The Market Failure of Anonymity Services

Heiko Rossnagel

The Market Failure of Anonymity Services

Heiko Rossnagel

Fraunhofer Institute for Industrial Engineering (IAO),
Nobelstr.12 70569 Stuttgart, Germany
heiko.rossnagel@iao.fraunhofer.de

Abstract. While technologies for anonymous communication have been thoroughly researched and despite the existence of several protection services, the deployment of such services has not yet reached the mass market of end users. So far only a very small fraction of users are using anonymity services and early adopters, which are necessary to reach a critical mass of adopters, have not been attracted. Consequently, there is no beneficial market today for anonymity services. In this paper we conduct an analysis grounded in the diffusion of innovations theory on the reasons for the slow diffusion of anonymity services. We conclude that an unclear relative advantage, a high complexity and the inability to observe or demonstrate that the communication is really anonymous are major hindrances. Furthermore, we discuss several possibilities on how to stimulate the adoption.

1 Introduction

Since Chaum proposed a method for anonymous and unobservable delivery of electronic messages [13] technologies for anonymous communication have been thoroughly researched. The concept has been adapted to internet data traffic [42], ISDN call routing [41] or mobile technology [22]. Furthermore, several protection services that provide anonymous communications such as TOR [20] or AN.ON [10] 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 anonymity services [34] and early adopters, which are necessary to reach a critical mass of adopters, have not been attracted [23]. Consequently, there is no beneficial market today for providers of anonymity services.

Only as of late there is a growing body of research in the area of economics of privacy enhancing technologies. Most of the work, however, is concerned with the willingness of users to pay for privacy services [49] or under which circumstances users are willing to disclose private information [5]. Also, the effects of privacy assurance methods like privacy seals or policy statements have been widely researched [36]. What seems to be missing is an analysis on possible reasons for the slow diffusion of anonymity services, despite having been available and useable for free such as the AN.ON service [10].

The adoption and diffusion of information technology has been well researched in the economics and information systems domains. This has led to the development of widely accepted and used theories such as the diffusion of innovations theory [44] and the technology acceptance model [18]. However, the adoption of security technology and in particular of privacy enhancing technologies (PET) has not enjoyed similar attention. Instead, PETs continue to be designed with technological factors in mind, valuing increases in security guarantees and even technical complexity over practical relevance.

Feigenbaum *et al.* [23] provides first steps to determine economic barriers in the deployment of privacy technology. With our contribution we want to build on this work and extend it by performing an analysis grounded in the diffusion of innovations theory [44] on the reasons for the slow diffusion of anonymity services. We try to identify driving factors and major obstacles and to provide recommendations on how to design and deploy anonymity services in order to achieve higher acceptance in the future. The rest of this paper is structured as follows. We first review related work on economic aspects of privacy in section 2. In section 3 we will present the theoretical foundation for our analysis. We apply these theories to anonymity services in section 4 and in section 5 we discuss possible efforts to bootstrap the adoption. Section 6 concludes our findings.

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 [53]. 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.

Other studies examined the circumstances under which users are willing to disclose private information [5,3,9]. 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. This demonstrates discrepancies between attitudes towards privacy and actual behaviour [9].

The effects of privacy assurance methods like privacy seals or policy statements have also been widely researched [57,36,8]. Kai-Lung *et al.* [31] showed that the existence of a privacy statement induced more subjects to disclose their personal information while that of a privacy seal did not. They also demonstrated that monetary incentives have a positive influence on disclosure while information requests have a negative one. The results of Belanger *et al.* [8] 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 [4]. He attributes the small market size to the low amount of people who are conscious of their security needs [3] 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" [4]. Shostack [49] 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.* [23] 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 anonymity services has been researched in [51] and [52], 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 Euro per month while 10% would have paid more then 5.00 Euro.

On a more general level, the adoption of information technology has been widely researched in the economics and information systems domains. Theories such as the diffusion of innovations theory [44] and the technology acceptance model [18] have been applied to explain the adoption and diffusion of a great variety of innovations ranging from new methods of agriculture [47] to modern communication technology [29]. However, to our knowledge there are only a few studies that use these theories to examine the adoption of security technology. Ozment and Schechter [39] discuss several possibilities to bootstrap the adoption of internet security protocols while Rossnagel [46] applies the theories to explain the slow adoption of electronic signatures.

3 Theoretical Background

3.1 Diffusion of Innovations

In the information systems literature, a variety of theoretical perspectives have been advanced to provide an understanding of the determinants of usage. One line of research has examined the adoption and usage of information technology from a diffusion of innovation perspective [44,55]. This research examines a variety of factors which are thought to be determinants of IT adoption and usage [54]. Rogers defines diffusion as "the process in which an innovation is communicated through certain channels over time among the members of a social system" and as a "special type of communication, in that the messages are

concerned with new ideas" [44]. An innovation is defined as an "idea, practice, or object perceived as new by an individual or other unit of adoption" [44].

The Innovation-Decision Process. "The innovation-decision process is the process through which an individual passes from gaining initial knowledge of an innovation, to forming an attitude toward the innovation, to making a decision to adopt or reject, to implementation of the new idea, and to confirmation of this decision" [44]. A model of the innovation-decision process is illustrated in figure 1. The start and speed of the innovation-decision process varies between the different members of the social system. Therefore, the various decisions to adopt or reject the innovation are also spread over time. The dynamic of this process is a result of the changes in the information the individual acquires and possesses about the innovation [32].

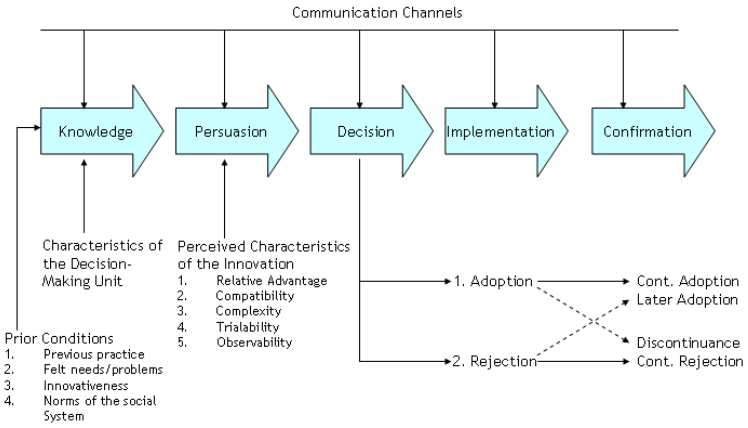

Fig. 1. Model of the five stages in the innovation-decision process [44]

Perceived Attributes of Innovations. Rogers defines five attributes of innovations, as perceived by the members of the social system that determine the rate of adoption [44]:

Relative advantage. is the degree to which an innovation is perceived as better than the idea it supersedes. It is not so important if the innovation has an objective advantage, but rather if the individual perceives the innovation as advantageous. Advantages can be measured in economic terms, but social prestige, convenience, and satisfaction also can play an important role.

Compatibility. is the degree to which an innovation is perceived as being consistent with the existing values, past experiences, and needs of potential adopters.

An Innovation that is consistent with the existing values will diffuse more rapidly than one that is incompatible with the norms and values of the social system.

Complexity. is the degree to which an innovation is perceived as difficult to understand and use. Innovations that are easier to understand will be adopted more rapidly than those which require the adopter to develop new skills and understandings.

Triability. is the degree to which an innovation may be experimented with on a limited basis. New ideas that can be tried before the potential adopter has to make a significant investment in the innovation are adopted more quickly.

Observability. is the degree to which the results of an innovation are visible to others. The easier it is for individual to observe the results of an innovation, the more likely they are to adopt [44,35].

Adopter Categories. Adopters can be classified into five categories based on their rate of innovativeness. Figure 2 shows the normal frequency distribution and the approximate percentages of the individuals included [44].

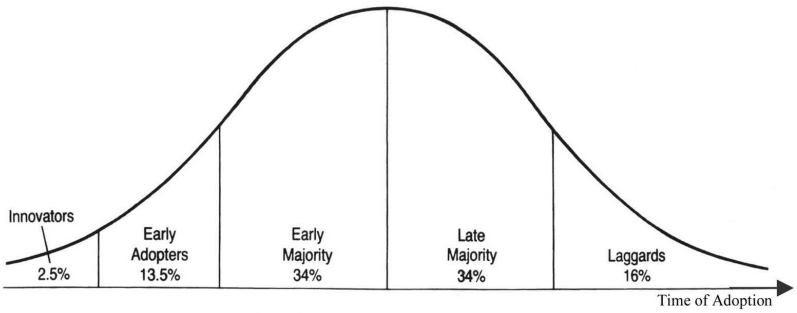

Fig. 2. Adopter categorisation on the basis of innovativeness [44]

Innovators. play an important role in the diffusion process. They launch a new idea within the social system by importing an idea from the outside of the system boundaries. However, innovators might not be respected by other members of the social system. Innovators need the ability to understand and apply complex technical knowledge and must be able to cope with a high degree of uncertainty about an innovation at the time of adoption.

Early adopters. are more integrated in the social system than innovators. This adopter category has the biggest influence and degree of opinion leadership within the system. Potential adopters look at early adopters for advice and information about an innovation. Therefore, early adopters help trigger the critical mass when they adopt an innovation.

Early majority. The early majority adopts innovation before the average members of a system. They do not possess a position of opinion leadership in the system, but interact with a lot of members of the social system. They are not the first to adopt an innovation, but follow with a deliberate willingness.

Late majority. The late majority adopts an innovation after the average member of the system. They approach innovations sceptical and cautious and adoption results because of economic necessity or increasing peer pressure.

Laggards. are the last members of a system to adopt. They possess almost no opinion leadership.

Interactive innovations and network effects An interactive innovation is an innovation that is of little use to an adopting individual unless other individuals with whom the adopter wants to communicate also adopt. Thus a critical mass of individuals has to adopt the innovation before it is of use for the average member of the system [33]. The individuals who have adopted an innovation form a network and with each new member the overall value of the network increases [33]. This fundamental value proposition is being called network effects, network externalities, and demand side economics of scale [48]. Until a critical mass occurs in the diffusion process the rate of adoption is relatively slow [33]. After the critical mass is achieved the rate of adoption accelerates and leads to a take off in the adoption curve [38].

3.2 Technology Acceptance

As a second line of research the Technology Acceptance Model (TAM) [18] has emerged as a powerful way to explain the acceptance and adoption of technology. In several studies the TAM has been tested in a variety of situations with all kinds of different empirical data [18,17,40] and has been proven to be a valid and reliable model for the explanation of technology acceptance [54,28]. The TAM is based on the "Theory of Reasond Action (TRA)" from social psychology [24]. Davis defines two determining factors for the intention to use and the resulting actual usage of an information system. These factors are the "perceived usefulness", which is analogous to the relative advantage construct of the diffusion of innovations theory, and "perceived ease of use", which is the converse construct to "complexity" [54].

4 Analysis of Anonymity Services

4.1 The Innovation-Decision Process.

Based on the limited market penetration so far, we can assume that only a fraction of the innovators have adopted anonymity services. Furthermore, the results presented in [3] suggest that most of the individuals that participated

in their study had not even reached the knowledge stage. While almost 90% of their sample claimed to be highly or moderately concerned about privacy they clearly underestimated the risks of privacy abuses [3]. Acquisti [5] attributes this discrepancy to the construct of bounded rationality which is the inability of the individuals to calculate and compare the magnitudes of payoffs associated with various strategies in privacy-sensitive situations. This includes the "inability to process all the stochastic information related to risks and probabilities of events leading to privacy costs and benefits" [5]. This lack of awareness or underestimation of privacy risks is further reinforced by the tendency of users to assume that negative events are less likely to happen to them than to others and that positive events are more likely to happen to them than others [43,58]. So far marketing efforts or awareness campaigns on the dangers associated with identity theft have not been as prevalent as similar campaigns that have been undertaken for other preventive innovations like HIV prevention and seat belt usage. Even if the individual is aware of the privacy risks, he or she also has to know about the existence of privacy protecting technology in order to adopt. The results of [3] suggest that even technologically highly educated people are not familiar with technology to protect their online privacy. If this knowledge about existing technology is obtained, the user enters the persuasion phase. Only if the potential benefits of using privacy enhancing technologies outweigh the associated costs, a positive adoption decision will be formed by the individual. A lack of observability of the positive impacts of using PET might also lead to a discontinuance of the adoption during the implementation and confirmation stages.

4.2 Perceived Attributes of Anonymity Services

Relative Advantage and Perceived Usefulness. As stated above, an awareness of the privacy risks associated with unprotected online behaviour is required to perceive a relative advantage of using anonymity services. Also, anonymity services are preventive innovations, which are ideas that are adopted by an individual at one point in time to lower the probability that some future unwanted event (i.e. Surveillance of the users traffic) will occur [44]. Preventive innovations usually have a very slow rate of adoption, because the unwanted event might not happen even without the adoption of the innovation (i.e. no surveillance occurs despite not using anonymity services). Therefore, the relative advantage is not very clear cut. Furthermore, bounded rationality and optimistic biases diminish the perceived usefulness of this technology [4].

In addition, being able to surf anonymously will not necessarily lead to an advantage by itself. The usefulness is dependent on the context of the accessed information and the actual situation of the user. For example there should be usually a higher demand to anonymously access adult entertainment material than to anonymously access news or weather reports. Also individuals might wish to be anonymous when accessing some information such as sports results while being at work; they might not be concerned about their anonymity when performing the same task at home. Even reading the website of the New York

Times might require different degrees of anonymity depending on the country from which you access the website. Also as stated in [23], anonymity services can also be classified as interactive innovations that are subject to network effects. For example in [21] it has been shown that the size of the anonymity sets of web anonymizers and therefore their usefulness is dependent on the number of users of the system. Therefore, the adoption of PETs will be rather slow until a critical mass of users will be reached. In some cases the usage of an anonymity service might even lead to the opposite of the intended effect by reducing the number of potential suspects due to the small number of people who posses the required knowledge to use such a system. Network effects also influence the performance of the system. The more users are active on a system, the better the performance of the systems becomes. This in turn influences usability, and specifically in the case of web sites, loading speeds have been shown to be a major usability factor [27]. Such reductions in performance and loading speeds will form costs that the individuals will weigh against the perceived benefits of adopting, which have been shown to be rather nebulous. However, the relative advantage of using anonymity services could be improved by bundling the use of the technology with different services that particularly require or benefit from anonymous communications (see next section).

(Social) Compatibility. Usage of privacy measures is quite common in the offline world. We use curtains to protect the privacy of our homes [49]. Caller-ID blocking, voice mail services, and unlisted numbers are used to protect ourselves against unwanted phone calls [49]. Traditional mail is usually sent in an envelope and cash has been a widely used form of anonymous payment. In the online world, however, we are used to identifying ourselves in order to access particular services. Online shopping is rarely anonymous [37] and users usually do not encrypt their mail [3]. On the other hand, users are starting to undertake steps to protect their online privacy. Spam filters are used to block unwanted mails and people supply no or false information in online forms [3]. Therefore, a high degree of compatibility could be achieved, especially if the anonymity service is able to motivate its usage by paralleling similar applications in the offline world.

Complexity and Ease of Use. Complexity and missing user-friendliness of anonymity solutions can pose a major barrier for their adoption. The correct installation and usage of local proxies and related browser configuration is often too hard for users to be properly carried out [14]. Also the time required to install the software, the added complexity of maintaining the additional software, the complexity of uninstalling software one doesn't like, and the risk that any software downloaded from the Internet may contain malware add to the complexity and limit the ease of use. Technical problems include possible information leakages due to DNS [20], browser plug-ins, or plain configuration faults during installation [10]. However, there have been major improvements in this regard. The "XeroBank"-browser [50] for example is a modification of the popular Firefox browser, readily compiled with a client for the TOR network that is usable

out of the box without requiring any complicated configurations. The limited popularity of this software might be attributed, apart from the problems stated above, to the deactivation of several features such as Javascript and Active-X due to security reasons.

Triability. Since several anonymity services are available for testing without financial charges the degree of triability is quite good. If the trend to commercialise these services continues, the degree of triability might decrease in the near future. However, it seems to be very likely that there will be free solutions available that can be tested even years from now.

Observability. A lack of observability or missing ability to demonstrate the effects of anonymous communications is a major concern for the adoption of such services. While confidentiality can be achieved by the sender using encryption, anonymity cannot be created by the sender or receiver. Instead users have to trust the infrastructure to provide protection [1]. Furthermore, without some technical expertise users are not able to reliably detect if they are really communicating anonymously. There might be indications like a symbol or message in the browser or a decreased performance when accessing web sites, but still users have to trust their systems configuration and the used infrastructure. In the context of malicious nodes this asymmetric information about the reliability of the used technology could lead to a lemons market [25], which was defined in [7]. In this pioneering article the author argues that information asymmetry and uncertainty about the product quality will lead to a market failure, unless appropriate counteracting mechanisms are undertaken. In a market that contains good and bad (lemons) anonymity services, imperfect information about service quality causes the user to average the quality and price of the service used. The information gap enables the opportunistic behaviour of the owner of a lemon to sell it at average price. As a result, the better quality service will not be used since the price it deserves can not be obtained. The consequence of such practice will lead to a continuous fall of both quality and value of services.

4.3 Summary

Looking at anonymity services from a diffusion of innovations perspective, it seems rather unlikely that adoption will develop naturally. 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. Also, the attributes that determine the rate of adoption seem to be quite unfavourable. While triability and compatibility can be achieved, the lack of observability, a high complexity and the missing or unclear relative advantage will be significant barriers to the adoption of PET.

5 Bootstrapping the Adoption of Anonymity Services

Since we argued in the last section that adoption of anonymity services will not increase naturally, we will now discuss various possibilities to facilitate their adoption. We first outline the different options and then try to provide some recommendations.

5.1 Approaches to Stimulating Technology Adoption

There are several ways to stimulate the adoption of security technology. Some of which can be quite invasive while others do not require such a great amount of intervention by policy makers.

Information Provisioning. One possibility to facilitate the adoption of privacy technology is to increase the awareness of users about the risks of unprotected online communications. Similar campaigns have been carried out for other preventive innovations like seat belt usage, designated drivers and safer sex. The rationale behind such campaigns is that when individuals are aware of the associated risks and the possibilities of protection they will apply the respective protection measures. Such campaigns, however, often fail to achieve the desired effectiveness [19].

Mandatory Adoption. The most invasive form to stimulate adoption is to mandate the usage of the technology and to impose this mandate by issuing fines for noncompliance. Users who adopt will receive the relative advantage of not being subjected to the fines [39]. One example of a partial mandate to adopt anonymity technology can be found in the German Teledienstedatenschutzgesetz (TDDSG). According to 4 par. 6 TDDSG, service providers are required to provide anonymous or pseudononymous access to their service, if this is technically possible and economic reasonable. However, this mandate has not been enforced so far, although there are cases where this reasonability exists [26].

Bundling Complements. Another way to increase the relative advantage of adopting a technology is to bundle it with complementary goods [39]. In the case of anonymity services one such complementary good could be to provide access to websites that are blocked for particular user groups. Recent examples are Chinas Internet filtering system [15] or the Pandora.com internet radio [60] that is not accessible outside the USA.

Facilitating Subnetwork Adoption. Adoption may start within a subnetwork. If this group is large enough and well coordinated this could lead to natural adoption [39]. Privacy technology could be selectively offered to users of services which have a more obvious demand for anonymity. For example users of pornographic material could be a promising target group for the deployment of

anonymous services [45], since they usually have a high demand for anonymity, a high level of innovativeness and a high willingness to pay and have been drivers of technological innovation in the past [16]. However, technology designers might have ethical issues directly promoting the usage of their technology to access pornographic material. Dating services are another example where privacy technology could be tailored to a specific target group [26,12].

Coordination. Coordination is a related approach in which individuals and organisations try to adopt together. For example different service providers could form a single network of anonymous users in order to increase the anonymity set and therefore the usefulness of their services. Of course such an approach will also create costs for recruiting, drafting contracts and other coordination activities [39].

Subsidization. Another approach is to decrease the costs associated with the adoption by subsidizing the technology. Since some anonymity services can be used without service charges a decrease of monetary costs on the user side is not possible. Nevertheless, generating incentives for service providers to handle personal information in a new way, can allow the growth of the market [4].

5.2 Recommendations

A successful adoption of anonymity services without some additional stimulation seems to be very unlikely. Vendors of anonymity services should try to bundle their technology and services with complementary goods in order to increase the relative advantage of their solution. Furthermore, specifically targeting subnetworks which have an obvious demand for anonymous access and ideally have a large percentage of early adopters could be a promising approach to bootstrap the adoption. The German video on demand service provider videoload.de for example 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 service [56][1]. Also policy makers could intervene in order to protect the privacy of the citizens by creating incentives to adopt anonymity services. One such measure could be to increase the perceived usefulness by raising the awareness about the risks of unprotected online communications and the technologies to protect against these risks. However, bounded rationality, immediate gratification and optimistic bias could still prevent users to adopt this technology.

Expecting end users to adopt on their own, even when given incentives may be too much to ask of them [59]. Therefore, a paradigm shift in the design of PET from user centric solutions to privacy respecting infrastructures might be necessary. A similar paradigm shift has been proposed in [12] and [11] advocating a "Positive-Sum" approach instead of the now prevailing "Zero-Sum" approach

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

and making a case for building privacy into information technology systems at an early stage. Legal intervention could be used to generate incentives for service providers to handle personal information in a privacy respecting way by applying privacy enhancing infrastructures. As one measure to create those incentives several U.S. states have enacted laws that require organizations to notify the affected individuals if personal data under their control is believed to have been acquired by an unauthorized person [6]. The results of [2] show a negative and statistically significant impact of data breaches on a company's market value on the announcement day for the breach. Creating incentives to develop privacy respecting infrastructures could allow a growth of the market for the respective technologies [4]. These incentives could also be created by either a partial mandate to provide anonymous access when reasonable or by subsidizing.

6 Conclusion

In this paper we conducted an analysis grounded in the diffusion of innovations theory on the reasons for the slow diffusion of privacy enhancing technologies. We have identified driving factors and barriers for the adoption of these technologies. We concluded that an unclear relative advantage and the inability to observe or demonstrate that the communication is really anonymous are major hindrances. Furthermore, we argued that most of the potential adopters have not even reached the first stage of the innovation-decision-process by being unaware of the risks of unprotected communication and the technologies to protect against these risks. Therefore, we conclude that adoption of these services will not occur naturally and consequently that they will not be commercial successful. We also discussed possibilities to stimulate the adoption of anonymity services. We identified steps that can be carried out by vendors, like bundling with complementary goods or tailoring their service to subnetworks with an obvious demand for anonymity. In addition, we discussed possibilities of legal intervention to protect the privacy of the citizens and to stimulate a market growth for anonymity services. We believe that in order to be successful, there has to be a paradigm shift in the design of privacy enhancing technology from user centric solutions to privacy respecting infrastructures. Our work has several limitations. The most obvious one being that we only provided qualitative arguments that should be substantiated by empirical research in the near future. Due to the complexity of this research field our work can only provide some small first steps to explain the missing adoption of anonymity services. We strongly encourage further research efforts in that direction.

References

1. Acquisti, A., Dingledine, R., Syverson, P.: On the economics of anonymity, Financial Cryptography FC03 (2003).
2. Acquisti, A., Friedman, A., Telang, R.: Is There a Cost to Privacy Breaches?: An Event Study, Proceedings of the Twenty Seventh International Conference on Information Systems, Milwaukee, WI (2006).

3. Acquisti, A., Grossklags, J.: Privacy and Rationality in Individual Decision Making, IEEE Security & Privacy, 3, (1), 26-33 (2005).
4. 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).
5. Acquisti, A.: Privacy in Electronic Commerce and the Economics of Immediate Gratification, Proceedings of the EC04, ACM, New York, New York (2004).
6. Anderson, R., Boehme, R., Clayton, R., Moore, T.: Security Economics and the Internal Market, http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf (2008).
7. Arkerlof, G.A.: The Market for Lemmons: Quality, Uncertainty and the Market Mechanism, The Quaterly Journal of Economics, 84, (3), 488-500 (1970).
8. 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).
9. Berendt, B., Guenther, O., Spiekermann, S.: Privacy in E-Commerce: Stated Preferences vs. Actual Behavior, Communications of the ACM, 48, (4), 101-106 (2005).
10. Berthold, O., Federrath, H., Koepsell, S.: Web MIXes: A system for anonymous and unobservable Internet access, in: Federrath, H. (eds.), Proceedings of Designing Privacy Enhancing Technologies, pp. 115-129, Springer, Berlin Heidelberg (2000).
11. Cavoukian, A.: Privacy and Radical Pragmatism: Change the Paradigm, Information and Privacy Commisioner of Ontario, Canada, 2008-08-08.
12. Cavoukian, A.: Privacy in the Clouds: Privacy and Digital Identity: Implications for the Internet, 2008-05-28.
13. Chaum, D.L.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Communications of the ACM, 24, (2), 84-88 (1981).
14. 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, pp. 41-51, New York, NY (2007).
15. Clayton, R., Murdoch, S.J., Watson, R.N.M.: Ignoring the Great Firewall of China, Proceedings of the 6th Workshop on Privacy Enhancing Technologies, Cambridge (2006).
16. Coopersmith, J.: Pornography, Technology and Progress, ICON, 4, 94-125 (1998).
17. Davis, F.D., Bagozzi, R.P., Warshaw, P.R.: User Acceptance of Computer Technology: A Comparison of Two Theoretical Models, Management Science, 35, (8), 982-1003 (1989).
18. Davis, F.D.: Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, MIS Quaterly, 13, (3), 319-340 (1989).
19. Diel, S.: Gestaltungsvorschlge zur Verteilung von Kosten und Nutzen qualifizierter elektronischer Signaturen, Master Thesis, Department of Business Administration and Economics, Goethe-University, Frankfurt am Main, 2007.
20. 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).
21. 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).

22. Federrath, H., Jerichow, A., Kesdogan, D., Pfitzmann, A., Spaniol, O.: Mobilkommunikation ohne Bewegungsprofile, in: Pfitzmann, A., Mueller, G. (eds.), Mehrseitige Sicherheit in der Kommunikationstechnik, pp. 169-180, Addison Wesley, Boston (1997).
23. 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).
24. Fishbein, M., Ajzen, I.: Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research, Addison-Wesley, Reading, Massachusetts (1975).
25. Fritsch, L., Abie, H.: Towards a Research Road Map for the Management of Privacy Risks in Information Systems, in: Alkassar, A., Siekmann, J. (eds.), Sicherheit 2008, pp. 1-16, Koellen Druck + Verlag GmbH, Bonn (2008).
26. 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).
27. Galletta, D.F., Henry, R., McCoy, S., Polak, P.: Web site delays: How tolerant are users? Journal of the AIS, 5, (1), 1-28 (2004).
28. Gefen, D., Karahanna, E., Straub, D.W.: Trust and TAM in Online Shopping: An Integrated Model, MIS Quaterly, 27, (1), 51-90 (2003).
29. Grantham, A., Tsekouras, G.: Diffusing Wireless Applications in a Mobile World, Technology in Society, (27), 85-104 (2005).
30. Huberman, B.A., Adar, E., Fine, L.R.: Valuating Privacy, IEEE Security & Privacy, 3, (5), 22-25 (2005).
31. Kai-Lung, H., Hock, H.T., Sang-Yong, T.L.: The Value of Privacy Assurance: An Exploratory Field Experiment, MIS Quaterly, 31, (1), 19-33 (2007).
32. Litfin, T.: Adoptionsfaktoren: Empirische Analyse am Beispiel eines innovativen Telekommunikationsdienstes, DUV, Wiesbaden (2000).
33. Mahler, A., Rogers, E.M.: The diffusion of interactive communication innovations and the critical mass: The adoption of telecommunication services by German banks, Telecommunications Policy, (23), 719-740 (1999).
34. 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).
35. Moore, G.C., Benbasat, I.: Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation, Information Systems Research, 2, (3), 173-191 (1991).
36. Moores, T.T., Dhillon, G.: Do Privacy Seals in E-Commerce Really Work? Communications of the ACM, 46, (12), 265-271 (2003).
37. Odlyzko, A.: Privacy and the Clandestine Evolution of E-Commerce, Proceedings of the ninth international conference on Electronic commerce, pp. 3-6, ACM Press, Mineapolis, Minnesota (2007).
38. Oren, S.S., Smith, S.A.: Critical Mass and Tariff Structure in Electronic Communications Markets, Bell Journal of Economics, 12, (2), 467-487 (1981).
39. 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).
40. Pavlou, P.A.: Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model, International Journal of Electronic Commerce, 7, (3), 101-134 (2003).

41. Pfitzmann, A., Pfitzmann, B., Waidner, M.: ISDN-mixes: Untraceable communication with very small bandwith overhead, Proceedings of the GI/ITG Conference on Communication in Distributed Systems, pp. 451-463 (1991).
42. Pfitzmann, A., Waidner, M.: Networks Without User Observability: Design Options, Advances in Cryptology - EUROCRYPT '85, pp. 245, Springer, Berlin Heidelberg (1986).
43. Rhee, H., Ryu, Y.U., Kim, C.: I Am Fine But You Are Not: Optimistic Bias and Illusion of Control on Information Security, Proceedings of the Twenty-Sixth International Conference on Information Systems (ICIS 05), pp. 381-394, AIS, Las Vegas, Nevada (2005).
44. Rogers, E.M.: Diffusion of Innovations, 5. edition, Free Press, New York (2003).
45. Rossnagel, H., Zibuschka, J., Pimenidis, L., Deselaers, T.: Facilitating the Adoption of Tor by Focusing on a Promising Target Group, Proceedings of the 14th Nordic Workshop on Secure IT Systems, Oslo, Norway, pp. 15-27 (2009).
46. Rossnagel, H.: Mobile Qualifizierte Elektronische Signaturen: Analyse der Hemmnisfaktoren und Gestaltungsvorschlaege zur Einfuehrung, Gabler, Wiesbaden (2009).
47. Ryan, B., Gross, N.C.: The Diffusion of Hybrid Seed Corn in Two Iowa Communities, Rural Sociology, (8), 15-24 (1943).
48. Shapiro, C., Varian, H.R.: Information Rules: A Strategic Guide to the Network Economy, Harvard Business School Press, Boston (1999).
49. Shostack, A.: 'People Won't Pay For Privacy,' Reconsidered, 2nd Annual Workshop 'Economics and Information Security', University of Maryland (2003).
50. Softonic: XeroBank Browser, http://xerobank-browser.softonic.de/, accessed 2008-05-20.
51. Spiekermann, S.: Die Konsumenten der Anonymitaet: Wer nutzt Anonymisierungsdienste? Datenschutz und Datensicherheit (DuD), 27, (3), 150-154 (2003).
52. 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).
53. Syverson, P.: The Paradoxical Value of Privacy, 2nd Annual Workshop 'Economics and Information Security', University of Maryland (2003).
54. Taylor, S., Todd, P.A.: Understanding Information Technology Usage: A Test of Competing Models, Information Systems Research, 6, (2), 144-176 (1995).
55. Tornatzky, L.G., Klein, K.J.: Innovation Characteristics and Innovation Adoption - Implementation: A Meta-Analysis of Findings, IEEE Transactions on Engineering Management, 29, 28-45 (1982).
56. Videoload.de: Pastewka Videoload Peinliche Momente, http://www.youtube.com/watch?v=5rBK4AUljUg, accessed 2008-04-25.
57. Vila, T., Greenstadt, R., Molnar, D.: Why We Can't Be Bothered to Read Private Policies: Models of Privacy Economics as a Lemons Market, 2nd Annual Workshop 'Economics and Information Security', Maryland (2003).
58. Weinstein, N.D.: Optimistic biases about personal risks, Science, (24), 1232-1233 (1989).
59. Weitzner, D.J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., Sussman, G.J.: Information Accountability, Communications of the ACM, 51, (6), 82-87 (2008).
60. Westergren, T.: Pandora Internet Radio, http://www.pandora.com/restricted, accessed 2008-05-21.