Geschäftsmodelle für privatsphärenfreundliche soziale Online-Netzwerke

Christoph Eunicke, Heiko Roßnagel, Jan Zibuschka

Fraunhofer IAO
Nobelstraße 12
70569 Stuttgart
{vorname.nachname}@iao.fraunhofer.de

Abstract: Soziale Netzwerke gewinnen zunehmend an Bedeutung. Bisher allerdings weisen diese sozialen Online-Netzwerke ganz erhebliche Defizite im Hinblick auf den Schutz der Privatsphäre ihrer Mitglieder auf. Ziel dieses Beitrags ist es anhand einer ausgewählten Beispiel-Community die Defizite im Hinblick auf Privatsphärenschutz der aktuellen Lösungen aufzuzeigen, sowie zu illustrieren, wie dies in der Zukunft privatsphärenfreundlich gestaltet werden könnte und welche Technologien dafür benötigt werden. Weiterhin werden die Marktchancen dieser Technologien über den konkreten Anwendungsfall der Beispiel-Community hinaus diskutiert und erste Ansätze für tragfähige Geschäftsmodelle in diesem Bereich aufgezeigt.

1 Einleitung

In den letzten Jahren haben Soziale Netzwerke zunehmend an Bedeutung gewonnen und die Anbieter solcher Netzwerke haben sich zu Multi-Milliarden-Konzernen entwickelt. Laut der eigenen Webseite hat Facebook mittlerweile mehr als 500 Millionen aktive Nutzer und es existieren über 1 Millionen Webseiten, die Facebook in ihre Seiten integriert haben [4]. Ähnliche Statistiken existieren auch für andere soziale Netzwerke, wie beispielsweise Twitter mit über 100 Millionen Nutzern, die über 55 Millionen Tweets jeden Tag posten [22]. Während sich diese sozialen Netzwerke von einfachen Kontaktsammlungen hin zu voll integrierten Kommunikationsplattformen entwickeln, gewinnen sie auch im täglichen Leben der Benutzer immer mehr an Bedeutung. So bot beispielsweise Facebook bereits seit seinem Start jede Menge Plattformfunktionalitäten an und arbeitet ständig daran diese auszubauen, indem es als Enabler für Browserspiele auftritt oder Plugins für Profile bis hin zu einem vollständigen föderierten Identitätsmanagementsystem mit Mehrwertdiensten (z.B. der „mag ich“-Button) anbietet.

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4
weitere Artikel online:
http://informatik2011.de/519.html

Darüber hinaus haben die Entwicklungen im Mobilfunkmarkt zu immer leistungsfähigeren mobilen Endgeräten und gleichzeitig zu immer effektiveren und günstigeren Übertragungsverfahren dazu geführt, dass diese sozialen Netzwerke jederzeit und überall, auch unter Verwendung von ortsbezogenen Daten der Nutzer, genutzt werden können. Zurzeit gibt es mehr als 200 Millionen aktive Nutzer, die mobil auf Facebook zugreifen [4] und 37% der Nutzer von Twitter verwenden ihr Telefon um Tweets zu erstellen [22]. Weiterhin werden zahlreiche Dienste angeboten, die direkt den Ortsbezug für solche sozialen Netzwerke ausnutzen wie beispielsweise FourSquare [7], Facebook Places [5] und Google Latitude [8]. Durch diese alltägliche und allumfassende Verwendung von sozialen Online-Netzwerken im täglichen Leben fallen aber auch eine Fülle von personenbezogenen Daten an, die in diesen Netzwerken verarbeitet werden und entsprechend geschützt werden müssen [15]. Bisher allerdings weisen diese sozialen Online-Netzwerke ganz erhebliche Defizite im Hinblick auf den Schutz der Privatsphäre ihrer Mitglieder auf, wie beispielsweise eine aktuelle Studie der Stiftung Warentest zu Online-Netzwerken zeigt [20]. Darüber hinaus ist insbesondere Facebooks Ansatz zum Privatsphärenschutz als „Privacy Trainwreck“ bezeichnet worden [1]. So hatten etwa Facebooks Werbekunden jahrelang Zugriff auf als geschützt gekennzeichnete Daten der Nutzer [13].

Gerade hier besteht offensichtlich ein dringender Handlungsbedarf um soziale Online-Netzwerke privatsphärenfreundlicher und sozialverträglicher zu gestalten. Die dafür notwendige Technologie ist bereits in Form von Privacy-Enhancing-Technologies (PET) verfügbar. Allerdings haben sich diese PETs bisher am freien Markt nicht durchsetzen können [6]. Die Gründe dafür sind vielfältig. Insbesondere fehlt es aber bisher an überzeugenden Anwendungsfällen und tragfähigen Geschäftsmodellen für diese Technologien [16]. Gerade der Bereich von sozialen Online-Netzwerken bietet ein sehr vielversprechendes Potenzial um diese Lücke zu schließen.

Häufig wird aber gerade im Zusammenhang mit sozialen Netzwerken darauf hingewiesen, dass die Folgen des Missbrauchs personenbezogener Daten äußerst gering wären [15]. Ziel dieses Beitrags ist es daher anhand eines bewusst überzeichneten Beispielszenarios, das aber gleichzeitig ein hohe praktische Relevanz aufweist und sich an realen Entwicklungen orientiert, die Defizite im Hinblick auf Privatsphärenschutz der aktuellen Lösungen aufzuzeigen, sowie zu illustrieren, wie dies in der Zukunft privatsphärenfreundlich gestaltet werden könnte und welche Technologien dafür benötigt werden. Weiterhin werden die Marktchancen dieser Technologien über den konkreten Anwendungsfall hinaus diskutiert und erste Ansätze für tragfähige Geschäftsmodelle in diesem Bereich aufgezeigt.

ISBN 978-3-88579-286-4

Der weitere Verlauf des Beitrags gliedert sich wie folgt. Im nächsten Abschnitt werden zunächst die methodischen Grundlagen beschrieben. Anschließend wird in Abschnitt 3 eine geeignete Beispiel-Community ausgewählt und genauer vorgestellt, die als durchgängiges Szenario für die weitere Analyse dienen soll. In Abschnitt 4 werden dann die Defizite der heutigen Lösungen anhand eines Fallbeispiels innerhalb dieser Community veranschaulicht und in einem weiteren Fallbeispiel aufgezeigt, wie die gleiche Funktionalität auch privatsphärenfreundlich angeboten und genutzt werden könnte. In Abschnitt 5 werden die im zweiten Fallbeispiel verwendeten Privacy-Enhancing-Techonologies genauer dargestellt und ihre Marktchancen über die Beispielcommunity hinaus betrachtet. Die zentralen Ergebnisse werden in Abschnitt 6 diskutiert und zusammengefasst.

2 Methodische Grundlagen

In diesem Beitrag wird grundsätzlich ein Design Science Ansatz nach [11] verfolgt. Wir zielen darauf ab, ein integriertes Datenschutzsystem im Sinne der (wirtschaftlich) tragfähigen Sicherheit [17] zu entwickeln. Ausgehend von empirischen Daten zur Nutzung von Anonymisierungsdiensten, wählen wir ein geeignetes Szenario als Grundlage für einen szenariobasierten Entwurfsprozess [3] aus. Szenariobasierte Ansätze sind gegenüber nutzerzentrischen Ansätzen beim Entwurf innovativer Systeme zu bevorzugen, da Nutzer häufig nicht in der Lage sind, die Vorzüge innovativer Lösungen richtig einzuschätzen [21].

Diese Vorgehensweise ist besonders hilfreich bei der Analyse von Vorteilen und Herausforderungen von entstehenden Infrastrukturen [3]. Darüber hinaus beruht diese Arbeit auf einer vorhergehenden empirischen Studie [18], deren Ergebnisse eindrücklich ein spezifisches Anwendungsszenario für den Privatsphärenschutz nahelegen. Weiterhin ist der szenariobasierte Ansatz insbesondere gut geeignet um komplexe mehrseitige Nutzeranforderungen zu erfassen und auch multiple Effekte von Entwurfsentscheidungen zu illustrieren [3].

3 Exemplarische Beispielcommunity

Datenschutztechnologien sind präventive Innovationen. Dies bedeutet, dass sie die Wahrscheinlichkeit verringern, dass ein ungewünschtes Ereignis (der Missbrauch der personenbezogenen Daten) in der Zukunft auftritt. Solche Innovationen haben häufig das Problem, dass ihr Nutzen für potenzielle Anwender nur schwer erkennbar ist. Um diesen Nutzen erkennen zu können ist ein Bewusstsein für die potenziellen Gefahren notwendig, die entstehen falls eine solche Technologie nicht eingesetzt wird [16]. Um nun diese Gefahren am Beispiel von Communities zu verdeutlichen, wählen wir bewusst ein drastisches Szenario, das aber gleichzeitig praktisch relevant ist und sich an aktuellen Marktentwicklungen orientiert. Gerade diese praktische Relevanz ist besonders wichtig, da Datenschutztechnologien bisher am Markt noch nicht den erwarteten Erfolg hatten. Unser Ziel war es ein Szenario auszuwählen, welches eine möglichst vielversprechende Community anspricht, bei der ein hoher Bedarf an Privatsphäre sowie eine hohe Innovationsbereitschaft der Mitglieder vorhanden ist. Um eine solches Szenario zu identifizieren bietet es sich an, die bisherige Nutzung von Datenschutztechnologien zu betrachten.

Im Rahmen einer empirischen Studie wurde untersucht, für welche Art von Inhalten Anonymisierungsdienste hauptsächlich eingesetzt werden [18]. Die Ergebnisse zeigen, dass mittels Tor überwiegend auf pornographische oder stark sexuell orientierte Inhalte zugegriffen wurde. Im Vergleich zu nicht anonymisierten Internetzugriffen wurde eine signifikant höhere Verwendung solcher Inhalte festgestellt. 57% der Zugriffe über Tor entfielen auf Klassen, deren Darstellung in der Öffentlichkeit in westlichen Ländern nicht vorstellbar wäre. Dieses Ergebnis ist nicht wirklich überraschend, da ja Sexualität eindeutig zum besonders schützenswerten Bereich der Privatsphäre zuzurechnen ist.

Daher bietet es sich an, als Beispielcommunity eine virtuelle Gemeinschaft mit stark sexuell orientiertem Inhalt auszuwählen. Eine solche Beispielcommunity findet sich im Bereich der Escort-Services, wo zunehmend Dienstleistungen online über soziale Netzwerke angeboten werden. So hat etwa eine Studie in New York gezeigt, dass inzwischen deutlich über 80% der Prostituierten über ein Facebook-Profil verfügen. Mindestens 25% der Kundenkontakte lässt sich dabei direkt auf diese Plattform zurückführen. Zudem sind die Kontakte via Facebook für die Prostituierten häufig lukrativer und weniger risikoreich als die klassische Straßenprostitution [23].

Hochpreisige Escort-Modelle werden zudem über Agenturen vermittelt. Da diese jedoch einen hohen Anteil der Transaktionskosten einbehalten, gründen Escorts vermehrt eigene Internetagenturen, die üblicherweise nur aus einer Webseite bestehen, um so den Eindruck zu erwecken, Teil eines größeren Netzwerks zu sein. Alles zusammen führt dazu, dass höherpreisige Escort-Services vermehrt über digitale Wege initiiert werden und die klassischen Mittelsmänner (etwa „Zuhälter“) aus dem Geschäft gedrängt werden [23].

ISBN 978-3-88579-286-4

Dies zeigt, dass in diesem Anwendungsfeld soziale Netzwerke mittlerweile intensiv genutzt werden, gleichzeitig aber eine Community mit höchsten Anforderungen an die Privatsphäre ihrer Nutzer entsteht. Insofern stellt diese Community ein ideales Anwendungsfeld für privatsphärenfördernde Technologien dar.

4 Beispielszenarien

Im Folgenden wird nun anhand eines überzeichneten Beispielszenarios die aktuelle Situation und deren Defizite im Hinblick auf Datenschutz vorgestellt. Anschließend wird aufgezeigt, wie diese Probleme durch aktuell bereits verfügbare Technologien gelöst werden könnten.

4.1 Aktuelle Situation

John Primeur ist auf Dienstreise in einer fremden Stadt im Staat Rotland und sucht nach weiblicher Begleitung für den Abend. Im Hotel benutzt er sein dienstliches Notebook, um über das dortige WLAN eine Internetverbindung aufzubauen. Auf Facebook sucht er nach einschlägigen Angeboten, und findet ein geeignetes Angebot des seriös erscheinenden Dienstleisters „Schnuffi Escort Services“, der zunächst zur Altersverifikation von Herrn Primeur eine Kreditkartennummer verlangt. Aufgrund seiner Präferenzen, entscheidet sich John, die einzige Blondine im Angebot des Dienstleisters zu buchen. Sie stellt sich selber als die Inhaberin Schnuffi vor. Da John mit den dargestellten Konditionen sehr zufrieden ist, verabredet er sich in einer diskreten Bar. Um sich vor Ort zu finden, verwenden beide Facebook Places.

4.2 Exemplarische Probleme des aktuellen Szenarios

Während John Primeur in der Bar auf Schnuffi wartet wird er dort von Geschäftspartnern überrascht, die ihn über Facebook Places geortet hatten und spontan vorbeischauen. Als Schnuffi auftaucht und die beiden daraufhin peinlich berührt gehen wollen, betritt zudem ein ehemaliger Kunde von Schnuffi die Bar, der sie vor allen Personen lautstark beschimpft – auch er hatte Sie rein zufällig über Facebook Places geortet.

Da John Primeur sein dienstliches Notebook verwendet hat, haben seine Recherchen in Internet im firmeninternen Logging Spuren hinterlassen. Der Arbeitgeber von John Primeur verbietet in seiner IT-Policy explizit das aufrufen von Seiten mit erotischem Inhalt, was später zu einer Abmahnung oder sogar zu einer Kündigung führen kann.

Facebook hat durch die umfangreiche Suche eindeutige Hinweise für die Präferenzen von John Primeur erhalten und schaltet in Zukunft bei jedem Besuch von Facebook entsprechende Werbung in seinem Profil, was zu unangenehmen Fragen von Frau Primeur führt. Da Herr Primeur seinen Facebook-Account auch beruflich nutzt, werden so auch die Kollegen über seine Interessen informiert.

ISBN 978-3-88579-286-4

Da „Schnuffi“ nicht mit der Bezahlung von Herrn Primeur zufrieden war, ermittelt sie über Facebook seine Firma und seine Kontakte. Sie erpresst ihn mit der Drohung, Details über die Transaktion an seine beruflichen und privaten Kontakte weiterzugeben [19].

Ursprung der schlechten Bezahlung durch Herrn Primeur war jedoch, dass Schnuffi weder blond war, noch annähernd der gefälschten Fotos auf der Seite entsprach. Herr Primeur hatte jedoch keine Möglichkeit, die von ihr vorgegebene Identität im vorab zu überprüfen.

Der Dienstleister war zudem keine verlässliche Agentur. Die von Herrn Primeur als Altersverifkation verwendete Kreditkartennummer wird wenige Tage später in einschlägigen Foren verkauft.

In Rotland ist das Buchen von Escort-Services erst ab 21 Jahren erlaubt. Da Herr Primeur erst 20 ist, gab er gegenüber Schnuffi ein höheres Alter vor. Da sie seinen Ausweis nicht überprüfen konnte, machte sich Schnuffi dennoch strafbar, was die Polizei später anhand der Facebook-Logs ermitteln konnte..

Als Herr Primeur wieder zu Hause angekommen ist, findet sein Sohn zudem im Browser-Cache mehrere Dokumente, die er für die anstehende Taschengeldverhandlung nutzt.

4.3 Privatsphärenfreundliche Lösung

John Primeur ist auf Dienstreise in einer fremden Stadt und sucht nach weiblicher Begleitung für den Abend. Im Hotel benutzt er sein dienstliches Notebook, um über das dortige WLAN eine Internetverbindung aufzubauen. Allerdings startet John seinen Browser von einem extra hierfür angefertigten USB-Stick, der ein anonymes surfen mit TOR sowie eine Löschung der lokalen Cache-Daten gewährleistet („Porno-Modus“). Auf einer sichererern Community als Facebook (auf der technischen Grundlage von „Clique“ und „Scramble!“) sucht er nach einschlägigen Angeboten, und findet ein geeignetes Angebot des seriös erscheinenden Dienstleisters „schnuffi escort services“. Allerdings verraten die hier verwendeten Credentials John schnell, dass es sich bei dieser Agentur nur um Schnuffi handelt, die verschiedene Perücken trägt. Daher wählt John eine andere, seriöse Agentur. Aufgrund seiner einschlägigen Präferenzen, entscheidet sich John, die einzige Blondine im Angebot des Dienstleisters zu buchen. Da John mit den dargestellten Konditionen sehr zufrieden ist, verabredet man sich in einer diskreten Bar. Um sich vor Ort zu finden, verwenden beide einen speziellen Ortungsdienst, der eine feingranulare Zugriffskontrolle erlaubt.

ISBN 978-3-88579-286-4

5 Basistechnologien

Im Folgenden werden nun die Technologien genauer vorgestellt, die im privatsphärenfreundlichen Szenario eingesetzt werden und ihre Marktchancen diskutiert, die über das Beispielszenario hinaus vorhanden sind.

Tor: Anonymisierung ist eine essentielle Grundlage für jedes mehrseitig sichere Datenschutzsystem, da so ein hohes Schutzniveau hergestellt wird, von dem aus kontrolliert Identitätsattribute weitergegeben oder zurückgehalten werden können [10]. Während sich Tor bisher nur in Nischen durchgesetzt hat, bietet das hier dargestellte Szenario ein großes Potenzial, den Betreibern von Anonymisierungsknoten eine Rückgewinnung eines Teils ihrer Kosten zu ermöglichen [18]. In dem dargestellten Szenario entfaltet Tor insbesondere hinsichtlich des Arbeitgebers, aber auch z.B. gegenüber Hotelangestellten oder anderen Hotelgästen eine Schutzwirkung. Die anderen dargestellten Probleme können aber durch Anonymisierungsdienste alleine nicht adressiert werden. Über das dargestellte Szenario hinaus, sind die Marktchancen allerdings als eher kritisch zu bewerten, wie in [16] dargestellt.

Clique: Clique ist eine Erweiterung der Open Source Community Lösung Elgg, die es Teilnehmern ermöglicht ihre Kontakte zu gruppieren, und eine Zugriffskontrolle in Abhängigkeit von der Gruppenzugehörigkeit durchzuführen [12]. Clique und ähnliche Technologien können viele der dargestellten Datenschutzprobleme adressieren, insbesondere können unerwünschte Begegnungen mit Kollegen in der Freizeit oder mit ehemaligen Kunden vermieden werden. Allerdings kann durch die Angabe von Interessen die Pseudonymität der Nutzer kompromittiert werden. Ähnliches gilt für die direkte Begegnung, die durch den Verlauf der Dienstleistung notwendig ist. Über das hier dargestellte Szenario hinaus, sind auch hier die Marktchancen als schwierig zu bewerten, da gerade der Erfolg von Community-Lösungen sehr stark von der Anzahl der jeweiligen Mitglieder abhängig ist und somit Netzwerkeffekten unterliegt.

Idemix: Idemix bietet die Möglichkeit bestimmte Eigenschaften verbindlich zu zertifizieren und kann dabei trotzdem eine weitgehende Anonymität der Benutzer sicherstellen [2]. Innerhalb des vorgestellten Szenarios bietet Idemix die notwendige Grundlage für viele der datenschutzfreundlichen Lösungen. Insbesondere werden ein anonymer aber verbindlicher Altersnachweis sowie die Zertifizierung von datenschutzkritischen Attributen wie Gesundheitsdaten grundsätzliche vorstellbar. Über dieses Szenario hinaus, wurden bisher allerdings nur sehr eingeschränkt marktfähige Anwendungsszenarien wie anonymes Anmieten von Autos vorgestellt, so dass unklar bleibt, ob sich diese vielversprechende Datenschutzinfrastruktur auf die Dauer als tragfähig erweisen wird.

„Porno-Modus“ im Browser: Zunächst fällt am „Porno-Modus“ der ungewöhnliche Name auf. Dieser wurde nicht von den Anbietern der Browser vergeben. Es ist interessant zu beobachten, dass die Nutzer für diese erfolgreiche Datenschutztechnologie einen Namen aus diesem Genre gewählt haben. Durch diese Technologie werden im vorgestellten Szenario insbesondere die Zugriffe auf den Browser-Cache sowie die personalisierte Werbung unterbunden oder zumindest eingeschränkt. Die Technologie ist in allen aktuellen Browsern umgesetzt und hat somit eine sehr große Marktdurchdringung erreicht.

6 Diskussion

Ziel dieses Beitrags war es anhand eines offensichtlich überzeichneten Szenarios aufzuzeigen, welche Risiken für personenbezogene Daten in sozialen Netzwerken bestehen. Gleichzeitig zeigt sich, dass es durchaus möglich ist mit aktuell verfügbaren Technologien diese Probleme zu adressieren und eine Lösung zu schaffen, die eine privatsphärenfreundliche Bereitstellung der gleichen Funktionalität bietet. Das vorgestellte Szenario ist gleichzeitig äußerst marktrelevant und orientiert sich an aktuellen Entwicklungen im Bereich von Online-Communities. Insbesondere was den integrierten Einsatz verschiedener Datenschutztechnologien angeht bietet dieses Szenario ein großes Potenzial, da der Inhalt der Kommunikation einen besonders schützenswerten Bereich der Privatsphäre berührt. Somit kann dies den Grundstein für die Realisierung eines datenschutzfreundlichen und gleichzeitig tragfähigen Gesamtsystems bilden. Empirische Studien haben gezeigt, dass sowohl die Bereitschaft zum Einsatz von datenschutzfreundlichen Technologien als auch die Zahlungsbereitschaft in dem hier vorgestellten Anwendungsfall besonders hoch sind.

Allerdings zeigt unsere Analyse, dass die Marktchancen für die einzelnen Technologien über das Anwendungsszenario hinaus größtenteils als schwierig bis kritisch einzuschätzen sind. Das häufig bemühte Paradigma des technischen Selbstdatenschutzes [9] setzt aber zwingend voraus, dass Benutzer die Werkzeuge im täglichen Gebrauch einsetzen, um sich mit ihnen vertraut zu machen. Dafür sind aber relevante Anwendungsfälle nötig, die in anderen Bereichen nur schwer zu finden sind.

Literaturverzeichnis

[1] Boyd, D. (2008) Facebook’s Privacy Trainwreck: Exposure, Invasion, and Social Convergence, *Convergence: The International Journal of Research into New Media Technologies*, 14, 1, 13-20.

[2] Camenisch, J. and Van Herreweghen, E. (2002) Design and Implementation of the idemix Anonymous Credential System, *Proceedings of the 9th ACM Conference on Computer and Communications Security (ACM CCS'02)*, Washington, D.C:, ACM, 21-30.

[3] Carroll, J. M. (2000) Five Reasons for Scenario-based Design, *Interacting with Computers*, 13, 43-60.

[4] Facebook (2010) Statistics, *http://www.facebook.com/press/info.php?statistics*, accessed 2010-11-30.

[5] Facebook (2011) Places, *http://www.facebook.com/places/*, accessed 2011-05-16.
[6] Feigenbaum, J., Freedman, M., Sander, T. and Shostack, A. (2002) Economic barriers to the deployment of existing privacy technology: Proceedings of the Workshop on Economics and Information Security, Berkley, CA.
[7] Foursquare (2011) Foursquare, *https://de.foursquare.com/*, accessed 2011-05-16.
[8] Google (2011) Latitude, *http://www.google.de/latitude*, accessed 2011-05-16.
[10] Hansen, M., Berlich, P., Camenisch, J., Clauß, S., Pfitzmann, A. and Waidner, M. (2004) Privacy Enhancing Identity Management, *Information Security Technical Report*, 9, 1, 35-44.
[9] Hansen, M. and Krause, C. (2003) Technische Möglichkeiten des Selbstdatenschutzes, *Stiftungstagung „Technik für Nutzer“*, 16.5., Stuttgart.
[11] Hevner, A. R., March, S. T., Park, J. and Ram, S. (2004) Design Science in Information Systems Research, *MIS Quaterly*, 28, 1, 75-105.
[12] Holtz, L. (2010) Datenschutzkonformes Social Networking: Clique und Scramble!, *Datenschutz und Datensicherheit (DuD)*, 7, 439-443.
[13] Ihlenfeld, J. (2011) Sicherheitslücke: Werbekunden konnten auf Facebook-Nutzerdaten zugreifen, *Handelsblatt*, 11.05.2011.
[14] Post-Privacy-Spackeria (2011) Privatsphäre – warum die Netzkommunity naiv ist. http://blog.spackeria.org/2011/04/10/privatsphare-warum-die-netzcommunity-naiv-ist/, 10. April 2011
[15] Rosenblum, D. (2007) What Anyone Can Know: The Privacy Risks of Social Networking Sites, *IEEE Security & Privacy*, 5, 40-49.
[16] Roßnagel, H. (2010) The market failure of anonymity services, in P. Samarati, M. Tunstall and J. Posegga (Eds.), *Information Security Theory and Practice. Security and Privacy of Pervasive Systems and Smart Devices*, 2010-04-12-14, Springer, Berlin Heidelberg, 340-355.
[17] Roßnagel, H. and Zibuschka, J. (2010) Tragfähige IT-Sicherheitslösungen, *digma. Zeitschrift für Datenrecht und Informationssicherheit*, 10, 2, 68-72.
[18] Roßnagel, H., Zibuschka, J., Pimenidis, L. and Deselaers, T. (2009) Facilitating the Adoption of Tor by Focusing on a Promising Target Group, *Identity and Privacy in the Internet Age - Proceedings of the 14th Nordic Workshop on Secure IT Systems (NordSec 2009)*, 14th-16th October, Oslo, Norway, 15-27.
[19] Siebers, W. (2007) Heisse Hure mit heisser Rache - Internetpranger für nicht erschienene Freier, *http://strafprozess.blogspot.com/2007/06/heisse-hure-mit-heisser-rache.html*.
[20] Stiftung Warentest (2010) Ungeschützt: Datenschutz bei Onlinenetzwerken, test 4.
[21] Tetard, F., Patokorpi, E. and Kadyte, V. (2004) User-Centred Design of Mobile Services for Tourists: A Case Study on Student Work on Mobile Design, *Mobile Information Systems: IFIP TC8 Working Conference on Mobilie Information Systems (Mobis)*, Oslo, Springer, 155-168.
[22] The Huffington Post (2010) Twitter User Statistics REVEALED, *http://www.huffingtonpost.com/2010/04/14/twitter-user-statistics-r_n_537992.html*, accessed 2010-11-30.
[23] Venkatesh, S. (2011) How Tech Tools Transformed New York's Sex Trade, *Wired*, 19.02.2011.