest that the respondents may have lacked familiarity with or understanding of the seals and statements.

In more market oriented research, Acquisti argues that the market of privacy conscious individuals willing to pay for their protection is small and therefore will not be satisfied [2]. He attributes the small market size to the low amount of people who are conscious of their security needs [1] and willing to pay for it. Furthermore, he claims that "while actual usage costs of privacy enhancing technologies are low once adopted, their adoption fees are high because they involve significant switching costs" [2]. Shostack [43] argues that when privacy protection is offered in a clear comprehensible way it does sell well. He supports this argument with several examples such as draperies and curtains. Accordingly he concludes that complex technologies that protect against nebulous threats will not sell well. Feigenbaum et al. [26] attribute the missing adoption of privacy-technology to economic factors like network externalities, asymmetric information, and moral hazard.

The willingness of users to pay for anonymization services has been researched in [45] and [46], in which the results of a survey of over 5000 users of the AN.ON privacy service were presented. When asked about their willingness to pay for anonymity services, 40% of the participants – all of them already users of an anonymity service – were not willing to pay anything at all. Approximately 50% were willing to pay between €2.50 and €5.00 per month while 10% would have paid more than €5.00.

There have also been observatory approaches, relying on the classification of logged traffic into several categories [25]. However, these results seem to be somewhat contradictory, concerning both background of usage (with self-reports overstating professional use compared with the measurement/categorization approach) and use cases (understating pornographic material). While this discrepancy may be explained with the well-documented bias of people to overstate their privacy sensitivity [3] [47] or the generally weak validity of self-report studies in the context of sexuality [10], to our knowledge, the publications based on direct measurements of Tor traffic do not describe a clear methodology that would allow us to retrace how the results were obtained. To overcome these restrictions of the available material, we decided to do a new analysis for this paper, with a clearly documented methodology described in Section 4.

3 Identifying Potential Target Group

In order to facilitate adoption of anonymity services in a subnet, a promising target group has to be identified. Ideally, members of this target group should have a high demand for anonymity and a high level of innovativeness. Furthermore, since the

focus is on commercial anonymity services, users should also have a high willingness to pay for anonymity services or associated products and services.

One such target group could be consumers of pornographic online material. Obviously they have a high demand for anonymity [19]. For example, the German video on demand service provider videoload.de is running a commercial in which the absence of embarrassing moments (i.e. when returning pornographic tapes) is advertised as one of the key features of their service¹ [50].

Also, users of pornographic material have shown a high level of innovativeness in the past [18]. Adult-oriented content has been reported as a main driver for the establishment of several wide-spread technologies and infrastructures, such as VCRs, DVDs, computers, or the internet itself [19] [18]. Even the success of VHS over the Betamax VCR standard, has been attributed to pornography [5]. In addition, consumers of pornography have shown a high willingness to pay in the past [18] [4].

Furthermore, the market for pornographic material is quite substantial. In Italy alone, the turnover deriving from selling or renting pornographic movies to the final users is about 224,000,000 € [23]. Globally, pornography generated a turnover of over 97 Billion Dollar in 2006 with over 2.8 Billion Dollars coming from internet pornography [48].

Also, it is notable that users are obviously consuming a large amount of multimedia content over the Tor network, in spite of its reported sluggishness [22]. So, while fast response times are a big factor when browsing web sites [29], for larger multimedia content, this factor seems less deterring, especially in the case of adult entertainment.

Looking at the numbers given in [25], it is quite obvious that this is a promising use case for web anonymizers. However, tapping into the potential of the pornography market should be done very cautiously, as mixing adult content and mainstream media is not acceptable in many cultures [32] [6]. So, to be successful in this context, the service needs to be carefully aimed at the proper audience, and make sure not to mix the mainstream and adult-oriented contexts.

If consumers of pornographic online material have a higher demand for anonymity and a higher level of innovativeness than regular internet users, the percentage of user's accessing pornographic material should be higher within the Tor Network than on the internet. This should also be visible in the percentage of pornographic material within the data traffic transferred over these networks. Therefore, we formulate a research hypothesis:

H1: *Traffic transferred over the Tor Network contains more pornographic material than regular internet traffic.*

4 Research Methodology

In order to test our hypothesis we analysed the output² of a Tor exit node and compared these results to those of an outgoing proxy of a German university. The

¹ Please note, however, that videoload.de does not provide anonymous access to their services.

² Due to the nature of Tor, plain HTTP requests and their responses can only be seen when leaving the network; their origin is, however, untraceable.

choice of a university proxy as a control group to Tor was based on the fact that we were unable to get a more representative data set from an internet service provider (ISP), because the data we would have needed is usually not recorded. Similarly, we investigated a single Tor exit node as a representative of the entire network, as such data is not recorded by many exit nodes. We hold that our data is of interest as traffic statistics of this granularity are usually not publicly available.

We restricted our analysis to HTTP traffic for several reasons. HTTP is, after Peer to Peer (P2P), the second largest traffic class [42]. While P2P traffic comprises a significant amount of data traffic, its analysis is tedious as the content is often transferred in chunks and from different hosts. This makes an analysis of the type of transferred data very difficult, if not impossible. Also, the ratio of the transferred bytes per connection suggests that P2P is mostly used for videos rather than still pictures [33].

Furthermore, HTTP has a long tradition of scientific analysis and there are well known methods for analysing HTTP traffic in a privacy-preserving way. In order to stick to lawful research³ we used the following method of data acquisition and analysis, which was developed together with data protection officers. First, we collected a set of URLs which have been requested by users over either Tor or the university's proxy. We did not save any information except the requested URL itself; this includes any additional header information like Cookies, etc. Requests sent with methods other than GET, e.g. POST requests, or any requests containing GET-variables, were completely left out of the analysis. We also blurred the time stamp of a request to store only the year and the month and then reordered the requests per month so to hide any information about the order of requests and also thwart guesses narrowing down the date of a request within a month. In the case of Tor, we also could not collect the source IP of the request by definition, in the case of the university's proxy we asked the proxy's administrator specifically not to copy the IPs, even if they were recorded. All of this was done automatically and any data not of interest was already discarded at this stage. Then, more people were involved to select a subset of the URLs. These were polled by a program and the content was dispatched without these helpers being able to store it. Finally, the content was analysed by people not knowing its source. This procedure ensured that the researchers for the actual analysis did not have access to the original data, whereas the others did not know the content of the URLs⁴.

In order to reliably classify the type of content we had to inspect the type of the actually transferred data. This holds true as especially in the case of free image web hosting it is not possible to learn the type of the image by the URL's pattern alone. To make sure, we retrieved 7,000 images from each of the sets of URLs with the procedure described above. To rule out that the results would be drowning in a vast amount of small pictures that are used as icons or frame borders in web pages, we limited the search to images with a size of larger than 10,000 bytes.

³ The authors of the aforementioned [33] were threatened to be legally prosecuted due to their methodology.

⁴ Also note that this procedure preserved picture owner's privacy which use any kind of authentication mechanism to prevent access to their pictures.

We then used a set of pattern matching techniques described in [20], to classify the images into five categories:

- Class 0 definitely inoffensive images
- Class 1 lightly dressed persons
- Class 2 partly nude persons
- Class 3 nude persons
- Class 4 pornographic, i.e. one or more persons engaging in sexual intercourse

In order to minimize the error of the classification process, we used the automated classification method for a preliminary result, as the pictures extracted from the URL streams were too diverse in order to produce acceptable results in the first run: the overall correct classification rate was 33% in the case of the pictures coming from Tor and 44% for the pictures from the university's proxy. The classification ratio was raised to 70%, resp. 75% if a deviation of one class was deemed an acceptable error.

5 Empirical Results

The input of the automated classification was enhanced in a manual process of re-classification. Due to time constraints and data protection concerns we only used a random sample of 1,000 images from each set for a final manual classification. The results of our analysis are listed in Table 1. Content categorized by image recognition technique

	Class 0	Class 1	Class 2	Class 3	Class 4
Tor	28%	15%	15%	14%	28%
Plain	66%	7%	8%	8%	11%

Table 1. Content categorized by image recognition technique

Our results show that the Tor network has a much higher percentage of sexually oriented material than normal traffic: 72% of the pictures in the Tor network and 34% in normal traffic were classified in Class 1 to Class 4. Even if material from “Class 1”, which can be encountered in everyday's advertising in most western countries, is not counted, the percentage remains substantially higher for the Tor network (57% vs. 27%). While the percentages for the Classes 1-3 are about twice as high for Tor traffic, this difference spreads even further for Class 4 (28% vs. 11%).

To test our hypothesis, we used a χ^2 -test to check if both the differences between these distributions are due to statistical fluctuation or whether they differ significantly. The test clearly shows that the distributions differ significantly with $p < 0.0001$. We also used the one-sided Wilcoxon Rank Sum test to check whether the traffic from Tor contains significantly more pornographic material than plain traffic. The obtained result confirmed our hypothesis with $p < 2.2 * 10^{-16}$, which means that the Tor traffic *does* contain a significant higher percentage of adult traffic.

This correlates with results of related work that activities related to sexual behaviour are very privacy sensitive and therefore subject to privacy protection techniques [49].

6 Business Models

Having identified a potential target group in which to facilitate adoption and shown its presence in the targeted medium, we present possible business models and analyse their motivation, restrictions, and opportunities.

6.1 User side revenue generation

The only approach that has been applied so far is to directly offer anonymity services to potential users. In this scenario the users have to install software on their computers in order to anonymize the traffic. Examples of this approach are JonDoFox [31], which combines Firefox with Jondos, a commercial spin-off of the AN.ON project and the XeroBank Browser [44], which is a modification of the popular Firefox browser, readily compiled with a client for the Tor network.

This approach has not been successful even for services that are free of charge [41]. Potential adopters are neither aware of the privacy risks they face when communicating online nor of the available technology to protect themselves against these risks [41]. Also, these PETs are preventive innovations, which are ideas that are adopted by an individual at one point in time in order to lower the probability that some future unwanted event will occur [40]. Preventive innovations usually have a very slow rate of adoption, because the unwanted event might not happen even without the adoption of the innovation. Therefore, the relative advantage is not very clear cut [40]. Furthermore, users of anonymity services have been shown to have a small willingness to pay in the past [46].

Due to the complexity and missing user-friendliness of current anonymity solutions, users also endure a large amount of search costs in order to setup the software correctly at their side. The technical problems include possible information leakages due to DNS [21], browser plugins [27], or plain configuration faults at the installation [21] [9]. It is widely agreed that the correct installation and usage of local proxies and related browser configuration is often too hard to be properly carried out by users [17].

Some of these problems, like for example the willingness to pay, might be reduced if consumers of pornographic material are specifically targeted. Nevertheless, a success of this model remains rather doubtful.

6.2 Advertising at the exit node

The second possibility that we discuss is the generation of additional revenue by implementing advertising at the exit node. This is the last node of the anonymity network, where the user's traffic leaves the network and is finally redirected to its

destination. This fact makes the operator of the last node one of the most vulnerable parts in the setup of any overlay network. If a request which is forwarded out of the network contains or requests any malicious content, it is this operator that is made responsible for this in the first place. For this reason, only a minority of node operators are actually allowing traffic to exit through their nodes out of the overlay network. Due to this fact, it is critical for any network to have an appropriate number of exit nodes. Therefore, it can be argued that remunerating these operators more than others, or even remunerating only exit node operators, can be accepted from an ethical or fairness point of view. Additionally, a solution propagating the revenues from the exit node back across the anonymization network may be implemented, so the discussion of the exit nodes may serve as a basis for progress in recuperation of other nodes.

In contradiction to the wide-spread, but wrong, believe of average users that all traffic through anonymity networks cannot be seen by any third parties, the content of the actual request is plainly visible to the exit node. Thus, the exit node operator can deploy a software component to rewrite the user's request as well as the related content before forwarding them to their respective targets. Rewriting can include the following parts:

- (1) The node operator may replace existing advertisements in web pages with advertisements where the exit node operator profits from possible click rates or sells. Although the exit node operator can replace arbitrary content, for an economical gain, it would be sufficient to replace ads, advertisement, and banners in the transferred pages. With this technique, the exit node operators could profit from the flow of traffic through their node: if they replace a certain amount of advertisement with a set of links to their customers, they get remunerated for their services.
- (2) Another rather aggressive way would be to redirect users sending queries to search engines directly to partner sides of the exit node operator, or just reorder the search engine's result.
- (3) Finally, the exit node operator is capable to inject small pieces of Javascript into an HTML page in order to trigger loading of pop-up windows. As we personally feel that pop-ups are becoming a growing annoyance, we would not recommend this technique and only list it for completeness purposes.

It can be said with some confidence that such a system should be able to recover costs of operation. Assuming a cost per Gigabyte of about US\$0.20, an average click rate on web advertisement of around 2 to 3 per thousand advertisements [14], and a financial gain of US\$0.01 per click, there should be at least 20 clicks per Gigabyte, i.e. 8,000 advertisement displacements.

This means that if an exit node operator owns one banner per 131 Kilobyte of traffic, he can do a break-even. As has been shown in [39], the size of an average HTML-page is 5 Kilobyte. Even if we multiply it by a safety factor of 10, resulting in an average HTML-page size of 50 Kilobyte, it would be sufficient for an exit node operator to only insert or replace an advertisement in about every third page.

Some of these methods presented here may face legal problems in some jurisdictions, because they are defrauding the content providers, owners of the underlying web sites, e.g. based on intellectual property regulation. Besides legal risks, the exit node operators also face a second problem: the Tor community itself is

known to be highly critical of any kind of content modification by the exit node operators. If a certain node starts to actively replace content in the relayed data streams, it might face exclusion from the Tor network.

So, while the numbers add up for this method, it faces serious legal problems, and motivates investigation of business models involving the service and content providers in a more prudent fashion.

6.3 Revenue generation from content providers

Another possible approach is revenue generation at the content providers whose products the users consume over the anonymization network. There may be several motivations of revenue generation in this context:

- (1) The content provider may be able to charge his users a premium for services and products offered to them anonymously, which should result in an additional payoff if a willingness to pay for privacy exists on the user side [12].
- (2) The content provider may have a willingness to make payments assuring the continuous operation of a third party anonymization network, if it is used by a large set of his customers in conjunction with its services.
- (3) Providing anonymous access to its products could enable the content provider to differentiate itself against competitors.

As our traffic analysis has shown, a suitably large number of users are consuming online pornography. So, adult content providers seem to be operating in a niche market where an increased user's need for privacy exists. Given that these user preferences translate into an increased willingness to pay (a sensible assumption, given that the public Tor network we investigated has significant performance issues [22]), an investment of Tor service providers should result in an ability to price their products at a premium. Böhme and Koble [12] point out that this assumption about privacy-enhancing technologies holds under a broad set of assumptions. The results of [4] show that especially non-Internet savvy individuals whose time is valuable are willing to pay for online pornography in order to avoid hidden costs (e.g. search costs or the risk of virus infection).

This suggests a business model in which adult service providers cooperate with a subset of nodes in an anonymization network, resulting in their ability to offer anonymized services. This subset of nodes may consist of Tor exit nodes, assuring recompensation for their increased exposure, or coordinated MIX cascades, which may be able to offer special services like increased performance to the customers of the service provider. This may also be possible using Tor, however, and both systems have their strengths and weaknesses [11]. However, for demonstrating the technological viability of this business model, cooperation with a commercial anonymization cascade operator seems like the more traceable choice.

There are several possibilities for the implementation of such a system. A solution that blocks all incoming traffic except the one from a certain set of anonymization exit nodes has been proposed in [28]. Also, systems, that implement full client-side anonymisation (including e.g. a streaming media player with built-in anonymization), or full server-based anonymization are both viable for executing this business model.

As can be seen in comparison with the business models discussed in the previous sections, this offers several key advantages. It is easy to operate this system in a lawful way for both node operators and end users. Service providers can realize additional revenue streams by leveraging their users' willingness to pay for privacy.

However, to make this business model work, it is necessary for anonymization node operators to establish relations with potentially interested content providers. Using the results of our earlier traffic analysis, we have identified adult entertainment as a viable application field.

One essential prerequisite for implementing this business model is the establishment of a working model for anonymous payment at the content provider. Anonymous payment can be achieved by using highly sophisticated cryptographic solutions such as [15] or [13]. However, these payment systems have not been applied in real business scenarios so far and exist mainly as research prototypes. Also their chances of success have been questioned [35]. An alternative solution would be the use of pre-paid cards, such as calling cards or anonymous pre-paid SIM cards. Another possibility would be to accept cash payments sent with regular mail on behalf of specific pseudonymous user accounts, which is one of the methods used by JonDos [31].

7 Limitations

We have shown that the percentage of pornographic material is higher in the Tor-Network than in plain Internet traffic, and we concluded that the consumers of that material have a higher demand for anonymity services. However, a higher willingness of these consumers to pay for anonymous access to online pornography has not been empirically validated. We encourage future research in that direction.

For anonymity service provider to successfully generate revenue from adult content providers, a working method of anonymous payment has to be established. So far such a method is missing. We have only sketched several possible approaches. Furthermore, a cost-benefit analysis for content provider should be performed in the future, in order to support our argument of the feasibility of that approach.

8 Conclusion

While the technology for anonymous communication has been thoroughly researched and despite the existence of several protection services, a business model for anonymous web surfing has not emerged as of yet. So far only innovators are using privacy enhancing technology and early adopters, which are necessary to reach a critical mass of adopters, have not been attracted. Therefore, there is no beneficial market today for providers of anonymity services. With our contribution we tried to bridge this gap. In order to find a suitable target group for anonymity services we conducted a traffic analysis. Our results show that there is a significant demand for anonymous access to pornographic material. Furthermore, the users of pornographic material have shown a high level of innovativeness and a high willingness to pay in

the past and have been drivers of technological innovation. Therefore, it seems to be the logical choice to target this specific customer group for the deployment of anonymous services. We then examined the different possibilities to generate revenue for such anonymous services. We concluded that business models that create revenue by directly offering anonymity service to users have failed in the past. Models that aim at creating revenue by inserting advertisements of third parties into the traffic at the exit node might be profitable but face serious legal problems. Finally, we argued that the most promising approach is to generate revenue from content providers like adult entertainment distributors. The latter could benefit from offering anonymous access to their products by differentiating against competitors or by selling their products at a higher price over the anonymous channel.

References

- [1] Acquisti, A., Grossklags, J.: Privacy and Rationality in Individual Decision Making, *IEEE Security & Privacy*, 3, (1), 26-33 (2005).
- [2] Acquisti, A.: Privacy and Security of Personal Information: Economic Incentive and Technological Solutions, in: Camp, J., Lewis, R. (eds.), *The Economics of Information Security*, pp. 1-9, Kluwer (2004).
- [3] Acquisti, A.: Privacy in Electronic Commerce and the Economics of Immediate Gratification, *Proceedings of the EC04, ACM, New York, New York* (2004).
- [4] Ang, E.X.Y., Kwan, J.W.Y., Teo, J., Chua, C.E.H.: Why Do People Pay for Information Goods?: A Study of the Online Porn Industry, *Proceedings of the Twelfth Americas Conference on Information Systems (AMCIS 06)*, pp. 73-77, AIS, Acapulco, Mexico (2006).
- [5] Angell, I.O.: Ethics and Morality: a business opportunity for the Amoral? *Journal of Information System Security*, 3, (1), 3-18 (2007).
- [6] Bazak, A., King, S.A.: The Two Faces of the Internet: Introduction to the Special Issue on the Internet and Sexuality, *CyberPsychology & Behavior*, 3, (4), 517-520 (2000).
- [7] Belanger, F., Hiller, J.S., Smith, W.J.: Trustworthiness in electronic commerce: the role of privacy, security, and site attributes, *Journal of Strategic Information Systems*, (11), 245-270 (2002).
- [8] Berendt, B., Günther, O., Spiekermann, S.: Privacy in E-Commerce: Stated Preferences vs. Actual Behavior, *Communications of the ACM*, 48, (4), 101-106 (2005).
- [9] Berthold, O., Federrath, H., Köpsell, S.: Web MIXes: A system for anonymous and unobservable Internet access, in: Federrath, H. (eds.), *Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability*, pp. 115-129, Springer, Berlin Heidelberg (2000).
- [10] Brener, N.D., Billy, J.O.G., Grady, W.R.: Assessment of Factors Affecting the Validity of Self-Reported Health-Risk Behavior Among Adolescents: Evidence From the Scientific Literature, *Journal of Adolescent Health*, 33, 436-457 (2003).
- [11] Böhme, R., Danezis, G., Díaz, C., Köpsell, S., Pfitzmann, A.: Mix Cascades vs. Peer-to-Peer: Is One Concept Superior, *Privacy Enhancing Technologies (PET 2004)*, pp. 243-255 (2004).
- [12] Böhme, R., Koble, S.: Pricing Strategies in Electronic Marketplaces with Privacy-Enhancing Technologies, *Wirtschaftsinformatik*, 49, (1), 16-25 (2007).
- [13] Camenisch, J., Piveteau, J., Stadler, M.: An Efficient Fair Payment System, *Proceedings of the 3rd ACM Conference on Computer and Communication Security (CCS 96)*, New Dehli, India (1996).
- [14] Chatterjee, P., Hoffman, D.L., Novak, T.P.: Modeling the clickstream: Implications for web-based advertising efforts, *Marketing Science*, 12, (4), 520-541 (2003).

- [15] Chaum, D.: Blind Signatures for Untraceable Payments, *Crypto* 82, pp. 199-203, Plenum, New York (1983).
- [16] Chaum, D.L.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, *Communications of the ACM*, 24, (2), 84-88 (1981).
- [17] Clark, J., Van Oorschot, P.C., Adams, C.: Usability of anonymous web browsing: an examination of tor interfaces and deployability, *Proceedings of the 3rd symposium on Usable privacy and security (SOUPS 2007)*, pp. 41-51, New York, NY (2007).
- [18] Coopersmith, J.: Pornography, *Technology and Progress, ICON*, 4, 94-125 (1998).
- [19] Cronin, B., Davenport, E.: E-rogenous Zones: Positioning Pornography in the digital Economy, *The Information Society*, 17, (1) (2001).
- [20] Deselaers, T., Keyers, D., Ney, H.: Discriminative Training for Object Recognition using Image Patches, *Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2005)*, pp. 157-162, San Diego, CA, USA (2005).
- [21] Dingledine, R., Mathewson, N., Syverson, P.: Tor: The Second-Generation Onion Router, *Proceedings of the 13th USENIX Security Symposium*, pp. 303-320, San Diego (2004).
- [22] Dingledine, R., Mathewson, N.: Anonymity loves company: Usability and the network effect, *The Fifth Workshop on the Economics of Information Security (WEIS 2006)*, University of Cambridge (2006).
- [23] D’Orlando, F.: The Market for Pornography in Italy: Empirical Data and Theoretical Considerations, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1125129, 2008-04-25 (2008).
- [24] Federrath, H., Jerichow, A., Kesdogan, D., Pfitzmann, A., Spaniol, O.: *Mobilkommunikation ohne Bewegungsprofile*, in: Pfitzmann, A., Müller, G. (eds.), *Mehrseitige Sicherheit in der Kommunikationstechnik*, pp. 169-180, Addison Wesley, Boston (1997).
- [25] Federrath, H.: *Privacy Enhanced Technologies: Methods - Markets - Misuse*, in: Katsikas, S., Lopez, J., Pernul, G. (eds.), *Trust, Privacy, and Security in Digital Business*, pp. 1-10, Springer-Verlag, Berlin Heidelberg (2005).
- [26] Feigenbaum, J., Freedman, M., Sander, T., Shostack, A.: Economic barriers to the deployment of existing privacy technology: *Proceedings of the Workshop on Economics and Information Security*, Berkley, CA (2002).
- [27] FortConsult: *Practical onion hacking: Finding the real address of tor clients* (2006).
- [28] Fritsch, L., Roßnagel, H., Schwenke, M., Stadler, T.: Die Pflicht zum Angebot anonym nutzbarer Dienste: Eine technische und rechtliche Zumutbarkeitsbetrachtung, *Datenschutz und Datensicherheit (DuD)*, 29, (10), 592-596 (2005).
- [29] Galletta, D.F., Henry, R., McCoy, S., Polak, P.: Web site delays: How tolerant are users? *Journal of the Association for Information Systems*, 5, (1), 1-28 (2004).
- [30] Huberman, B.A., Adar, E., Fine, L.R.: Valuating Privacy, *IEEE Security & Privacy*, 3, (5), 22-25 (2005).
- [31] JonDos GmbH: *JonDoFox: Private and Secure Web Browsing (2.1.2)*, www.jondos.de/en/jondodox, accessed 2008-11-30.
- [32] Lambiase, J.: *Sex: Online and in Internet Advertising*, Lawrence Erlbaum Associates (2003).
- [33] McCoy, D., Bauer, K., Grunwald, D., Kohno, T., Sicker, D.: Shining Light in Dark Places: Understanding the Tor Network, in: Borisov, N., Goldberg, I. (eds.), *Proceedings of the 8th Privacy Enhancing Technologies Symposium (PETS 2008)*, pp. 63-76, Springer, Berlin Heidelberg (2008).
- [34] Murdoch, S.J.: Economics of Tor performance, <http://www.lightbluetouchpaper.org/2007/07/18/economics-of-tor-performance/>, 2007-07-18 (2007).

- [35] Odlyzko, A.: The Case Against Micropayments, in: Wright, R. (eds.), Proceedings of 7th International Conference Financial Cryptography (FC'03), pp. 77-83, Springer, Berlin Heidelberg (2003).
- [36] Ozment, A., Schechter, S.E.: Bootstrapping the Adoption of Internet Security Protocols, Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS 06), Cambridge (2006).
- [37] Pfitzmann, A., Pfitzmann, B., Waidner, M.: ISDN-mixes: Untraceable communication with very small bandwidth overhead, Proceedings of the GI/ITG Conference on Communication in Distributed Systems, pp. 451-463 (1991).
- [38] Pfitzmann, A., Waidner, M.: Networks Without User Observability: Design Options, Advances in Cryptology - EUROCRYPT '85: Proceedings of a Workshop on the Theory and Application of Cryptographic Techniques, pp. 245, Springer, Berlin Heidelberg (1986).
- [39] Pitkow, J.E.: Summary of WWW characterizations, Computer Networks and ISDN Systems, 30, (1-7), 551-558 (1998).
- [40] Rogers, E.M.: Diffusion of Innovations, 5. Auflage, Free Press, New York (2003).
- [41] Roßnagel, H.: Bootstrapping the Adoption of Privacy Enhancing Technology, Proceedings of the 1st IDIS Workshop, Arona, Italy (2008).
- [42] Schulze, H., Mochalski, K.: Internet Study 2007: The Impact of P2P File Sharing, Voice over IP, Skype, Joost, Instant Messaging, One-Click Hosting and Media Streaming such as YouTube on the Internet, <http://www.ipoque.com/resources/internet-studies/internet-study-2007> (2007).
- [43] Shostack, A.: 'People Won't Pay For Privacy,' Reconsidered, 2nd Annual Workshop 'Economics and Information Security', University of Maryland (2003).
- [44] Softonic: XeroBank Browser, <http://xerobank-browser.softonic.de/>, accessed 2008-05-20.
- [45] Spiekermann, S.: Die Konsumenten der Anonymität: Wer nutzt Anonymisierungsdienste? Datenschutz und Datensicherheit (DuD), 27, (3), 150-154 (2003).
- [46] Spiekermann, S.: The desire for privacy: Insights into the views and nature of the early adopters of privacy services, International Journal of Technology and Human Interaction, 1, (1) (2004).
- [47] Syverson, P.: The Paradoxical Value of Privacy, 2nd Annual Workshop 'Economics and Information Security', University of Maryland (2003).
- [48] Top Ten Reviews: Internet Pornography Statistics 2009, <http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html#anchor1>.
- [49] Tsai, J., Egelman, S., Cranor, L., Acquisti, A.: The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, Proceedings of Workshop on the Economics of Information Security, Pittsburgh, PA (2007).
- [50] Videoload.de: Pastewka Videoload Peinliche Momente, <http://www.youtube.com/watch?v=5rBK4AUljUg>, accessed 2008-04-25.