Diplomarbeit

zur Erlangung des akademischen Grades
Master of Science in Engineering

Datenschutz und Informationssicherheit in Social Communities

ausgeführt von

Johannes Nagl, BSc
Dr.-Vogl-Gasse 37, 3400 Klosterneuburg

Begutachter/innen:

1. Begutachter/in: FH-Prof. DI Alexander Mense
2. Begutachter/in: DI Dr. Gerd Holweg

Klosterneuburg, 14.05.2008

Ausgeführt an der Fachhochschule Technikum Wien
Studiengang Multimedia und Softwareentwicklung

FACHHOCHSCHULE
TECHNIKUM WIEN

Kurzfassung

Die vorliegende Diplomarbeit beschreibt das Spannungsfeld zwischen Datenschutz, Informationssicherheit und Social Communities. Der Wert eines sozialen Netzwerks steigt mit dessen Informationsgehalt und der Benutzeranzahl. Dadurch verstärken sich jedoch ebenfalls die datenschutzrechtlichen Probleme.

Die Arbeit beleuchtet die erfolgreichsten Communities im Internet und zeigt, wie stark die Bemühungen rund um den Datenschutz auf den jeweiligen Plattformen variieren können. Hierzu wurden fünf ausgewählte Community-Anbieter analysiert und miteinander verglichen. Ziel ist es, Benutzer über die Gefahren der Teilnahme aufzuklären und für vermehrten Selbstschutz zu sensibilisieren. Eine durchgeführte Umfrage unter Benutzern von Communities zeigt, ob diese beim Veröffentlichen ihrer Daten über Datenschutz nachdenken und diesen berücksichtigen. Dabei wird analysiert, inwieweit Vorwissen über das Thema das Nutzungsverhalten verändert. Die Ergebnisse des Vergleichs und der Umfrage werden Experten vorgelegt und abschließend diskutiert.

Das Ergebnis der Diplomarbeit ist eine Momentaufnahme der Internetkultur, die zeigt, dass Datenschutz und Informationssicherheit in verschiedenen Social Communities sehr unterschiedlich behandelt werden. Benutzer des *Social Web*[1] machen sich Gedanken über Datenschutz, verstehen darunter jedoch nicht das gleiche wie Betreiber der Plattformen.

Abstract

This master thesis deals with privacy and data protection issues arising in social communities in the internet. Together with the usage of social websites, the amount of stored information rises tremendously, which leads to an intensification of privacy-related problems.

In the theoretical part, the legal conditions as well as the steady growth of the communities are examined. In the practical section however the author analyses five selected communities and their management of privacy. A survey among users of social communities shows whether users are interested in privacy related topics and if there is a significant cohesion between their previous knowledge and the extent to which sensitive features of communities are used. In the final part of the thesis experts in legal, technical and social aspects of social communities will comment on the results of the comparison and the survey.

Schlagwörter

Internet, Social Communities, Social Networks, soziale Netze, Social Web, Datenschutz, Privacy, Datensicherheit, Informationssicherheit, Privatsphäre, Web2.0, MySpace, Facebook, studiVZ, Kaioo, Diplomarbeit, Data Protection, IT-Sicherheit, Information Security

[1] Synonym für den Begriff Web2.0, der im Kapitel 3.2 erklärt wird.

Eidesstattliche Erklärung

„Ich erkläre hiermit an Eides Statt, dass ich die vorliegende Arbeit selbständig angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Die Arbeit wurde bisher weder in gleicher noch in ähnlicher Form einer anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht."

Klosterneuburg, 14.05.2008

Danksagung

Die vorliegende Arbeit und die damit verbundene Abschlussprüfung beenden einen wichtigen Lebensabschnitt. Die letzten vier Jahre haben sehr viel in Bezug auf mein Wissen, Können, Denken und Handeln verändert. Danke an alle Vortragenden, Studienkollegen, Sekretärinnen und Kontakte, die ich innerhalb dieser Zeit knüpfen durfte. Mein (soziales) Netzwerk ist durch die Fachhochschule extrem gewachsen und ich hoffe, dass ich mit dieser Arbeit viel an das Netzwerk zurückgeben kann. Ich würde mich daher freuen, wenn wir auch in Zukunft, nicht nur virtuell, in Kontakt bleiben und man sich hie und da auf einen Kakao trifft.

In Bezug auf diese Arbeit möchte ich mich stellvertretend für alle Helfer bei Personen bedanken, die mich tatkräftig bei der täglichen Arbeit unterstützt haben, damit die Umfrage, sowie die inhaltlichen Ausführungen noch aussagekräftiger wurden. S, danke bei der produktiven Hilfe rund um die Themenfindung. M, ohne deine Veröffentlichung auf deinem Blog, wäre die Umfrage wohl weitaus kleiner ausgefallen. H, dein wildes Posten in Foren war großartig. M, danke für die Corporate Communications, obwohl es doch gar kein Unternehmen war! T und M für die Hilfe bei der Erstellung der Umfrage und der relevanten Fragen. J, danke für das letztmalige Pushen der Umfrage zur re:publica 2008. Desweiteren möchte ich mich bei allen Teilnehmern an der Umfrage, sowie der Experteninterviews bedanken.

Ebenfalls möchte ich auch ein großes Dankeschön an meine Betreuer richten, die hilfsbereit zur Seite standen und mich dennoch selbstständig arbeiten ließen. Danke für die Betreuung!

Zuletzt möchte ich mich bei einer Person bedanken, die bereits seit vielen Jahren ein wichtiger Bestandteil meines Lebens ist und mir Tag täglich viele glückliche Momente bereitet. Danke für deine Hilfestellungen, deine Unterstützung und für deine liebenswerte Art. Du bist die Beste - K! Danke für die letzten 8 Jahre.

Der Autor möchte hier auch noch die Chance nutzen und allen Lesern 3 Werkzeuge ans Herz legen, die beim Schreiben einer ausführlichen Arbeit nicht fehlen sollten:

SVN: Gedacht als Versionierungshilfe in der Programmierung ist es ebenfalls hervorragend als Sicherungs- und Synchronisierungslösung geeignet, wenn auf mehreren Computern gearbeitet wird. USB-Sticks mit den falschen Datenbeständen gehören somit der Vergangenheit an. (http://subversion.tigris.org/)

Last.FM: Musik, Musik, Musik. „The Long Tail" in seiner besten Form. Der Autor empfiehlt "Progressive Rock". Auf den Datenschutz ist zu achten. (http://last.fm/)

Delicious: Ideal, wenn man auf mehreren Computer die gleichen Favoriten haben möchte. Mit dem entsprechenden Plugin für Firefox ideal zum schnellen Beschlagworten von Literaturquellen. Auf den Datenschutz ist zu achten. (http://del.icio.us/)

Inhaltsverzeichnis

Die Bezeichnungen sollen immer geschlechtsneutral verstanden werden.

1. Problem- und Aufgabenstellung

Die Wachstumszahlen von beliebten Communities im Web verdeutlichen: Das Partizipieren in sozialen Plattformen im Internet wird stetig beliebter (vgl. Göldi, 2008). Vor allem junge Menschen berichten ausführlich über ihr Leben in Communities, laden Fotos hoch, oder treten Gruppen bei, um gleichdenkende Personen kennenzulernen (vgl. CSCM, 2008). Experten sind sich bereits jetzt einig: Social Communities besitzen mehr Daten über ihre Benutzer, als Geheimdienstorganisationen jemals erlangen könnten. Themen wie Privatsphäre, Datenschutz und Informationssicherheit wurden jedoch sowohl von Betreibern als auch von Benutzern lange Zeit sehr stiefmütterlich behandelt. Dabei sind diese Themen angesichts der gespeicherten Datenmengen zentrale Themen. Eine vom Autor aufgestellte These zeigt eine mögliche Zwickmühle der Betreiber:

Je schärfer Datenschutz auf der Plattform gehandhabt wird, desto weniger Inhalt wird von den Benutzern erstellt. Communities, die sich jedoch ausschließlich über die Inhalte, die durch Benutzer erstellt werden, definieren, verlieren jedoch an Wert und Attraktivität für potentielle Investoren. Denn je mehr Inhalte eine Plattform bietet, desto attraktiver ist sie für Werbepartner oder Investoren. Datenschutz reduziert sich daher oftmals auf lückenhafte Informationssicherheit und Benutzer werden mit ihren Problemen alleine gelassen. Schlimmer noch: Informationen, die in Webdiensten gespeichert werden, können in manchen Fällen erst gar nicht mehr gelöscht werden. (s. Kapitel 4.1.4.1). Nach einiger Zeit kommt das böse Erwachen, wenn Fotos oder intime Einzelheiten aus dem Leben von Benutzern im Internet auftauchen. Darüberhinaus kämpfen Webseitenbetreiber mit Sicherheitslücken in den Systemen, die es unbefugten Dritten erlauben, Datenbestände einzusehen, obwohl diese nicht für die Öffentlichkeit bestimmt sind. Entgegen der Wünsche von Benutzern werden dafür neue Funktionen entwickelt, die weitere datenschutzrechtliche Probleme aufwerfen und das gegenseitige „Stalking“ in den Netzen forcieren.

Da der Autor selbst bereits seit vielen Jahren in sozialen Netzen aktiv ist und in seinen bisherigen Seminar- und Bachelor-Arbeiten über Internetthemen auf den fehlenden Datenschutz hingewiesen hat, bildet die vorliegende Diplomarbeit den idealen Rahmen, um die Vorkommnisse der letzten Monate in Bezug auf neue sowie erfolgreiche Plattformen zu analysieren und allen anderen Benutzern eine erweiterte und durchaus kritische Sicht auf die Nutzung zu ermöglichen. Um einen ganzheitlichen Blick auf das Thema werfen zu können, werden daher Communities **und** Benutzer analysiert. Dabei werden folgende Fragestellungen geklärt:

- Durch welche Merkmale unterscheiden sich einzelne Communities im Bezug auf den gelebten Datenschutz und die Sicherheit innerhalb der Plattform?
- Sind Benutzer über die Gefahren der Bekanntgabe ihrer privaten Daten aufgeklärt?
- Welche der involvierten Parteien bei der Veröffentlichung von Daten ist am maßgeblichsten für die Wahrung des Datenschutzes verantwortlich?
- Trägt das rasante Anwachsen der Social Communities in den letzten Jahren zur Entwicklung von neuen Datenschutzmaßnahmen bei oder gefährdet es den Schutz von Daten der Benutzer?

2. Einleitung

Die vorliegende Arbeit richtet sich an alle (zukünftigen) Benutzer von partizipativen Internetdiensten. Es werden vor allem nicht-technische Themen beleuchtet, die mit dem Datenschutz in Verbindung stehen oder für das Verständnis der behandelten Fragestellungen notwendig sind. Die Arbeit geht dabei nicht zu sehr in technische Details, damit Benutzer erkennen: Datenschutz und Informationssicherheit sind keine technischen, sondern volkswirtschaftliche und soziale Themen, die von jedem der Benutzer verstanden und gelebt werden müssen. Um die bisher aufgetretenen Probleme von Web Diensten erklären zu können muss dennoch auf die technischen Angriffs- und Abwehrszenarien eingegangen werden um Grundlagen für das Verständnis dieser Angriffe zu schaffen.

Im Kapitel 3 der Arbeit werden theoretische Grundlagen zu Datenschutz und Social Communities erklärt und definiert. Das Kapitel ist in Trichterform aufgebaut, dh dass die allgemeingültigen Aussagen im Laufe des Kapitels immer weiter auf die konkrete Anwendung in Social Communities eingegrenzt werden. Personen, die bereits Verständnis über Datenschutz haben, sei das gleichnamige Kapitel dennoch ans Herz gelegt. Das vom Autor eigens aufgestellte *Datenpyramiden*-Modell zeigt dabei die Zusammenhänge der Themengebiete deutlich auf. Da die verschiedenen Definitionen des Begriffs zu oftmaliger Verwirrung führen, werden Begrifflichkeiten daher für den Rahmen der Arbeit definiert.

Als Praxisteil der Arbeit wird in Kapitel 4 der Umgang mit Daten in Social Communities näher betrachtet. Eine Analyse und der Vergleich von fünf ausgewählten Plattformen zeigen Unterschiede im Umgang des Datenschutzes und der Informationssicherheit. Dabei wird nicht nur die Plattform an sich, sondern auch auf das Umfeld der Betreiber überprüft. Um eine Aussage über den Wissensstand bei Benutzern von Social Web Diensten treffen zu können, wurde eine Umfrage unter deutschsprachigen Internet-Benutzern durchgeführt. Die Ergebnisse dieser Umfrage, sowie des zuvor durchgeführten Vergleichs werden abschließend in einer Expertenrunde, bestehend aus einem Internet, einem Social Community und einem Rechtsexperten besprochen.

Das Fazit der Arbeit beinhaltet ein Resümee des praktischen Teils sowie Richtlinien für Benutzer sozialer Netze in Bezug auf Datenschutz und Informationssicherheit. Nachdem die Fragestellungen, die sich aus der Problemstellung ergeben haben, im Fazit geklärt werden, beinhält die Diskussion weitere Bedrohungsszenarien und einen Einblick in die Branche. Abschließend wagt der Autor einen Ausblick in die Zukunft von Social Communities, in der sich die Netzwerke im Internet durch die übermäßige Partizipation ihrer Benutzer nachhaltig verändern und selbst regulieren werden.

Während der Arbeit an der Master Thesis haben sich die Pressemitteilungen und Blogbeiträge über Social Communities überschlagen. Das Jahr 2008 wird ein entscheidendes Jahr für Plattformen und deren Positionierungen werden. Die große Konsolidierungsphase hat noch nicht begonnen. Die vereinzelten Aufkäufe von Netzen wie MySpace, Bebo oder eine geplante Übernahme von Yahoo durch Microsoft[2], die den Eigentümerwechsel von zahlreichen Social Web Diensten zur Folge hätte, zeigen jedoch, wohin der Weg führt. Die vorliegende Arbeit kann daher nur eine Momentaufnahme darstellen und für kommende Arbeiten als Basis dienen.

[2] Die Übernahme platzte kurze Zeit vor Beendigung der Arbeit. Eine Übernahme von Facebook durch Microsoft steht aktuell im Raum.

3. Theoretische Grundlagen

Datenschutz und Informationssicherheit sind komplexe und kontroverselle Themen, die alle Internetbenutzer und Betreiber von Webangeboten betreffen. Jeder von uns ist täglich mit diesen Themen konfrontiert, ob er es möchte oder nicht. Wer sich in das World Wide Web einwählt um Informationen zu suchen, Waren zu bestellen oder in *Social Communities* zu kommunizieren, wird in einer Vielzahl an Systemen erfasst. Daten werden auf dem eigenen PC (zwischen-)gespeichert, der Internetanbieter speichert die Sitzungsdaten und durch die technischen Eigenschaften des Internets wird jeder Seitenaufruf eindeutig zuweisbar gespeichert. Der Berg an Daten, die bei den vielen beteiligten Stellen anfallen, ist enorm. Um die Gefahren und Risiken, die im Internet lauern, praktisch erläutern und analysieren zu können, ist es daher im ersten Teil dieser Arbeit notwendig, grundlegende Begriffe zu definieren, die für den weiteren Verlauf der Arbeit zwingend notwendig sind. Deswegen werden Begrifflichkeiten erklärt und falls notwendig für den Rahmen der Arbeit eindeutig festgelegt. Die zwei großen Themenkomplexe, die in dieser Arbeit näher beleuchtet werden, sind der Datenschutz im Internet, sowie die Definition von Social Communities und eine Analyse deren besonderer Merkmale und Vermarktungsstrategien.

3.1. Datenschutz und Informationssicherheit

In der Literatur gibt es viele verschiedene Definitionen für die Begriffe Datenschutz und Informationssicherheit. Nicht nur die Definitionen sondern auch Übersetzungsprobleme zeigen, worauf es in diesem Zusammenhang ankommt. Das englische Wort „Privacy“ kann mit „Datenschutz“ wie auch mit „Privatsphäre“ übersetzt werden. Datenschutz wiederum als „privacy“, „data privacy“ oder „data security“. Eine allgemein gültige Definition gibt es daher nicht. Einzelne Staaten verabschieden Datenschutzbestimmungen; diese auf geltende Bestimmungen anderer Länder umzumünzen fällt ebenfalls schwer. Zu groß ist die Unschärfe alleine beim Übersetzen der einzelnen Fachtermini.

3.1.1. Datenschutz

Drews et al (1993, S. 88) definieren den deutschen Datenschutz in zwei Größen, nämlich im engeren und im weiteren Sinne:

> *„Datenschutz ist im engeren Sinne gemäß Bundesdatenschutzgesetz die Aufgabe, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird; Ist im weiteren Sinne die Aufgabe, durch den Schutz der Daten vor Mißbrauch in ihren Verarbeitungsphasen der Beeinträchtigung fremder und eigener schutzwürdiger Belange zu begegnen.“*

Datenschutz ist laut obiger Definition eine Tätigkeit, die durch das Gesetz einzelne Personen davor schützt ihren zustehenden Persönlichkeitsrechten beraubt zu werden. Darüberhinaus definieren Drews *et al*, dass Daten in jeder Phase vor Missbrauch geschützt werden müssen.

8 Jahre später definierten Müller und Reichenbach den „neuen Datenschutz“ (2001, S. 193) wie folgt:

> *„Zum klassischen Schutz der individuellen Privatsphäre im Sinne der Verwirklichung der informationellen Selbstbestimmung tritt untrennbar sowohl die notwendige Berücksichtigung der kommunikativen Autonomie aller an der elektronischen Kommuni-*

> *kation Beteiligten als auch die notwendige Gewährleistung einer hinreichenden technischen Datensicherheit als Grundvoraussetzung hinzu […] Die erfolgreiche Erfüllung aller Aufgaben hängt dabei zunehmend von der Realisierung der vier wichtigsten informationstechnischen Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Zurechenbarkeit ab, d.h. der technologisch auszuschließenden unbefugten Kenntnisnahme Dritte sowie unbefugter Veränderung der Daten, der bedarfsnahen Zugänglichkeit relevanter Informationen und der im – autorisierten – Bedarfsfall möglichen Identifikation der kommunizierenden Nutzer."*

Müller und Reichenbach erweitern den definierten Datenschutz um die Gewährleistung der Datensicherung und Autonomie aller Beteiligten. Vier Grundziele (Vertraulichkeit, Integrität, Verfügbarkeit und Zurechenbarkeit) werden erkannt und mit dem Thema „Datensicherheit" in Verbindung gebracht. Die beiden Autoren sind der Meinung, dass ein völlig nahtloser Datenschutz in komplexen Netzwerken, wie es das Internet zweifelsohne darstellt, nicht erreicht werden kann.

> *„Das zunehmende Aufkommen personenbezogener Daten, die Dezentralisierung der Datenerhebung und die Dezentralisierung der Datenverarbeitung in komplexen Netzwerken macht allein die Feststellung sämtlicher potentiell sensibler Verarbeitungsprozesse unmöglich, von einer wirkungsvollen Aufsicht oder Kontrolle ganz zu schweigen"* (Müller & Reichenbach, 2001, S. 191)

Es muss daher noch zusätzliche Maßnahmen geben, damit Persönlichkeitsrechte gewahrt bleiben können. Demnach müssen Firmen nicht Datenschutzbestimmungen beachten, sondern müssen darauf aufbauend eigene Mechanismen zur Abwehr von unbefugten Dritten schaffen. Die rechtmäßige Verwendung und die Informationspflicht des Nutzers stellt Steiner (2006, S. 47f) in den Mittelpunkt von Datenschutz:

> *„Personenbezogene Daten dürfen aber nur genutzt werden, wenn gesetzliche Vorschriften dies zulassen oder der Betroffene ausdrücklich eingewilligt hat, und zwar in schriftlicher Form. Im Internet wird häufig eine elektronische Einwilligung angefordert, z.B. durch das Anklicken eines Buttons. Personenbezogenen [sic] Daten müssen nach ihrer Nutzung gelöscht werden […]. Außerdem muss der Nutzer darüber informiert werden, welche Daten zu welchem Zweck gespeichert wurden. Wenn etwa Daten zur Erstellung eines Nutzerprofils oder im Rahmen einer Untersuchung gespeichert wurden, muss dem Nutzer dies mitgeteilt werden."*

Der Vergleich mit einer englischsprachigen Variante der Definition von Datenschutz, bzw. Privacy zeigt eine deutlich andere Herangehensweise: Fischer-Hübner (2001, S. 10-11) beschreibt sechs Themenblöcke als *Basic Privacy Principles*, die dem Begriff Privacy zugrunde liegen:

> *"Principle of lawfulness and fairness*
> *Principle of the purpose specification and purpose binding (also called purpose limitation)*
> *Principle of necessity of data collection and processing*
> *Information, notification and access rights of the data subjects*
> *Principle of security and accuracy*
> *Supervision and sanctions"*

Die angesprochenen Prinzipien beinhalten Fairness beim Speichern der Daten, das Überlegen, ob Daten tatsächlich gespeichert werden müssen, die Sicherheit gegen Angriffe unbefugter Dritter und die Supervision der angewandten Methoden durch eine dafür vorgesehene Person. Die definierten Prinzipien bieten einen guten Überblick über das Thema. Ob allerdings Fairness und Sorgfalt 100%ig definierbar sind, ist fraglich.

Herr Sterbik-Lamina ergänzt in einem Interview mit derStandard (2008a):

> *"Personenbezogene Daten unterliegen laut dem österreichischen Datenschutzgesetz einem besonderen Schutz. […] Jeder kann im Grunde selbst darüber bestimmen, welche Informationen er öffentlich preisgeben will. Die Praxis zeigt, dass mit sensiblen Daten sehr freizügig umgegangen wird. […] Hat ein User sich erst einmal für diesen Schritt entschieden, könne er auch nicht mehr nach Datenschutz verlangen. "*

Benutzer sind in sozialen Netzen selbst dafür verantwortlich, welche Informationen veröffentlicht werden. Zusammenfassend definiert der Autor Datenschutz in Bezug auf Social Communities daher als *Aufgabe des Betreibers, dafür zu sorgen, dass Benutzer und deren personenbezogene Daten in jeder Phase ihrer Verarbeitung vor Missbrauch geschützt werden.* Daten von Benutzern dürfen nur dann für eigene Zwecke benutzt werden, wenn dies ausdrücklich vom Benutzer zugestimmt wurde. Sowohl Betreiber als auch Benutzer müssen die Möglichkeit der jederzeitigen Kündigung der Vereinbarung haben, die eine komplette Löschung aller vom Benutzer eingegebenen Daten nach sich zieht. Es muss ebenfalls zu jedem Zeitpunkt der Mitgliedschaft die Möglichkeit zur Auflistung aller bisher publizierten Daten, sowie die Möglichkeit der vollständigen Löschung, ohne die Mitgliedschaft beenden zu müssen, geben.

3.1.2. Informationssicherheit

Informationssicherheit, auch Daten- oder IT-Sicherheit genannt wird oftmals als die „technische Seite“ von Datenschutz beschrieben. (vgl. Fischer-Hübner, 2001, S. 35) Es kann sich dabei um einen Zustand sowie um Vorkehrungen oder Maßnahmen handeln. *„IT Sicherheit ist zunächst einmal ein Zustand und wird im Allgemeinen als die Abwesenheit von Sicherheitslücken verstanden.“* (vgl. Schoolmann & Rieger, 2005, S. 23.). Die Abwesenheit von Sicherheitslücken kann nur dann festgestellt werden, wenn Systeme regelmäßig überprüft werden. Die Informationssicherheit kann nicht allgemeingültig definiert werden, deswegen ist der Fokus auf ein spezielles Interessensgebiet zwingend notwendig:

„Die Grundeigenschaften sind allerdings keine absoluten Werte. Bedeutet zum Beispiel „meine Daten sind sicher“, dass die Daten immer rund um die Uhr zugreifbar sein müssen? […] Der Zustand „IT-Sicherheit“ muss also für jedes Unternehmen und jedes verwendete IT-System spezifisch festgelegt werden.“ (Schoolmann & Rieger, 2005, S. 26)

Bemühungen um das Fehlen von Sicherheitslücken gewährleisten zu können hängen daher stark von dem Einsatzzweck ab. Wie bereits im Kapitel Datenschutz erwähnt, gibt es drei (bzw. vier) Regeln der Datensicherheit:

> *„Ziel bzw. Ergebnis aller Vorkehrungen und Maßnahmen um einen Zustand zu erreichen, in dem Informationen geschützt sind vor dem Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit. Dies bedeutet, daß Informationen zu schützen sind bei der Erhebung, der Erfassung, der Bearbeitung, der Speicherung und der sonstigen Verarbeitung.“* (Drews et al, 1993, S. 148)

Unter Informationssicherheit in Social Communities versteht der Autor jene Tätigkeiten, die vor, während und nach der Eingabe von personenbezogenen Daten durch den Benutzer notwendig sind, damit die verarbeiteten Daten jederzeit den Grundsätzen der Vertraulichkeit, Integrität, Verfügbarkeit und Zurechenbarkeit entsprechen. Diese Maßnahmen beinhalten ebenso die Verweigerung von Funktionen auf der Plattform, bei denen eine allgemeingültige Sicherheit nicht garantieren werden kann. Alle Maßnahmen, die zur Informationssicherheit (bzw. IT-Sicherheit) beitragen und diese laufend überwachen, müssen dokumentiert und in regelmäßigen Abständen an den Datenschutzbeauftragten übergeben werden.

3.1.3. Das “Datenpyramide”-Modell

Die vom Autor definierte „Datenpyramide“ (siehe Abbildung 1) verdeutlicht die Zusammenhänge und die Schichtenwirkung visuell. Die zwei eingefärbten Bereiche der Pyramide zeigen die passiven Maßnahmen, die Betreiber setzen können, um Schutz auf der Plattform gewährleisten zu können. Der dritte Teil der Pyramide steht für die Bemühungen der Betreiber sich selbst durch technische Vorkehrungen schützen zu wollen.

Der Datenschutz stellt die rechtliche Grundlage für die Speicherung von Daten dar. Er grenzt weitläufig „ungesetzmäßige“ Handlungen durch Benutzer und Betreiber der Plattform aus und stellt einen verbindlichen Vertrag zwischen den involvierten Parteien dar. Der Verlass auf den Datenschutz ist jedoch nicht genug. Da sich nicht alle Personen an gültiges Recht handeln, bzw. internationale Unterschiede in der Rechtssprechung existieren, versucht die Informationssicherheit offene „Schlupflöcher“ für Angreifer durch technische Maßnahmen weitestgehend zu schließen. Informationssicherheit wird hierbei als Prozess definiert. Ein sogenannter Selbstschutz (vgl. „Hausverstand“) dient dem Benutzer sinnvolle Entscheidungen in Bezug auf Datenschutz zu treffen. Fragestellungen wie „Soll ich dieses Foto ins Netz stellen? Soll ich diese Angabe über mich treffen? Soll ich wirklich auf diesen Link klicken?“ stehen im Mittelpunkt des Selbstschutzes, der eine aktive Maßnahme darstellt.

Prinzipiell kann das Datenpyramide-Modell aus zwei verschiedenen Ansichten betrachtet werden. Die Variante 1 des Modells sieht als Basis und größten Teil der Pyramide einen (gesetzlich) definierten Rahmen, in dem das Handeln von Personengruppen definiert wird. Webangebote müssen also gesetzlichen Auflagen entsprechen und diese einhalten. Datenschutz ist ausführlich spezifiziert und wird eingehalten. Die Bemühungen der Betreiber sind so groß, dass ein Selbstschutz in diesem Falle höchstens sekundär ist. Die Gesetzgebung und der Betreiber sind daher größtenteils für den Schutz der Daten verantwortlich.
Variante 2 hingegen sieht den Selbstschutz durch den Benutzer selbst als wichtigstes Glied in der Datenpyramide an. Die Grundüberlegung ist: Daten, die nicht publiziert werden, benötigen auch keine Sicherheitsvorkehrungen und gesetzliche Schutzbestimmungen. Daher spielt es eine entscheidende Rolle, wie Benutzer selbst über Sicherheitsthemen informiert sind. Im Gegensatz zu Variante 1 spielt der Datenschutz eine untergeordnete Rolle, da Benutzer vor dem Publizieren von Daten über die Folgen nachdenken und nur wenig personenbezogene Daten Preis geben. Selbst- bzw. Datenschutz alleine helfen jedoch nicht, denn:

Parry Aftab (zitiert in Poulsen 2008a): "*If kids are doing what they think they need to do, and are still having their photos picked up by slimebags on the internet ... then these are serious issues […]*". Daher wurde die Pyramide als Modell gewählt. Die Grafik verdeutlicht: Egal wie man das Bild betrachtet: Informationssicherheit ist immer ein zentrales Thema, das nicht vernachlässigt werden darf. Daher müssen in jedem Fall die Bemühungen um Vertraulichkeit und Integrität gleich hoch angesetzt werden.

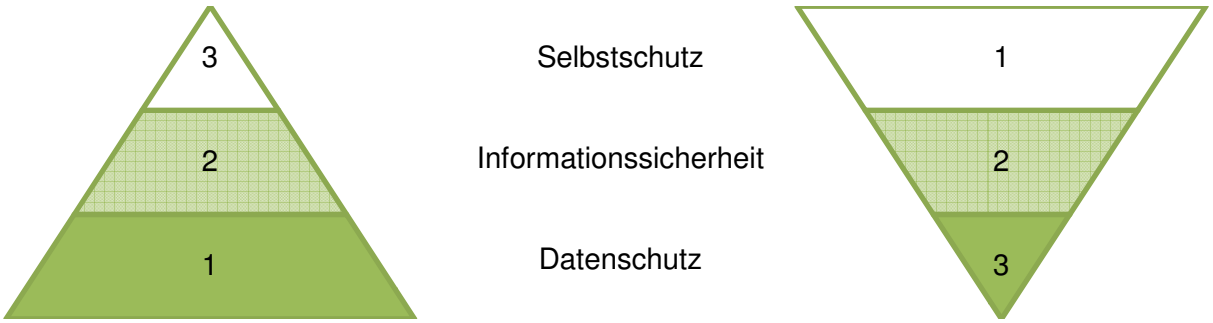

Abbildung 1: Das Modell der Datenpyramide nach Nagl, Variante 1 und 2

3.1.4. Der gläserne Mensch

Durch mangelhaften Datenschutz und fehlende Privatsphäre wird in der Literatur oftmals von dem „gläsernen Menschen“ gesprochen. Staatliche Kontrollstellen haben auf Kreditkarteninformationen, Krankenstandsdaten und Steuerzahlungen Zugriff (vgl. Agarwala, 2006). Durch die breite Verfügbarkeit von sozialen Netzen und der darin gespeicherten Daten eröffnen sich Überwachungsmöglichkeiten für jedermann. Dazu meint Jana Herwig in einem Interview des Standards (2008a):

> *"Wir haben es hier mit einem Grunddilemma zu tun", stellte Jana Herwig, Medienwissenschaftlerin mit Schwerpunkt user generated content, einleitend fest. "Einerseits befinden wir uns in einer aktuellen Situation, in der sich die Menschen zunehmend Sorgen um ihre Privatsphäre machen. Andererseits stellen wir aber auch fest, dass die Bereitschaft der Nutzer, persönliche Informationen im Internet preis [sic] zu geben, weiter steigt […] Hier kommen soziale Funktionen zum Einsatz, die durchaus Sinn machen. Gleichzeitig werden dadurch allerdings sensible Stammdaten berührt, die es ermöglichen, einen Menschen eindeutig zu identifizieren"*

Die beiden folgenden Beispiele zeigen, in wie weit es heute möglich ist, durch die aktive Mithelfe von allen Benutzern sozialer Netze gläserne Menschen in unserer Gesellschaft zu erschaffen. War es früher notwendig, im Freundes- und Verwandtenkreis von Personen über Einzelheiten zu recherchieren, genügt heute ein Blick ins Internet und die Social Communities. Rasch hat man ein Profil auf MySpace, Facebook oder studiVZ gefunden und hat mit etwas Glück Informationen, die weit über konventionelle Rechercheergebnisse hinausgehen – und diese aus erster Hand. Fotos, Freunde, Profildaten, Kontaktadressen, alles auf einen Blick. (vgl. derStandard, 2008b)

> „*Weil Millionen von Menschen ihre privatesten Details im Internet ausbreiten, hat die Bild-Zeitung ihre zuverlässigsten Informanten entdeckt: die Opfer selbst. […] Das Schönste daran: Die Nutzer stellen ihre privaten Vorlieben auch noch freiwillig ins Netz. […] Eine Tatsache, die sich die Bild-Zeitung schamlos zu Nutze macht. Als Anfang März in Hamburg beinahe eine Lufthansa-Maschine abgestürzt wäre, "enthüllte" Bild "das traurige Geheimnis der schönen Pilotin" auf ihrer Titelseite - ein Blick ins StudiVZ reichte, um herauszufinden, was die Hobbies und Vorlieben, was die Ängste von "Maxi J. (24)" waren. Die passende Bebilderung? Lieferte ein einfacher Klick auf das private Fotoalbum, das die Pilotin auf der Online-Plattform veröffentlicht hatte. In anderen Fällen ging die Berichterstattung weit darüber hinaus. Als im Januar etwa eine junge Frau bei einem Ski-Unfall ums Leben kam, druckte die Bild am Sonntag nicht nur ein dort gepostetes Foto der Frau ab - sondern zählte auch ihre Kontakte bei StudiVZ, um sie als "sehr beliebt" zu charakterisieren und nannte ihre liebsten Schulfächer.*“ (Kaul, 2008)

Das öffentliche Interesse an „Maxi J“ wird sich vor März 2008 auf studiVZ in Grenzen gehalten haben. Sie benutzte die Plattform wie 5 Millionen anderer Benutzer auch, ohne sich über die Folgen Gedanken zu machen. Der Irrglaube, dass die eigenen Daten nur für Freunde interessant sind, wurde ihr zum Verhängnis. Für die Journalisten sind die persönlichen Informationen rasch sehr wertvoll geworden. Das Beispiel der jungen Frau, die bei einem Ski-Unfall ums Leben kam zeigt, wie Informationen über Personen schnell durch Medien missinterpretiert werden können, denn wer kann nach der Auszählung der Freunde auf studiVZ wirklich feststellen, ob eine Person „beliebt“ ist? Es mag eine nützliche Funktion sein, seine Kontakte auf Plattformen abzubilden. Benutzer müssen sich allerdings die Frage stellen: „Was kann aus diesen Informationen abgeleitet werden?“

Wie ein System der Kontrolle und des Datenschutzes ad absurdum geführt werden kann, zeigt Hasan Elahi, der jeden seiner täglichen Schritte im Internet dokumentiert und seine

Privatsphäre dadurch aufgegeben hat. Grund hierzu war, dass der Kunstprofessor mit dunkler Haut und arabisch klingendem Vornamen vom FBI für einen Terroristen gehalten wurde. Obwohl sich diese Anschuldigung als Fehler herausstellte, musste Elahi fortan dennoch bei einem FBI-Agenten melden, wenn er das Land verlässt. Daraufhin änderte er die Art der Berichterstattung:

> *„Hasan stellt Hunderte Fotos von dem, was er macht, jeden Tag auf seine Homepage, eine Karte zeigt immer an, wo sich der Mann mit den kurzen, blond gefärbten Haaren gerade aufhält. Bilder von seinem Essen, Flughäfen oder den Wohnungen seiner Freunde. Er überschwemmt die Welt mit Informationen. "Dadurch, dass ich alles offenlege, bin ich komplett anonym geworden", sagt Hasan, "keinen interessiert wirklich so detailliert, was ich mache, auf welchem Klo ich gerade war."* (Buttler, 2007)

Elahi, der von Buttler als „Kunstobjekt“ definiert wird, hat den Spieß umgedreht. Durch das vermehrte Spamen an Informationen macht sich der Kunstprofessor laut eigener Aussage anonym. In diesem Falle dürfte das Wort „anonym“ jedoch falsch verwendet sein. Jeder kann über Hasan Elahi Informationen finden. Er ist also nicht anonym. Vielmehr sind die Daten, die über ihn gefunden werden können, unbrauchbar und uninteressant. Jeder kann alles über ihn erfahren. Es gibt keine Geheimnisse. Für Geheimdienstorganisationen ist er nun vollständig transparent. Die Werbeindustrie würde sich vermutlich sehr über mehr Personen wie Elahi freuen.

3.1.5. Probleme der Rechtsvergleichung

In den einleitenden Worten des Kapitels wurde bereits auf die Schwierigkeit der Begriffsdefinition und der unterschiedlichen Sprachen hingewiesen. Eine Konsequenz daraus sind Probleme in der Rechtsvergleichung. Es gibt keine weltweit gültigen Datenschutzgesetze. Das Internet, das Benutzer in der ganzen Welt miteinander verbindet, stellt daher einen Problembereich dar.

> *„In the EU, privacy protection should be enforced by the EU Data Protection Directive. Nevertheless, even if the EU Directive can help to enforce a relatively high standard of data protection in Europe, it will not be able to protect privacy sufficiently in the global information society. […] Privacy is therefore an international problem, and an international harmonization of privacy regulations is needed.”* (Fischer-Hübner, 2001, S. 24)

Die Datenschutzrichtlinie der EU regelt den Datenschutz und die Datensicherheit in Europa. Länder müssen diese verbindlichen Richtlinien in nationales Recht umwandeln. Eine internationale Lösung gibt es zurzeit noch nicht. Ein Zitat über die Vereinten Staaten von Amerika zeigt, dass diese, was den Datenschutz anbelangt, der EU hinterherhinken: “*So far, the US have been criticized for being the first in technology but the last in data protection.*” (Fischer-Hübner zitiert Wayne Madsen, 2001, 26). Welches Recht bei Problemen im Internet tatsächlich anwendbar ist, stellt Juristen vor einige offene Fragen. So sind nicht die Daten, die verarbeitet werden entscheidend, sondern Niederlassungen des Anbieters:

> *„Im Hinblick auf die dezentrale Struktur und den internationalen Datenaustausch im Bereich des Internet stellt sich zu Beginn jeder juristischen Betrachtung die Frage, welches nationale Recht anwendbar ist. Innerhalb der Europäischen Union (EU) richtet sich das anwendbare Datenschutzrecht nach dem Standort der Datenverarbeitung. Danach gilt das Recht des Ortes, an dem der Anbieter (als für die Verarbeitung Verantwortlicher) Daten verarbeitet. Dabei kommt es nicht auf die Herkunft der Daten an, entscheidend ist lediglich der Sitz der verarbeitenden Niederlassung. Der Begriff der Niederlassung wird im Gesetz nicht legal definiert. Schon der Betrieb eines Ser-*

> *vers stellt nach herrschender Meinung eine solche Niederlassung dar. […] Folglich muss ein Anbieter sicherstellen, dass jede seiner Niederlassungen auf dem Gebiet der EU den Anforderungen des jeweiligen Landesrechts entspricht. […] Bisher existieren jedoch keine internationalen Regelungen für die Feststellung des anwendbaren Rechts im Bereich des Internets. […] Sollen potenzielle Nutzer in Ländern außerhalb der EU angesprochen werden, muss man zusätzlich prüfen, ob in diesen eventuell das Recht des jeweiligen Empfängerlandes zur Anwendung kommt."* (Hippner *et al*, 2002, S. 78f)

Gewiefte Anbieter können diese Regelungen ausnutzen und ihre Server in Ländern aufstellen, die deutlich geringere Datenschutzrichtlinien vorschreiben. Das Auslagern von unternehmerischen Daten bzw. Servern wird in der Fachliteratur als „Offshoring" bezeichnet. Transferieren und speichern europäische Unternehmen personenbezogene Daten in Drittländer, in denen das europäische Datenschutzniveau nicht erreicht wird, drohen hohe Geldbußen. (vgl. Bereszewski, 2007). IT-Unternehmen, die meist an keine geographischen Hürden gebunden sind, können dieses Problem zur Gänze umgehen, in dem Firmen direkt in Ländern gegründet werden, in denen nur wenige Datenschutzgesetze existieren. Deutschsprachige Benutzer, die sich auf amerikanischen Webseiten registrieren, vergessen oftmals, dass ihre Daten in einem Drittland gespeichert werden. Während die Zahl an Benutzern, die das Datenschutzgesetz des eigenen Landes kennen, sehr gering sein dürfte, ist die Zahl an Benutzern, die über das ausländische Datenschutzrecht informiert sind, schwindend gering. Es stellt daher aus rechtlicher Sicht einen großen Unterschied dar, wo ein benutztes Service die anfallenden Daten speichert. Ob sich Benutzer über dieses Problem bewusst sind, klärt das Kapitel 4.2.3.

3.1.6. Das Geschäft mit den Nutzerdaten

Web2.0[3] Dienste bestehen zumeist ausschließlich aus „user generated content", der eine Plattform einzigartig macht. Der Wert eines Dienstes, egal ob Videoplattform, Blogdienst oder Social Community liegt daher weniger in den Funktionen und dem Programmcode, sondern viel mehr im Benutzerstamm. Aus diesem Grund werden sämtliche Daten aus den Diensten analysiert um Dienste verbessern und attraktiver für Benutzer und Werbepartner machen zu können. Um dies bewerkstelligen zu können, ist der Einsatz von drei auf einander aufbauenden Techniken notwendig.

3.1.6.1. Datamining

Unter dem Begriff des Dataminings versteht man eine statistische Analyse der Daten, um neue Daten und Zusammenhänge zu generieren.

> *"Werber gieren nach möglichst präzisen Informationen über ihr Publikum. Denn die Nutzer stumpfen immer mehr gegenüber einfach so auf Webseiten platzierten Bannern ab. Sie klicken Werbung seltener an. Das US-Wirtschaftsmagazin Businessweek zitiert eine Studie des Online-Vermarkters Eyeblaster, derzufolge [sic] auf Yahoo-Seiten die sogenannte Klick-Quote im Verlauf des Vorjahres um zwei Drittel gesunken sein soll – von 0,75 auf 0,27 Prozent."* (Lischka, 2007a)

Datamining kann als mögliches Anwendungsszenario Daten von Social Web Diensten analysieren und Benutzer zu untersuchen. Aus den daraus gewonnen Daten können mittels Targeting sehr genaue Nutzungsprofile und dazu passende Informationen erstellt werden. Das Aggregieren der Daten ist dabei anonym und erfolgt ausschließlich unidirektional. Erlau-

[3] Der Begriff Web2.0 wird im Kapitel 3.2 näher definiert.

ben Benutzer jedoch ausdrücklich auch die Auswertung von personenbezogenen Daten ist auch dieses Verfahren rechtlich abgesichert:

> „*Aggregierte Daten sind nicht personenbezogen, da sie nur den Bezug auf eine Gesamtmenge von Individuen herstellen und somit keinen Rückschluss auf eine einzelne Person ermöglichen. Umgekehrt wird der Personenbezug allerdings hergestellt, wenn eine Person als Mitglied einer Gruppe gekennzeichnet wird, über die bestimmte Angaben gemacht werden. […] Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn eine gesetzliche Regelung oder eine andere gesetzliche Vorschrift dies ausdrücklich erlaubt bzw. anordnet oder der Betroffene zuvor eingewilligt hat. Folglich ist jede Datenverarbeitung unzulässig, sofern sie nicht auf eine gesetzliche Erlaubnis oder die Einwilligung des Betroffenen gestützt werden kann.*“ (Hippner *et al*, 2002, S. 82f)

3.1.6.2. Targeting

Basierend auf den Ergebnissen des Dataminings versucht Targeting ähnliche Benutzer eines Dienstes in Gruppen zu formen. Vorteil des Targetings ist im Gegensatz zur personalisierten Werbung, dass hierbei keine personenbezogenen Daten an den Werber übertragen werden.

> *„Noller glaubt, dass allzu perfekt und persönlich personalisierte Werbung nicht erfolgreich sein kann. Sie müsse einen Mittelweg finden: "Online-Werbung muss exakt genug personalisiert sein, um spezielle Zielgruppen ansprechen zu können und ungenau genug personalisiert sein, um Nutzern nicht das Gefühl zu vermitteln, sie würden ausgespäht."* (Lischka, 2007a)

Der Ansatz des Targetings ist nicht einen einzelnen Nutzer auszuspionieren, sondern anhand einer Gruppe von ähnlichen Personen Verhalten abzuleiten. Hierbei wird das über Jahre hinweg praktizierte 1:1 Marketing über Bord geworfen und sich auf moderne, statistische Auswertungsverfahren verlassen:

> *„Die alte Branchenweisheit konzentriert sich darauf, eine Person zu identifizieren und dann in eine One-to-One-Marketingbeziehung einzutreten“, beschreibt Adam Sarner von Gartner die gelernten Vorgehensweisen. Aber die Realität der neuen Online-Welt werde aus anonymen Online-Persönlichkeiten bestehen, die sich durch Verhaltensmuster, Vorlieben, Abneigungen, Aktivitäten oder ihrer jeweiligen Rolle in einer Online-Umgebung definieren. Das moderne Markteting [sic] werde Wege finden müssen, mit diesen anonymen Persönlichkeiten eine Beziehung aufzubauen und zu erhalten. Also: Targeting ja, dumpfe Kategorisierung nein, sagt Gartner […]“* (Postinett, 2008).

3.1.6.3. Personalisierte Werbung

Personalisierte Werbung geht einen Schritt weiter als Targeting und versucht ein wesentlich spezifischeres 1:1 Marketing erneut einzuführen. Dabei entscheidet ein Benutzer, bzw. dessen Umfeld, welche Werbung zu ihm passt. Merkmale der eigenen Person, oder Beziehungen zu anderen Personen helfen hierbei ein genaues Bild über eine Person zu bekommen. Die hierfür notwendige Auswertung personenbezogener Daten stößt dabei bei Benutzern auf wenig Freude. Die Spiegel Online Umfrage zum Thema „Welche Art von Personalisierung finden Sie akzeptabel?“, an der 925 Personen teilnahmen, zeigt ein ernüchterndes Ergebnis:

Fast 3 von 4 Teilnehmern sprechen sich dafür aus, dass keine Personalisierung akzeptabel ist. 16% finden eine anonymisierte Analyse des Surfverhaltens ok. Lediglich 5 % sagen, dass sie eine Analyse für unproblematisch halten würden. (vgl. Spiegel, 2008). Auch amerikani-

sche Benutzer von Internetsystemen zeigen, wie unwohl sie sich bei der Personalisierung von Seiteninhalten und Werbung fühlen. Nachdem den Teilnehmern Regeln vorgelegt wurden, die die Personalisierung der Daten eingrenzt und näher erklärt, steigt jedoch die Akzeptanz der Methode:

> *"A six in ten majority (59%) are not comfortable when websites like Google, Yahoo! and Microsoft (MSN) use information about a person's online activity to tailor advertisements or content based on a person's hobbies or interests. A quarter (25%) is not at all comfortable and 34 percent are not very comfortable; […] After four privacy/security policies were introduced, U.S. adults did change their opinions: By 55 to 45 percent, a majority of U.S. adults indicates that they would be more comfortable with companies using information about a person's online activities to provide customized advertising or content; Interestingly, once the privacy/security policies were presented the percentages of those who are very comfortable increases only very slightly to 9 percent from 7 percent. The percentage of those who are somewhat comfortable given the privacy/security policies increases more significantly to 46 percent from 34 percent;"* (Harrisinteractive, 2008)

Ergebnisse der Social Networking Services Umfrage der Forschungsgruppe Kooperationssysteme München zeigt ein anderes Bild: 30 % der befragten Teilnehmer geben an, dass ihnen personalisierte Werbung egal ist. Nur 18 % sind der Meinung, dass sie Targeting definitiv stört. Hier dürfte der Kontext der Fragestellung entscheidend sein. Wenn dezidiert nach dem Datenschutz gefragt wird, sind stark differenzierende Ergebnisse festzustellen. Dieses Bild zeigt ebenfalls die eigens durchgeführte Umfrage, deren Auswertung im Kapitel (4.2.3) vorliegt.

3.1.7. Angriff- und Abwehrszenarien in Webapplikationen

Webapplikationen haben, wie jede andere Software, Fehler. Soziale Netzwerke wie MySpace oder Facebook werden jedoch im Vergleich zu „unkritischeren Applikationen" von mehreren Millionen Personen im Monat benutzt. Einen Fehler auf diesen Plattformen zu finden und auszunutzen kann daher für viele Personen einen enormen Schaden bedeuten. Die wichtigsten Angriffsformen, die in den nächsten Unterkapiteln beschrieben werden, zeigen, wie bereits kleine Lücken ausreichen, um großen Schaden anrichten zu können. Angriff und Abwehr dieser Attacken sind Themen, die in erster Linie technischer Natur sind. Die Benutzer von Applikationen verweisen daher auf den Betreiber, der die Benutzer zu schützen hat. In Wahrheit sind jedoch nicht nur die Applikationen selbst Ziel der Angriffe. Moderne Angriffsformen zeigen deutlich: Nicht die Plattform selbst ist Ziel der Angriffe, sondern deren Benutzer. Die Informationssicherheit einer Applikation definiert sich daher nicht nur über die Sicherheit innerhalb der Applikation, sondern ist ebenfalls von der Aufklärung und Sensibilisierung der Benutzer abhängig. Daher entschloss sich der Autor dieses Kapitel in die Arbeit aufzunehmen. Zum weiteren Verständnis der analysierten Social Communities sind die folgenden Begriffsdefinitionen daher nicht unwesentlich und tragen zu einem größeren Bewusstsein der Benutzer bei.

3.1.7.1. SQL Injection

Bei Structured Query Language (SQL) Injection Angriffen versuchen Angreifer schadhaften Code direkt in der Datenbank einer Webseite auszuführen. Dabei werden mangelhafte Überprüfungen von Formularfeldern ausgenutzt um Daten zu manipulieren.

> *„Mit SQL Injection kann ein Angreifer Anfragen, die an eine Datenbank gesendet werden, dadurch modifizieren oder hinzufügen, dass er mit der Eingabe in die Web-*

> *Anwendung spielt. Die Attacke funktioniert, wenn ein Programm Anfragen auf der Grundlage von Zeichenketten vom Client aufbaut und an den Datenbankserver weitergibt, ohne die Zeichen, die für den Server eine besonderer [sic] Bedeutung haben, zu überprüfen.“* (Huseby, 2004, S. 30)

Die Angriffe können verschiedene Ziele verfolgen. Angreifer können durch bestimmte Eingaben versuchen sich ohne bestehenden Benutzeraccount in die Applikation einzuloggen, oder Datenbestände auszulesen. Bei der gefährlichsten Form von gezielten SQL Injection Angriffen können gesamte Datenbestände (sowohl Datenbank selbst als auch das komplette Dateisystem am Server) gelöscht und modifiziert werden.

3.1.7.2. Social Engineering

Eine Sonderform des Angriffs eines Computersystems stellt das sogenannte Social Engineering dar, in dem nicht das System selbst, sondern deren Benutzer angegriffen wird:

> „*Frei übersetzt bedeutet der Begriff: soziale Instrumentalisierung. Als Social Engineering wird ein Vorgehen bezeichnet, das Menschen aufgrund ihrer Gutgläubigkeit zu manipulieren versucht und somit anfällig macht für Missbräuche aller Art*.“ (Klau, 2002, S. 89)

> *Je häufiger die Nutzer nach ihren persönlichen Informationen gefragt werden, desto schneller geben sie sie freiwillig heraus, da vieles an anderer Stelle im Netz schon bekannt ist. Damit steigt die Anfälligkeit für Spam oder gar Phishing-Attacken. "Viele Leute sind immer noch blauäugig oder sogar auf beiden Augen blind", konstatiert Hardy. […] Um das zu beweisen, startete er im Online-Netzwerk Wer-kennt-wen Anfang des Jahres ein Experiment. Unter dem Pseudonym "Natalie" erstellte Hardy ein Profil mit dem Foto einer leicht bekleideten jungen Frau sowie einigen Angaben zu persönlichen Interessen und Vorlieben. Er beschrieb Natalie unter anderem als "suchend" und "für alles aufgeschlossen". "Ziel des Versuchs war es, herauszufinden, was innerhalb von fünf Minuten ohne eigenes Zutun mit einem solchen Profil passiert", so Hardy. Das Ergebnis war erhellend: Als Hardy das Profil nach fünf Minuten wieder entfernte, hatte die fingierte Single-Frau bereits 19 sofort bestätigte neue Kontakte, 27 E-Mails mit Kontaktanfragen sowie 48 Nachrichten. Über Natalie hatte Hardy freien Zugang zu den persönlichen Daten dieser Mitglieder, wie zum Beispiel Adresse, Alter, Instant-Messenger-Name und persönliche Interessen. Social Networks sind laut Hardy "ein Daten-Eldorado für Spammer und Phisher."* (Hülsbömer, 2008).

Der Versuch von Herrn Hardy zeigt, dass Social Communities der ideale Platz für Social Engineering Angriffe sind. Durch gefälschte Profile ist es oft ohne technische Mittel möglich an die persönlichen Daten vieler anderer registrierter Benutzer zu kommen. Der Test zeigt ebenfalls, wie schnell der virale Effekt zuschlägt und Personendaten bereits bei der ersten Kontaktaufnahme herausgegeben werden. Während klassische Social Engineering Angriffe auf einzelne Personen gerichtet sind, ist das Vorgehen in diesem Fall wesentlich einfacher. Hat man es als Angreifer nur auf unbestimmte Daten abgesehen, ist die oben beschriebene Variante ideal. Ohne viel Mühe aufgewendet zu haben, senden Personen ohne Anfrage ihre Daten zu. Eine Kontaktaufnahme ist meist gleichbedeutend mit dem indirekten Erhalt der kompletten Profildaten. Die so angewandte „Reverse Social Engineering“ Methode, bei der Zielpersonen selbst die Kontaktaufnahme einleiten gilt als noch erfolgsversprechender, da Personen keinen Missbrauch vermuten (vgl. Granger, 2001).

Eine Sonderform von Social Engineering stellt das sogenannte „Phishing“ dar, die auf technischen Angriffsmitteln beruht. Gefälschte, zum Verwechseln ähnliche E-Mails werden hierbei verschickt um an Benutzerdaten zu kommen. Seit dem Jahr 2004 ist Phishing eine oft diskutierte Angriffsform, die anfänglich vor allem für Angriffe auf Banken genutzt wurde. (vgl.

Janowicz, 2007, S. 253) Für geübte Benutzer sind Phishing Attacken leicht zu erkennen. Neueinsteiger, die über die Gefahren im Internet noch nicht aufgeklärt wurden, haben jedoch naturgemäß deutlich größere Probleme diese Angriffe zu erkennen.

3.1.7.3. XSS – Cross Site Scripting Angriffe

Jeremiah Grossman (zitiert in Mook, 2005) verdeutlicht die Bedrohung dieser Angriffe: "*Found in over 90 percent of Web sites, Cross-Site Scripting vulnerabilities are by far the most common security issue* […]". Diese Form der Angriffe nutzt Fehler in der Überprüfung von Formularfeldern aus, um schadhaften Code in Teile der Seite einzubauen. Die Angriffe sind in erster Linie nicht gegen das System selbst gerichtet. Der Code wird im Browser des Benutzers angezeigt und ausgeführt. Diese Angriffe sind gefährlich weil so Benutzerinformationen sowie Logindaten ausgelesen bzw. durch asynchrone Aufrufe im Hintergrund beliebige Seiteninhalte (Passwort?) an ein Skript des Angreifers weitergeleitet werden können. Es wird daher wie bei Social Engineering Methoden der Benutzer einer Applikation angegriffen. XSS-Angriffe (vgl. Alexander, 2006, S. 406 und Huseby, 2004, S. 111). Benutzer selbst merken von diesen meist unsichtbaren Angriffen nichts und müssen auf die Sorgfalt der Betreiber vertrauen.

> *"It's also important to note that a user's web browser or computer does not have to be susceptible to any well-known vulnerability. This means that no amount of patching will help users, and we become solely dependent on a website's security procedures for online safety. Browser vendors, software developers and information security professionals working with web applications are the key to stopping this entirely preventable attack"* (Grossmann, 2006, S. 6).

Bekannte XSS-Attacken wie Samy (s. Kapitel 4.1.1.1) verfolgen das Ziel, dass sich der schadhafte Code in immer mehr Benutzerprofile kopiert. Ein erfolgter Angriff infiziert daher weite Teile einer Applikation; ein Filtern des schadhaften Codes ist oftmals nicht mehr möglich.

3.1.7.4. Webcrawling

Suchmaschinen indizieren seit vielen Jahren das Internet. Bekanntes Beispiel dafür ist Google, das mit seinem GoogleBot drei Mal mehr Seiten indiziert, als jeder andere Kontrahent[4]. Google verfolgt dabei einen für weite Teile gemeinnützigen Dienst. Im Gegenzug dazu gibt es Hacker, die das Web, bzw. einzelne Webseiten ebenfalls indizieren, bzw. „crawlen". Bei diesen Angriffen werden jedoch keine gemeinnützigen Interessen verfolgt.

> *„A Web community can be loosely defined as a collection of Web pages that are focused on a particular topic or theme. Viewed from the framework of traditional information retrieval, the problem of community identification would be expressed in terms of document content or explicit relations between documents. However, given the hyperlinked structure of the Web, the community identification problem can be reformulated so as to exploit the implicit relations between documents that are formed by hyperlinks".* (Levene & Poulovassilis, 2004, S. 45)

Das Internet und vor allem soziale Netze bieten ideale Bedingungen für Crawling-Attacken, da relevante Dokumente (bzw. Personen) durch Links miteinander in Verbindung stehen. So ist es sehr einfach möglich, basierend auf einer Startseite, viele ähnliche Seiten in kurzer Zeit

[4] Vgl. http://www.google.com/help/indexsize.html

zu erhalten, da Webseiten durch ihre Verlinkungen als Graphenstruktur definiert werden können.

> *„Web crawlers are programs that exploit the graph structure of the Web to move from page to page. […] From the beginning, a key motivation for designing Web crawlers has been to retrieve Web pages and add them or their representations to a local repository. Such a repository may then serve particular application needs such as those of a web search engine."* (Levene & Poulovassilis, 2004, S. 153)

Die so gewonnenen Daten werden in eine eigene Datenbank gespeichert. Das automatisierte Besuchen von Webseiten ist rein rechtlich gesehen nicht strafbar. Die Verwendung der Daten, bzw. die persistente Speicherung kann jedoch zu rechtlichen Problemen führen. Um das automatisierte Indizieren von Webseiten zu verhindern, werden in den letzten Jahren häufig zufällig generierte Bilder eingesetzt, die vom Benutzer beschrieben werden müssen.

3.1.7.5. CAPTCHA

Completely Automated Public Turing Test To Tell Computers and Humans Apart (CAPTCHA) wurden im Jahr 2000 an der Carnegie Mellon Universität entwickelt. Die Idee dahinter ist simpel:

> *"it is a test, any test, that can be automatically generated, which most humans can pass, but that current computer programs cannot pass. Notice the paradox: a CAPTCHA is a program that can generate and grade tests that it itself cannot pass […] this approach has the beneficial side effect of inducing security researchers, as well as otherwise malicious programmers, to advance the field of AI."* (Von Ahn *et al*, 2004)

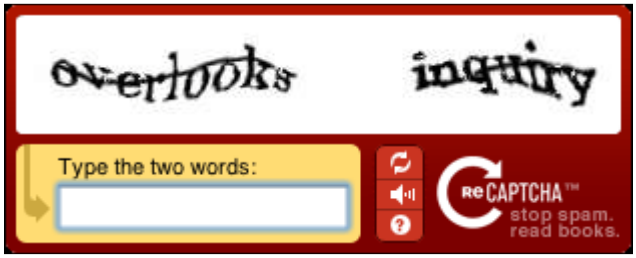

Abbildung 2: Beispiel eines CAPTCHAs (vgl. http://recaptcha.net/captcha.html)

Es handelt sich bei CAPTCHAs um Bilder, die von Menschen verstanden werden, aber von Maschinen nicht interpretiert werden können. Abbildung 2 zeigt ein Beispiel solch eines CAPTCHAs, bei dem Benutzer die zwei dargestellten Wörter als Überprüfung eintippen müssen. Die Absicherung durch diese Bilder hat viele Anwendungsfälle: Kommentarspam auf Webseiten kann ausgeschlossen werden, Registrierungsprozesse abgesichert werden (s. Kapitel 4.1.4.2) und Online Befragungen abgesichert werden. Dennoch kamen CAPTCHAs bereits öfters wegen mangelhafter Implementierungen und oftmaliger Barrieren für körperlich eingeschränkte Personen in die Kritik. Während täglich 150.000 Stunden an menschlicher Zeit zur Lösung von CAPTCHAs verbracht werden, werden Computersysteme, wie bereits von Von Ahn (2004) beschrieben „intelligenter". CAPTCHAs, die zur Bot-Abwehr von Microsofts Hotmail-Service verwendet werden, könnten bereits mit einer Trefferquote von 10-15% innerhalb von 6 Sekunden automatisiert gelöst werden. (vgl. Greif, 2008 und Carnegie Mellon University, 2008). Nicht nur Computersysteme, auch Hacker werden intelligenter, wie Nachrichten zeigen, die berichten, dass CAPTCHAs mit Hilfe von Pornoseiten bzw. durch billige Arbeitskräfte aus Indien gelöst werden. (vgl. Krüger, 2008).

3.2. Social Communities

Social Communities sind virtuelle Netzwerke, die das Kommunizieren ihrer Benutzer auf der Plattform in den Vordergrund stellen und als direkte Antwort auf die „soziale Isolation“ von Internetteilnehmern zu verstehen, die oftmals in den Beginnen des Internets vermutet wurde. (vgl. Schulzki-Haddouti, 2005). Eine ausführlichere Definition findet Speck (2007):

> *“A social network is a social structure, community, or society made of nodes which are generally accounts, individuals or organizations. It indicates the ways in which they are connected through various social familiarities, affiliations and/or relationships ranging from casual acquaintance to close familial bonds.”*

Die Definition zeigt, dass soziale Netzwerke in erster Linie keine technischen Applikationen darstellen, sondern in ihrer Urform soziale Systeme. Als soziales Netz können Familien, Vereine, Firmen bzw. Schulverbände angesehen werden, in denen jeder Teilnehmer einen Knoten darstellt. Die Kanten zwischen den Personen sind unterschiedlich „lang“, was die Verbundenheit von Personen näher definiert.

Mit dem Einzug des *Web2.0* starteten soziale Netze auch im Internet durch. Unter dem Begriff „Web2.0“ versteht man eine neue Generation von Webdiensten, die vor allem die Interaktion mit dem Benutzer ins Zentrum aller Bemühungen stellen. Tim O’Reilly, der den Begriff erfunden hat, definiert 2005 den Begriff mit folgenden Worten:

> *“[…] delivering software as a continually-updated service that gets better the more people use it, consuming and remixing data from multiple sources, including individual users, while providing their own data and services in a form that allows remixing by others, creating network effects through an "architecture of participation […]"* (O’Reilly, 2005)

Während die Plattformanbieter lediglich Dienste zur Verfügung stellen, erstellen die Benutzer der Applikationen Inhalte, die oftmals den Wert einer Plattform darstellen. Dienste, die das Partizipieren ihrer Benutzer in den Vordergrund stellen, wuchsen in den letzten Jahren rapide und so wurde das Web2.0 zum „Social Web“[5], in dem Scharen von Benutzern ihr Leben dokumentierten. Im Jahr 2006 stellten Social Communities für die Gruppe der 12-21 jährigen Amerikaner den Hauptgrund ihrer Internetaktivitäten dar. 2/3 Jugendlichen benutzten damals bereits die sozialen Netze im Internet.

> *„Als Social-Networking-Services (SNS) werden Anwendungssysteme bezeichnet, die ihren Nutzern Funktionalitäten zum Identitätsmanagement (d.h. zur Darstellung der eigenen Person i.d.R. in Form eines Profils) zur Verfügung stellen und darüber hinaus die Vernetzung mit anderen Nutzern und so die Verwaltung eigener Kontakte ermöglichen“* (CSCM, 2008)

Soziale Netze funktionieren im Internet meist ähnlich. Nach erfolgreicher Registrierung erhalten Benutzer die Möglichkeit ein Profil über die eigene Person zu erstellen. Ist dieses ausgefüllt, kann mit weiteren Benutzern der Plattform ein Kontakt hergestellt, bzw. eine Beziehung aufgebaut werden. Die eigene Online-Identität wächst somit an Bedeutung, je mehr Beziehungen aufgebaut werden. Je nach Ausprägung der Plattform gibt es noch weitere Funktionen wie Blogs, Fotoalben, Gruppenzugehörigkeiten und Foren, in denen über bestimmte Interessensgebieten diskutiert werden können.

[5] Synonym für Web2.0

3.2.1. Das kleine Welt Phänomen

"Die Welt ist klein." heißt es im Volksmund. Dass dieses Phänomen tatsächlich wissenschaftlich belegbar ist, wurde anhand eines Experiments festgestellt.

> *"Milgram sent several packages to random people in the United States, asking them to forward the package, by hand, to someone specific or someone who is more likely to know the target. The average path length for the received packages was around 5.5 or six, resulting in widespread acceptance for the term six degrees of separation."* (Speck, 2007)

Vereinzelte Communities (vor allem Dating-Plattformen) bedienen sich einzig allein der Profilerstellung und Suche von passenden Profilen. Soziale Netzwerke im Web2.0 fokussieren sich zumeist eher auf die Vernetzung der Mitglieder untereinander. Sie beziehen sich dabei dem Prinzip oder *Phänomen der kleinen Welt*, das besagt, dass jeder jeden über circa 6 Ecken kennt. Vor allem Business Communities haben bereits früh erkannt, dass die Verbindung der Mitglieder untereinander einfach zu visualisieren ist und eine wichtige Funktion innerhalb von Netzwerken darstellen kann.

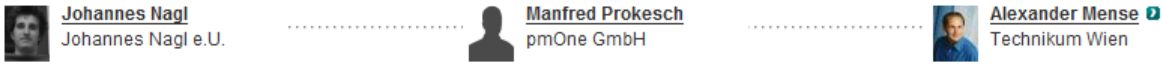

Abbildung 3: Das kleine Welt Phänomen auf Xing graphisch aufbereitet

In Abbildung 3 wird die Verbindung des Autors zu dessen Betreuer visuell verdeutlicht. Da noch keine direkte Kontaktaufnahme erfolgte, kennt man sich lediglich über eine gemeinsame Bekanntschaft. Wie groß das persönliche Netzwerk tatsächlich ist, verrät Xing ebenfalls auf einen Blick[6]:

Kontaktlevel	Benutzerzahl	Ø neue Kontakte pro Person
Primärkontakte	88	-
Sekundärkontakte	7.991	90
Tertiärkontakte	477.760	59

Tabelle 1: Die Kontakte des Autors auf Xing

Eine durchgeführte Studie von Xing (2007a) zeigt, dass der durchschnittliche Europäer 99 Primärkontakte hat. Die Plattform besitzt rund 5 Millionen Mitglieder (vgl. Ihlenfeld, 2008). Eine Hochrechnung vom Autor ergibt, dass bereits ein durchschnittlicher „Gewinn" von 11 neuen eindeutigen Kontakten der Tertiär-Kontakte bereits ausreichen würde, um nahezu mit jedem Mitglied von Xing in Kontakt zu stehen.

Kontaktlevel	Benutzerzahl	Ø neue Kontakte pro Person
Quartärkontakte (Hochrechnung)	5.000.000	11 (Hochrechnung)

Tabelle 2: Die Kontakte des Autors auf Xing - Hochrechnung

Die vage Hochrechnung zeigt, dass das kleine Welt Phänomen auf Social Web Plattformen definitiv anzuwenden ist. Ein Problem bleibt allerdings unangetastet, mit dem Social Communities zu kämpfen haben: Im Gegensatz zu dem theoretischen Konzept, das die gesamte Menschheit miteinander in Verbindung bringt, ist eine Verbindung in der virtuellen Welt nur

[6] Vgl. die persönliche Startseite des Autors auf Xing, Stand: 05.04.2008, unter https://www.xing.com/app/user?op=home

dann möglich, wenn die entsprechenden Personen auch tatsächlich in einem der Netzwerke registriert sind.

Im Gegensatz zu sozialen Netzen in der Realität sind die Beziehungen zwischen Personen immer genau gleich definiert. Die unterschiedliche Kantenlänge, die in regulären Netzen existiert, ist in den technischen Netzen immer ident. Entweder zwei Personen kennen sich, oder nicht. Diese Regelung führt vor allem in Social Communities zu Problemen, in denen Benutzer viele Informationen (Fotos, Gruppenzugehörigkeiten, …) über sich Preis geben. Die dort vorhandenen Privatsphäre-Einstellungen können, wie der Vergleich in Kapitel 4.1 zeigt, nur auf „Freunde", oder „Freundesfreunde" angepasst werden. Personen neigen jedoch dazu Beziehungen zu Personen aufzubauen, die sie im wahren Leben nicht als „Freund" bezeichnen würden. Es entsteht eine sogenannte „imaginary community", deren tatsächlicher Wert für Benutzer deutlich geringer ist. Durch die „binären" Freundschaftsbeziehungen haben daher oftmals mehr Personen auf sensible Daten Zugriff als dies abseits der Plattformen der Fall ist (vgl. Gross & Acquisti, 2005). Verdeutlicht wird dieser Trend durch eine Untersuchung des TV-Senders MTV, der 8- bis 24-Jährige Nutzer zum Thema Freundschaften befragt hat. Das Ergebnis zeigt, dass junge Deutsche ein Drittel ihrer Online-Freunde noch nie gesehen hat. (vgl. Bager, 2008)

3.2.2. Formen von Social Communities

Analysiert man den Zweck von Communities, kann dieser ebenfalls in zwei unterschiedliche Gruppen aufgeteilt werden. Bei General Interest Communities gibt es keinen Fokus auf eine bestimmte Zielgruppe; Betreiber versuchen sich an alle Benutzer des Internets (oder auf spezielle geographische Gebiete) zu wenden. Daraus resultiert eine oftmals sehr hohe Reichweite, die General Interest Netzwerke abdecken können. Betreiber stellen hierbei die technische Basis für den Betrieb der Community bereit und versuchen durch gezieltes Marketing Benutzer für die eigene Seite zu gewinnen. Im Gegensatz dazu bilden die Special Interest Netzwerke Anlauf für spezielle Themen. Business Plattformen, Communities speziell für Mütter, oder produktbezogene Portale sind tendenziell kleiner. Sie haben jedoch einen entscheidenden Wettbewerbsvorteil: Ihre Vertiefung auf ein Thema. Um die Plattform erfolgreich vermarkten zu können, versuchen Betreiber durch Anbieten von Informationen zum Thema Mitglieder zu gewinnen.

Die folgenden Zahlen von Andreas Göldi zeigen die großen Unterschiede in der aktuellen Marktsituation von Communities deutlich. Er unterscheidet zwischen Zielgruppen- (Special Interest) und Allgemeinrelevanten Communities (General Interest)[7]:

> *"Prozentual wachsen diese Nischennetzwerke deutlich stärker als die breit abgestützten Konkurrenten. Allerdings findet das Wachstum auf einem sehr viel kleineren absoluten Level statt." (Göldi, 2008)*

[7] Professor Böcker spricht in diesem Zusammenhang über „Special Interest" und „Social Network" (vgl. Böcker, 2008, S. 13). Der Autor findet die grundsätzliche Unterteilung in General- und Special Interest jedoch für treffender, da beide Formen soziale Netzwerke darstellen.

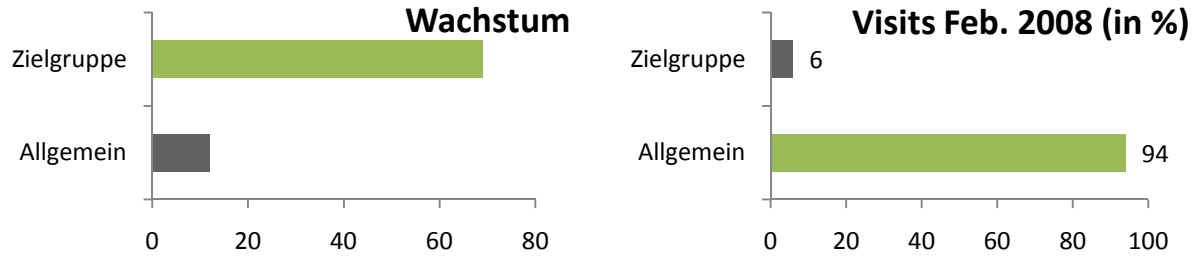

Diagramm 1: Wachstum von Social Communities und Visits 02/08, adaptiert von Göldi, 2008

Aus den Wachstumszahlen in Diagramm 1 kann abgeleitet werden, dass zukünftig vermehrt Special Interest Communities den Markt dominieren werden. Eine Hochrechnung ergibt, dass Zielgruppenspezifische Communities 2011 den allgemeinen Angeboten den Rang ablaufen könnten. Voraussetzung: Die Wachstumszahlen bleiben konstant. Der Markt der General Interest Plattformen ist durch die quasi Monopolstellungen von MySpace und Facebook gesättigt. Die Besucherzahlen der Communities zeigen ein deutliches Bild. Während MySpace bei rund 65 Millionen Visits im Februar 2008 lag, hat der 20. des Rankings, Google Orkut, gerade einmal 0,7% der Besucherzahlen von MySpace. (vgl. Göldi, 2008)

> *„Eine Rezension schreibt man nur einmal bei Amazon, seine Fotos lädt man nur einmal hoch bei FlickR, seine Bookmarks speichert man nur einmal bei del.icio.us, seine gebrauchten Artikel verkauft man bei eBay. Wer zu spät kommt, den bestraft der Nutzer“* (Alby, 2006, S. 161)

Haben Benutzer bereits ihre Lieblingsdienste im Netz gefunden, werden Sie diese auf Grund der angesammelten Daten nicht so schnell verlassen. Doch wird ein bestimmtes Themengebiet in einer anderen Community tiefergehend behandelt, so ist es sehr wohl möglich, dort ein Zweitprofil zu eröffnen. Die Bemühungen der OpenSocial Initiative sowie die Data Portability Funktionalität, die in Kapitel 3.2.5 beschrieben werden, könnten die von Tom Alby vorausgesagte Kapselung der Dienste jedoch nachhaltig verändern und die Daten, die ein Benutzer im Netz von sich publiziert, vernetzen. Ist es möglich, seine Daten von Plattform A nach B mit einem Klick mitzunehmen, ist wohl auch der Markt der General Interest Plattformen wieder härter umkämpft.

3.2.3. Der Erfolg von Social Communities

Ab wann eine Plattform erfolgreich ist, hängt oft von der Betrachtungsposition ab. Befragt man die Unternehmen selbst, sagt 1/3 der Betreiber, dass bereits eine kritische Masse bei 25.000 – 50.000 Mitgliedern erreicht ist. 40% der befragten Teilnehmer konnten die kritische Masse allerdings gar nicht erst abschätzen. (vgl. Böcker, 2008, S. 59). Daher stellt der Autor zwei Formeln vor, die den Erfolg, bzw. das Wachstum eines sozialen Netzes sehr wohl messen können.

3.2.3.1. MetCalfe’s Law

Robert Metcalfe gilt als der Erfinder des Ethernets (vgl. LAN). Er hat Ende der 1980er Jahre eine Formel für den Wert von Netzwerken aufgestellt: „*Simply put, it says that the value of a communications network is proportional to the square of the number of its users.*” (vgl. Metcalfe, erklärt in Briscoe et al, 2006). Das heißt, dass ein Netzwerk immer „wertvoller” wird, je mehr Personen daran teilnehmen. Briscoe schreibt weiter, dass diese Regel laut Metcalfe auf alle Formen von Kommunikationsnetzwerken anzuwenden ist, egal ob Telefon-, Compu-

ter- oder Social Network im Internet. Selbst kommt er jedoch zum rechnerischen Schluss, dass die Formel ungültig ist.

> "*If Metcalfe's Law were true, then two networks ought to interconnect regardless of their relative sizes. But in the real world of business and networks, only companies of roughly equal size are ever eager to interconnect. In most cases, the larger network believes it is helping the smaller one far more than it itself is being helped. Typically in such cases, the larger network demands some additional compensation before interconnecting. Our n log(n) assessment of value is consistent with this real-world behavior of networking companies*" (Briscoe et al, 2006)

Briscoe korrigiert die Formel und lässt den Wert nicht proportional sondern logarithmisch zu der Benutzerzahl steigen, was ein deutlich langsameres Wachstum bedeutet. Daraufhin antwortete Robert Metcalfe persönlich:

> "*As I wrote a decade ago, Metcalfe's Law is a vision thing. It is applicable mostly to smaller networks approaching "critical mass." And it is undone numerically by the difficulty in quantifying concepts like "connected" and "value." […] my law's critics should look at whether the value of a network actually starts going down after some size. Who hasn't received way too much email or way too many hits from a Google search? There may be diseconomies of network scale that eventually drive values down with increasing size.*" (Metcalfe, 2006).

Die Diskussion brachte zwei wertvolle Ergebnisse, die sicherlich einen großen Einfluss auf die anfängliche Formulierung des Wertes hatten. Einerseits wird die Verknüpfung zweier Netzwerke miteinander verglichen, die zweifelsfrei unterschiedliche Auswertungen auf den Wert der Netze hat, wenn diese unterschiedlich groß sind. Andererseits, und dies dürfte die weitaus wichtigere Erkenntnis sein: Der Wert einer Plattform steigt nicht unendlich lang. Der Wert eines Netzwerks kann ebenfalls bei zunehmender Größe sinken, wenn nicht genügend Vorkehrungen getroffen wurden, um schadhaftes Handeln innerhalb des Netzes zu unterbinden. Im Kapitel 4.1.3 zeigt der Autor die vielen Probleme, die MySpace aufgrund dessen Größe hat.

3.2.3.2. Die kritische Masse

Ein deutlich praktischerer Ansatz ist die Definition der kritischen Masse, die für einen „Hype" eines sozialen Netzwerks erforderlich ist, der von den Betreibern der Plattform whatsyourplace.de entwickelt wurde und in der Abbildung 4 mathematisch dargestellt wird.

$$Userzahl = \frac{Z}{X} + \frac{N}{X} + \left(\frac{N}{X}\right)^2 + \left(\frac{N}{X}\right)^3 + \cdots = \frac{Z}{X} + \sum_{t=0}^{\infty}\left(\frac{N}{X}\right)^t$$

Z: # Personen, die direkt erreicht werden
X: jede Xte erreichte Person wird zum User
N: jeder User erreicht wiederum N Personen

Abbildung 4: Der Ansatz der "kritischen Masse", nach whatsyourplace, 2008

Die Autoren von whatsyourplace (2008) erklären das mathematische Konstrukt wie folgt:

> *"Entscheidend ist der Ausdruck **N/X** im Summenterm. N/X ist der "**Word of Mouth Faktor**". Im schlimmsten Fall ist dieser Faktor gleich null (kein Besucher erzählt die Seite weiter). Im besten Fall beträgt der Wert mindestens 1. Dann werden im Endergebnis unendlich viele Besucher generiert. Natürlich wird es in der Realität immer Schranken geben, die das Wachstum einer Seite begrenzen (und sei es nur die Größe der Zielgruppe). Das Ergebnis drückt jedoch aus, dass bevor diese Wachstumsschranken erreicht werden, die Seite unbegrenzt wächst, wenn gilt N/X>1. Man könnte also einen Word of Mouth Faktor größer gleich 1 als "Hype-Bedingung" formulieren."*

Mundpropaganda (Word of Mouth) wird eine zentrale Rolle für das Erreichen einer kritischen Masse zugewiesen. Während Metcalfe nur die Benutzer des Systems selbst betrachtet, die tatsächlich im Netz vorhanden sind, gehen die Betreiber von whatsyourplace weiter. Die Zahl an Personen, die über die bereits angemeldeten Benutzer geworben werden, ist signifikant für den Erfolg bzw. das Auslösen eines Hypezustands. Wenn jeder Benutzer (X) mehr als eine Person (N) zur Registrierung akquiriert, explodiert das System.

Abbildung 5 zeigt die Kurvenfunktion und das Erreichen von U*, der kritischen Masse. Laut den Betreibern ist es notwendig bis zum Erreichen der kritischen Masse klassisches Marketing einzusetzen, da die Variable Z durch Marketing steuerbar ist. Ab dem Überschreiten des kritischen Punktes können die Marketingaktivitäten reduziert werden, da die Benutzer der Plattform selbst virales Marketing (früher: „Mundpropaganda") im Freundeskreis starten.

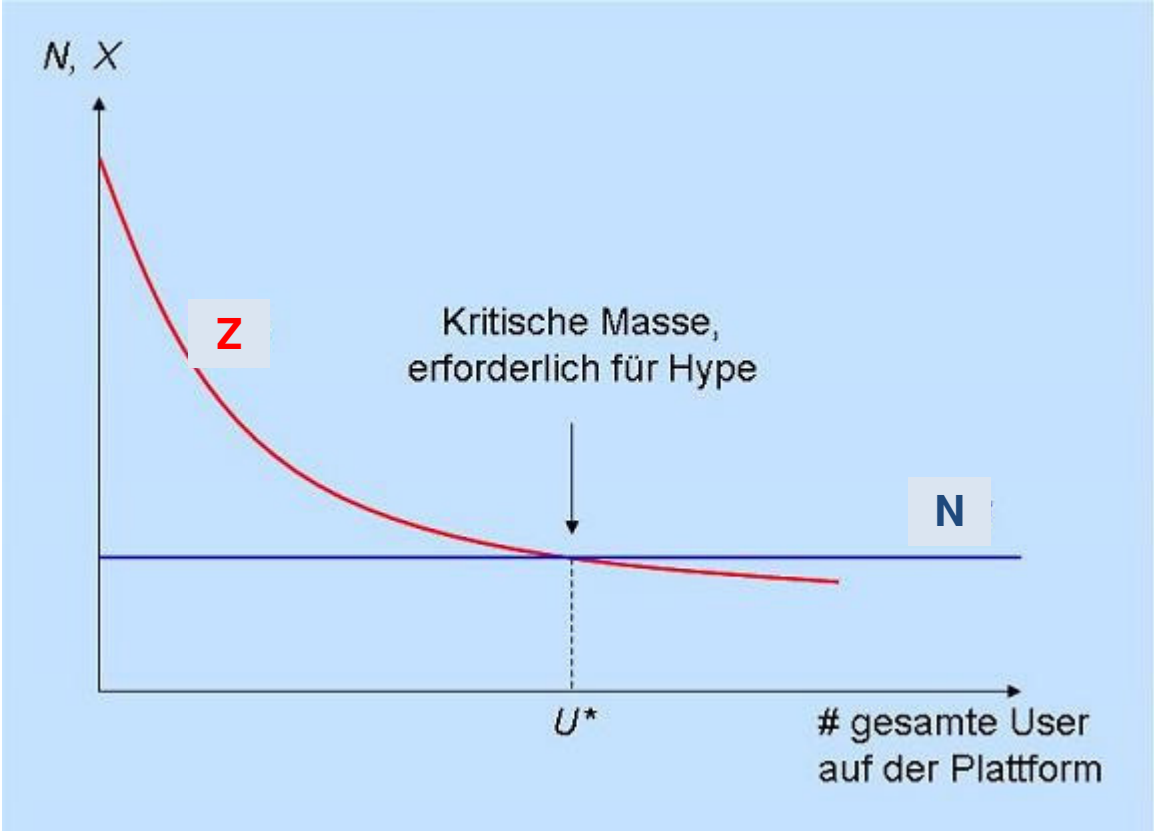

Abbildung 5: Die kritische Masse wird erreicht. (adaptiert nach whatsyourplace, 2008)

Diese Überlegung hat zur Folge, dass nachhaltiger Erfolg nur durch bezahltes Marketing möglich ist, denn die Anzahl der Personen Z, die ohne finanziellen Mitteln erreicht werden können (Freunde, Verwandtenkreis, …) ist zu gering um die kritische Masse zu erreichen. In Deutschland ist bisher keine einzige Community bekannt, die es ausschließlich durch virales Marketing geschafft hat, die kritische Masse zu erreichen. Ein Brancheninsider sagte zu den

Betreibern von whatsyourplace: „***Traffic muss man sich kaufen**, gerade am Anfang."* (vgl. whatsyourplace, 2008)

Im Gegensatz zum Erfolg bei den Nutzungszahlen ist der finanzielle Erfolg von Social Communities noch ungeklärt. Alle großen Anbieter befinden sich in den roten Zahlen. Geschäftsmodelle, die diesen Trend ändern könnten, fehlen oftmals (vgl. Mohr, 2007). Die Schaltung von Werbebannern ist aktuell die gängigste Form der Geschäftsmodelle. Die gespeicherten Daten der Nutzer stellen den Wert eines Netzes dar. Betreiber rechnen daher langfristig mit einer Konsolidierung bzw. einen Verkauf an größere (Medien-)Konzerne und haben ihre AGBs auf den Verkauf der Daten an Dritte ausgerichtet (s. Kapitel 4.1.8).

3.2.4. Rückgang der Verweildauer

Alle Statistiken zeigen, dass die Benutzerzahlen der sozialen Netzwerke steigen. Gleichzeitig ist der Höhepunkt der Verweildauer doch bereits bei vielen Plattformen erreicht und überschritten. Eine Statistik von Nielsen Online (siehe Abbildung 6) zeigt ein deutliches Bild:

> *„Reichweite und Verweildauer scheinen ihren Zenit in Deutschland - ebenso wie in Amerika - überschritten zu haben. Zudem liegt die durchschnittliche Verweildauer auf den MySpace-Seiten deutlich unter dem deutschen Durchschnitt, weil MySpace viel weniger für die Kommunikation genutzt wird […]"* (Schmidt, 2008)

Überraschend am Ergebnis: Alle Netzwerke haben in den Sommermonaten deutlich mehr Aktivitäten zu verzeichnen als in den zumeist stärkeren Wintermonaten. MySpace, das in Amerika zwischen 230-180 Minuten pro Monat genutzt wird, hinkt im Ranking den deutschsprachigen Communities deutlich hinterher. Business Communities wie Xing (40 Minuten) und LinkedIn (7 Minuten) sind ebenfalls am unteren Rande der Verweildauerstatistik zu finden.

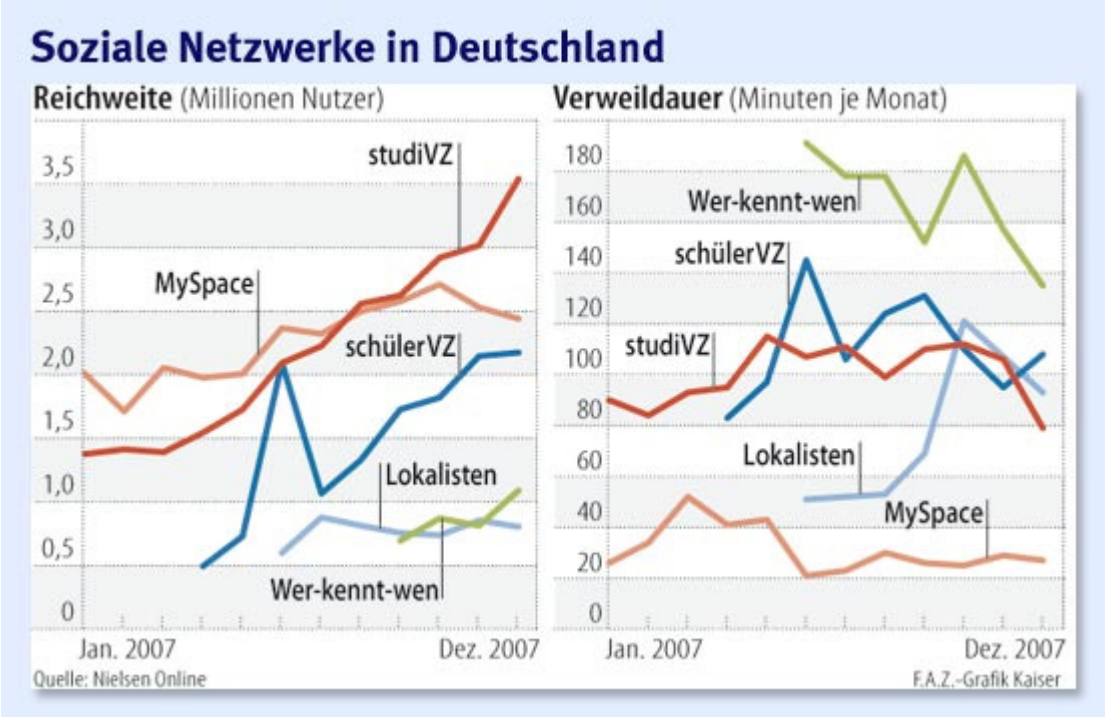

Abbildung 6: Nutzung von sozialen Netzwerken in Deutschland (vgl. Schmidt, 2008a)

Um dem Trend der sinkenden Verweildauer entgegen zu wirken, hat Facebook seine Hausaufgaben bereits erledigt. Durch die Ankündigung einer eigenen Instant Messaging Funktion könnten die Besuchszeiten deutlich steigen, und die Plattform damit an Wert steigern. Bereits im Vorfeld wurde die neue Funktion in Blogs beleuchtet, der Start hielt jedoch noch eine Überraschung bereit.

> "*The only thing new that we've learned is that Facebook Chat will incorporate minifeed stories into IM conversations. If you're chatting with someone and they do something to your profile, like post a message on your wall, you will get a notification into your chat window with them.*" (Hendrickson, 2008)

Die Chat-Funktionalität beinhält ebenfalls Informationen über die Benutzeraktivitäten auf Facebook außerhalb des Chats. Durch die Offenheit für Drittanbieter-Anwendungen in Facebook (s. Kapitel 4.1.1.2.2.) und dem Chat wird Facebook zu einer immer größeren Plattform, die in Zukunft wohl für weitere Innovationen offen ist. Eine dieser möglichen Innovationen stellt die Öffnung der Communities untereinander dar. Hierbei gibt es zwei Fraktionen, Die Data Portability und „Open Social" Initiative.

3.2.5. Data Portability, der Social Graph und die Bill of Rights

Benutzer von sozialen Netzwerken verbringen Stunden und Tage, um ihr Profil zu befallen, Kontakte zu finden und Nachrichten untereinander auszutauschen. Bisher sind diese Bemühungen immer auf einzelne Communities begrenzt. Möchte man sich bei einer zweiten Plattform registrieren, muss man erneut Stunden investieren, um alle Kontakte in dem neuen Netz wiederzufinden. Deswegen gibt es die Überlegung, dieses Inseldenken zu beenden:

> *„Die Idee hinter "DataPortability" klingt dabei eigentlich einfach: Die Nutzer der teilnehmenden Netzwerke sollen ihre Online-Freunde und die von ihnen hinterlegte Fotos, Videos und anderen Medien über alle Anwendungen, Miniprogramme (Widgets) und derzeit noch im Inselbetrieb existierenden Angebote hinweg stets erreichen können. Dazu müssen vorher neue Schnittstellen zum Informationsaustausch geschaffen werden - ein frischer digitaler "Kitt" zwischen den Netzwerken, der bislang kaum besteht. Dazu sollen vorhandene Protokolle, die jetzt schon offen geregelt sind, eingesetzt werden. […] Die Mitnahme von Freundesdaten kann zwar in den USA der aktuellen Gesetzeslage entsprechen, in europäischen Ländern sieht dies jedoch möglicherweise völlig anders aus."* (Schwan, 2008)

Während sich alle großen Anbieter wie MySpace, Facebook, Bebo, Google und bereits auch die deutschen Anbieter wie Xing zu Verbänden zusammenschließen und über den Datenaustausch über standardisierte Protokolle nachdenken, dürfte aus aktueller Sicht der Datenschutz eine entscheidende Rolle für das Gelingen/Scheitern des Vorhabens darstellen. Durch die verschiedenen Rechtsdefinitionen (s. Kapitel 3.1.5) ist es schwer einen gemeinsamen Nenner zu finden, der die Portability weltweit unterstützt.

Die technische Seite des Zusammenschlusses ist ebenfalls komplex. Jede Community repräsentiert einen „Social Graph", der die Beziehungen der Benutzer enthält:

> *„What I mean by "social graph" is a the [sic] global mapping of everybody and how they're related […] Unfortunately, there doesn't exist a single social graph (or even multiple which interoperate) that's comprehensive and decentralized. Rather, there exists hundreds of disperse social graphs, most of dubious quality and many of them walled gardens. […] Ultimately make the social graph a community asset, utilizing the data from all the different sites, but not depending on any company or organization as "the" central graph owner. "* (Fitzpatrick, 2007)

Die vielen Graphen haben unterschiedliche Qualität und meist äußerst verschiedene Merkmalsausprägungen. Während Facebook und studiVZ im Kern sehr ähnliche Benutzerdaten über ihre Benutzer, den Studenten, sammeln, ist eine Deckung der Attribute mit dem Social Graph von Xing nur äußerst gering. Der Weg, der in Zukunft eingeschlagen wird, lautet daher laut Fitzpatrick, dass Benutzer selbst Eigentümer von eigenen sozialen Graphen sein müssen. In den Grundrechten von sozialen Netzwerken (*„Bill of Rights"*) definieren Smarr et al 2007:

- *"**Ownership** of their own personal information, including:*
  - *their own profile data*
  - *the list of people they are connected to*
  - *the activity stream of content they create;*
- ***Control** of whether and how such personal information is shared with others; and*
- ***Freedom** to grant persistent access to their personal information to trusted external sites"*

Eine Frage, die gänzlich offen bleibt, ist jedoch die des Zwecks der Öffnung von Datenbeständen der Communities. Umfragen zeigen, dass nur wenige Benutzer von Social Communities tatsächlich mehr als 1 Netzwerk benutzen. (vgl. CSCM, 2008 und Kapitel 4.2.3). In erster Linie sind die angesprochenen Initiativen daher, momentan, noch nicht auf den Austausch von Daten innerhalb von Social Communities gedacht, sondern viel mehr um die Daten von Communities mit gänzlich anderen Web2.0 Diensten wie Flickr oder Twitter miteinander zu verbinden. Zukünftig wird der Zusammenschluss sozialer Netze funktionieren (s. Kapitel 4.3.2). Ein globales Netz an Informationen würde den Markt der Social Communities nachhaltig verändern und Vorteile für einzelne Benutzer schaffen. Eine andere Interessensgemeinschaft hat jedoch weit mehr Interesse daran, dass zukünftig die Aktivitäten von Benutzern zu einem gemeinsamen Netzwerk zusammenwachsen:

> *„Für Vermarkter dagegen wäre das soziale Supernetz eine völlig neue Plattform, die alles bisher Dagewesene in den Schatten stellt - ein Netzwerk, das womöglich jeden Einkauf bei Amazon, jeden Song-Download bei iTunes und jedes online gekaufte Konzert-Ticket an alle Freunde des Käufers weitermeldet - wo auch immer die sich aufhalten. Die Vermarkter jauchzen schon." (Stöcker, 2007a)*

3.2.6. Erweiterte Werbeformen in sozialen Netzwerken

Bis der globale Social Graph Realität geworden ist müssen sich Vermarkter und Betreiber nach anderen Werbeformen umsehen. Die bisherigen Bannerwerbungen werden zwar von Benutzern akzeptiert, jedoch selten angeklickt. Die tatsächliche Klick-Rate liegt bei 0,3 Prozent (vgl. Lischka, 2007a). Die Zugriffszahlen von den fünf größten OpenSocial-Partnern betragen im Monat September 2007 250 Millionen „unique visitors". (vgl. Stöcker, 2007b) Das zeigt, wie groß der Markt in Social Communities für Werbetreibende ist. Es müssen daher neue Werbeformen gefunden werden, die ähnlich der in Kapitel 3.2.3.2 beschriebenen kritischen Masse Benutzer fördern, Werbung aktiver wahrzunehmen.

> *„Bis auf wenige Ausnahmen setzt die Mehrheit der Social Networks auf Banner- und Kontextwerbung zur Finanzierung ihrer Plattformen. Diese einseitige Ausrichtung erweist sich für die Verwertung als Nachteil, da die beworbene Zielgruppe erst am Anfang ihrer Erwerbsexistenz steht, zunehmend werberesistent auftritt und eine erhöhte Klickmüdigkeit aufweist. Gleichzeitig weist die Zielgruppe eine im Vergleich überdurchschnittliche Medienkompetenz im Werbebereich aus; es steht deshalb zu erwarten, dass dieses Geschäftsmodell in naher Zukunft unter massiven Druck kommen wird"* (Speck, 2008)

Werbung in sozialen Netzen kann daher nur funktionieren, wenn Benutzer langfristig an eine Marke gebunden werden. Die Studie „CommunityEffects“, durchgeführt von der Tomorrow Focus AG, liefert grundlegende Aussagen darüber, welche Werbeformen für werbetreibende Unternehmen interessant sein können und zeigt, dass personalisierte Werbung, die bei allen großen Communities überlegt wird, nicht immer die einzige Form der Werbung darstellen muss. Die Umfrage hat ergeben, dass Community-Nutzer generell eine etwas höhere Toleranz gegenüber Online-Werbung haben. So definiert Inga Brieke (2008) in der Management Summary der Studie:

> *„Gesponserte Musik, Videos und Games treffen die zentralen Nutzungsinteressen der Community-Nutzer. Eine Auseinandersetzung mit dem Werbetreibenden durch die Kombination aus dezent kommunizierter Werbebotschaft, einem hohen Spaßfaktor und der indirekten Kommunikationsmöglichkeit mit anderen Nutzern ist besonders erfolgversprechend. Gut akzeptierte Standardwerbeformen wie Skyscraper und Superbanner sind hier die perfekte Ergänzung zu Community-spezifischen Werbeformen. […] Generell eignet sich jede Werbeform, die eine Interaktion erlaubt, für virale Kampagnen. Wichtig in der jungen Nutzerschaft von Social Networking-Angeboten ist die Selbstdarstellung in der Peer-Group. Besonders beliebt sind hier Musik, Games und virale Videospots. Bei Teens besitzen insbesondere Werbeformen ein hohes virales Potential, die sie dabei unterstützen, sich ihren Peers zugehörig zu fühlen (»WIR« mögen diesen Künstler, »WIR« tragen diese Marke, ...). Wichtig bei der Weiterleitung ist demnach die Kenntnis von geteilten Interessen und Vorlieben.“*

Ein erfolgreiches Beispiel für das angesprochene „Wir-Gefühl“ ist der Versuch von gesponserten Gruppen auf studiVZ oder Facebook. Als Beispiel sei die Gruppe „Apple auf StudiVZ/Facebook“ genannt, die regelmäßig Aktivitäten auf der Plattform durchführt, als Anlaufstelle für Probleme dient, und Rabatte beim Online Einkauf bietet. Durch die Teilnahme an einer gesponserten Gruppe verdeutlicht ein Benutzer die Sympathie zu einer Marke und kann sich mit weiteren Teilnehmern der Community austauschen. Bei dieser Form des Marketings werden zwar kurzfristig keine Gewinner erzielt, Benutzer jedoch mittelfristig an die Marke gebunden. Abbildung 7 zeigt das Ergebnis der Akzeptanz der verschiedenen Werbeformen.

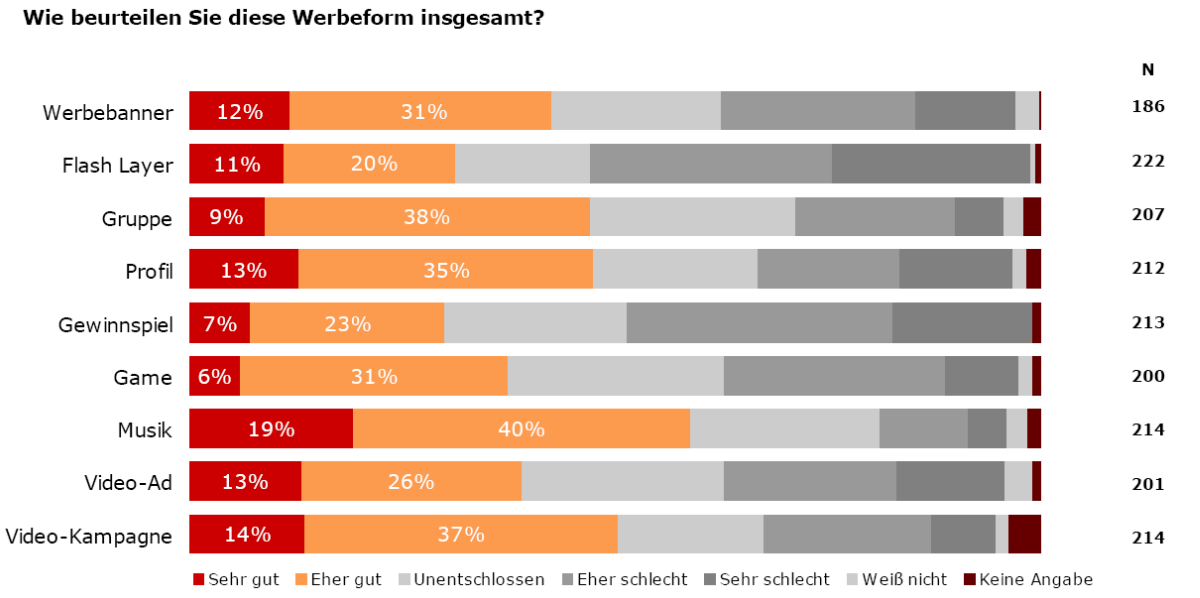

Abbildung 7: Werbeformen in Social Communities (übernommen nach Brieke, 2008)

Gewinnspiele und Games steigern die indirekte Wahrnehmung von Marken überdurchschnittlich gut. Musik und Videos haben die höchste Akzeptanz und Wirkung auf Benutzer. Das Anlegen von gesponserten Profilen zu neuen Hollywood-Filmen ist auf Plattformen wie Facebook und MySpace beliebt, in deutschsprachigen Communities jedoch erst in den Kinderschuhen.

4. Der Umgang mit den Daten in der Praxis

Das Kapitel über die theoretischen Grundlagen hat gezeigt, dass Datenschutz, Informationssicherheit, Privatsphäre und personalisierte Inhalte durchwegs heikle Themen sind. Im Web2.0 spielen diese Themen für viele Benutzer jedoch keine primäre Rolle. Blogs, Foren und nicht zuletzt Social Communities zum Austausch von Fotos, Videos, Musik und dem eigenen Wohlbefinden sind interaktive Plätze geworden, die vom so genannten „user generated content" leben. Soziale Netze zeigen es vor: Basierend auf dem "kleine Welt Phänomen" (s. Kapitel 3.2.1) wachsen die Plattformen, je mehr Benutzer sich registrieren und in Form von Beiträgen, Kommentaren und gegenseitigen Verlinkungen Daten miteinander verknüpfen. Die angesprochene Architektur des Partizipierens ist der Grund, warum sich das Web in den letzten Jahren massiv verändert hat. Jeder, der möchte, kann sein komplettes Leben im Internet publizieren (s. Kapitel 3.1.4). Dabei gilt jedoch, dass es natürlich auch für fast jeden möglich ist, diese Informationen wiederzufinden. Deswegen ist der Umgang mit den Daten in zweierlei Hinsicht entscheidend:

- **Die Sicht des Benutzers:**
  Welche Daten publiziere ich über mich im Internet?

- **Die Sicht des Betreibers:**
  Welche Vorkehrungen treffe ich, um Datenschutz und –sicherheit auf meiner Plattform zu forcieren, um meinen Benutzern zu helfen? Inwieweit ist fehlender Datenschutz ein Vorteil für meine Benutzer, die einfacher Informationen über Mitglieder auffinden können?

Bevor die Sicht der Benutzer selbst durch die Auswertung einer Umfrage analysiert und kommentiert wird, zeigt der Vergleich von namhaften Communities wie der Schutz von Daten in der Praxis gehandhabt bzw. ausgenutzt wird, um zukünftige Geschäftsmodelle einzuführen.

4.1. Vergleich von Datenschutzbemühungen einzelner Community-Betreiber

Jeder Community-Betreiber ist um zufriedene Benutzer bemüht. Um Benutzer auf die eigene Plattform aufmerksam zu machen, wird viel Geld in die Werbung und die Entwicklung innovativer Features gesteckt. Oftmals schreien besorgte Benutzer dennoch auf. Sei es das Anbieten von personalisierter Werbung oder Aktivitätsübersichten[8], die die letzten Aktivitäten von Kontakten auf einer Plattform kompakt zusammenfassen. Anbieter vergessen ihre Benutzer einzubinden, und an datenschutzrechtliche Probleme zu denken.

Aus diesem Grund wird im ersten Schritt des Kapitels beleuchtet, wie der Datenschutz in 5 beliebten Communities gehandhabt wird. Der Anmelde- sowie Abmeldeprozess, bzw. das tägliche Leben in den Communities wird beleuchtet und in Bezug auf Datenschutz und Informationssicherheit kritisch hinterfragt. Ein Vergleich der Nutzungsbedingungen beantwortet die Frage, welche Daten in den Communities gespeichert werden und welche Klauseln Benutzer (unwissentlich) akzeptieren.

Da eine Vielzahl an Social Communities in den letzten Monaten/Jahren entstanden sind und es alleine in Deutschland über 100 davon gibt (vgl. Weigert, 2007a) kann nur eine geringe

[8] im englischen unter „Mini-Feed" bekannt

Anzahl in der Arbeit für die Überprüfung herangezogen werden. Der Autor hat sich daher für den Vergleich von fünf äußerst verschiedenen Plattformen entschieden, die jedoch alle in den letzten Monaten wegen ihrer Datenschutzbemühungen in die Medien kamen.

Das nächste Kapitel bietet eine Einführung und Beschreibung der Plattformen und beleuchtet welche positiven und negativen Themen die Plattformen in die Medien brachten. Im Anschluss daran werden die Plattformen datenschutzrechtlich unter die Lupe genommen und miteinander verglichen.

4.1.1. Vorstellung der ausgewählten Plattformen

Die nachfolgende Tabelle zeigt eine Übersicht über die ausgewählten Plattformen, die im nächsten Kapitel analysiert werden:

Name	Herkunft	Typ	Interest
MySpace	Amerika	Kommerziell	General
Facebook	Amerika	Kommerziell	General
studiVZ	Deutschland	Kommerziell	General[9]
kaioo	Deutschland	Gemeinnützig	General
Xing	Deutschland	Kommerziell	Special

Tabelle 3: Vorstellung der ausgewählten Plattformen

Die Gründe für die Auswahl sind vielschichtig. Einerseits stellt MySpace das mit Abstand größte soziale Netzwerk der Welt dar. Gemeinsam mit Facebook, dem aktuell größten Konkurrenten von MySpace, werden beide Plattformen in Amerika betrieben. Die deutschsprachigen Vertreter sind wegen ihres Fokus auf deutschsprachige Benutzer deutlich kleiner, dementsprechend hierzulande allerdings um einiges beliebter. Als Underdog wird das Netzwerk von kaioo beleuchtet, das als einziger Vertreter im Feld als gemeinnütziger Verein geführt wird.

In der Vorstellung wird bewusst auf angebotene Funktionen der Plattformen verzichtet und nur auf relevante Themenbereiche eingegangen.

4.1.1.1. MySpace

MySpace.com ist die größte Social Community der Welt und laut dem Statistikdienst Alexa die 5. meist besuchte Seite im World Wide Web. (Stand: April 2008[10]) Die Plattform besitzt je nach Quellenangabe 200 bis 300 Millionen Benutzer. (vgl. 300 Millionen in Reissmann, 2008, 230 Millionen laut Myspace.com/tom, 200 Millionen laut Göldi, 2008), wovon sich rund 68 Millionen Benutzer pro Monat einloggen. Im Jahr 2005 wurde die Seite von der News Corporation für 580 Millionen USD gekauft. Während Tom Anderson, einer der Gründer von MySpace, behauptete, dass die Seite in dessen Garage entstand, kam es im Oktober 2006 zu einem Bericht, der diese Aussage wiederlegt. MySpace wurde dem Bericht zufolge von der Firma eUniverse ins Leben gerufen wurde. Erst durch eine Werbekampagne wurde der enorme Erfolg der Seite ausgelöst (s. Kapitel 3.2.3.2).

Statistiken wie die „February Top Social Networks“ (vgl. Freiert, 2008) zeigen, dass MySpace am Zenit seines Erfolgs angekommen sein dürfte. Erstmals deutet sich nicht nur ein Absin-

[9] StudiVZ wird als General Interest Community geführt, da die Benutzerzahlen zeigen, dass die Plattform nicht nur von Studenten genutzt wird (3,5 Millionen Studenten im deutschsprachigen Raum zu 4,8 Millionen Benutzern, vgl Schmidt, 2008b)

[10] http://www.alexa.com/site/ds/top_sites?ts_mode=global&lang=none

ken der Verweildauer (s. Kapitel 3.2.4) sondern auch ein Absinken der Zugriffe auf die Plattform ab. Obwohl MySpace knapp 3 Mal so viele Visits pro Monat hat wie das zweitplatzierte Facebook, sind es vor allem „kleine" Communities, die ihre Aufmerksamkeit auf sich ziehen. So konnten Twitter und Ning ihre Besuchszahlen im gleichen Zeitraum um den Faktor 5 steigern. (vgl. Freiert, 2008) Vor 2 Jahren sah das Bild für MySpace dagegen noch ganz anders aus, bei dem MySpace ein Wachstum um den Faktor 3.6 im Zeitraum von April 2005 – April 2006 vorweisen konnte. (vgl. Nielsen//NetRatings[11], 2006)

Dass die größte Social Community der Welt schon des Öfteren wegen dem Datenschutz und der Informationssicherheit in den Medien war, zeigen die folgenden Beispiele. Die Erfahrungen des Autors mit MySpace und deren offensichtlichen Problemen beschreibt das Kapitel 4.1.3.

Samy
Bereits 2005 kam es zu einem folgenschweren Fehler auf der Seite, weswegen MySpace für mehrere Stunden offline genommen werden musste. Durch eine XSS Lücke gelang es „Samy", dass innerhalb von 20 Stunden 1 Million Profile mit dem „Virus" infiziert wurden. Besuchte ein eingeloggter MySpace Benutzer ein infiziertes Profil eines Freundes, wurde automatisch eine Freundesanforderung an den Autor initiiert und akzeptiert. Das Vorfinden der Aussage „*but most of all, Samy is my hero"* war damals Indiz für eine infizierte Seite. Der Autor des Virus hatte außer dem Verlinken seines Profils keine weiteren Hintergedanken. Personendaten wurden zum Glück von MySpace nicht gestohlen. Dennoch: Der Samy Virus geht in die Geschichtsbücher ein, gilt er heute immer noch als der sich am schnellst verbreiteteste Virus aller Zeiten (vgl. Mook, 2005 und Lenssen, 2005).

Dass die Betreiber der Plattform nur wenig dazugelernt haben, zeigt der nächste Fall.

Nutzerdaten zum Download und Sexualstraftäter
Im Jänner 2008 wurde in Tauschbörsen eine 17 Gigabyte große Datei veröffentlicht, die mehr als eine halbe Million Fotos von MySpace Profilen beinhaltete.

> *„The creator of the file says he compiled the photos earlier this month using the MySpace security hole that Wired News reported on last week. That hole, still unacknowledged by the News Corporation-owned site, allowed voyeurs to peek inside the photo galleries of some MySpace users who had set their profiles to "private," despite MySpace's assurances that such images could only be seen by people on a user's friends' list."* (Poulsen, 2008b).

Obwohl die Profildaten als privat markiert wurden, konnten diese durch eine Lücke im System, die bereits Tage zuvor veröffentlicht wurde, ausgespäht werden. Poulsen, ehemaliger Hacker und nun Journalist bei der Webseite „wired.com" hat 2006 selbst seine Erfahrungen mit MySpace gemacht. Er hat rund ein Drittel aller MySpace Nutzer damals mittels eines simplen Programms gescannt und mit der amerikanischen Datenbank für Sexualstraftäter verglichen. Dabei fand Poulsen heraus, dass 744 Personen aus der Täterdatei auf MySpace registriert waren. 497 davon waren als pädophile Straftäter vermerkt. Einem mehrfach verurteilten Mann konnte detailiert sein Kontakt zu minderjährigen nachgewiesen werden, obwohl ihm dies gerichtlich strengstens untersagt wurde. (vgl. Merschmann, 2006). Ein Jahr später wurden nach einem drastischen Anstieg 29.000 Benutzerprofile von Sexualstraftätern aus Amerika gelöscht. (vgl. BBC, 2007). In Großbritannien setzt sich indes Innenministerin Jacqueline Smith dafür ein, dass sich Sexualstraftäter gar nicht mehr in Social Communities registrieren dürfen. Pläne, wie dies mit Betreibern gemeinsam umgesetzt werden können, soll das extra dafür gegründete „Child Exploitation and Online Protection Centre" entwickeln.

[11] Die Firma Nielsen//NetRatings macht darauf aufmerksam, dass in Zitaten immer nur der Firmenname verwendet werden soll. Daher entfällt in diesem Fall der Autorenname.

Geben Straftäter eine falsche E-Mail-Adresse ein, so soll dafür bis zu 5 Jahre Haft drohen. (vgl. Heise, 2008)

Phishing Attacken
Die Vielzahl der Benutzer von MySpace macht die Seite zum Risiko. Durch die mangelhaften Implementierungen (s. Kapitel 4.1.3) ist es für Benutzer schwierig zu erkennen, ob sie sich auf den offiziellen MySpace-Seiten befinden. MySpace wurde in den letzten Wochen vermehrt durch Phishing-Angriffe vor Probleme gestellt. Der Eigentümer selbst, Tom Anderson, spricht in seinem MySpace-Profil offen über den Ernst der Lage und zeigt einige der in Umlauf befindlichen Webseiten. In seinem Beitrag, der sich an alle MySpace-Benutzer richtet, appelliert er an die Benutzer sich nur nach eigenhändiger Eingabe der MySpace-Domain im System einzuloggen (vgl. Anderson, 2008).

Das Geschäft mit beliebten Profilen
Ein völlig neues Geschäftsmodell für Benutzer zeigt folgendes Zitat:

> *„Auch My-Space-Profile mit tausenden Freunden kann man im Internet kaufen um kostengünstig Spams über die „Bulletin" Funktion zu verschicken. Neuerdings gibt es auch Programme die automatisch Freunde einladen um diese dann wieder mit Spams zu nerven"* (Medienkulturzentrum, 2008a)

Am Beispiel MySpace wird klar, wie schwer es soziale Netzwerke haben, wenn sie erfolgreich sind. Bei einer potentiellen Benutzerzahl von 300 Millionen Menschen ist die Gefahr der unrechtmäßigen Nutzung deutlich größer, als bei kleinen Communities wie kaioo mit wenigen tausend Mitgliedern. Der Aufwand, der vor allem in die Informationssicherheit investiert werden muss, muss also ebenfalls ähnlich wie MetCalfes Law mit den Benutzerzahlen der sozialen Netzwerke steigen. Das Ökosystem von MySpace galt lange Zeit als in sich abgeschlossen. Durch die enorme Benutzerzahl gegenüber allen anderen sozialen Netzen und der daraus entstehenden Freundesnetzwerke konnte man sich lange Zeit die unflexible Struktur und das Blocken externer Dienste leisten. Mit dem immer stärkeren Aufkommen von Facebook dagegen, musste man handeln. Der Anschluss an die Data Portability Initiative kann als Öffnung dieses autoritären Systems angesehen werden. (vgl. Weigert, 2007b) Der Beitritt zur Initiative wird vermutlich nicht der letzte Schritt zu einer weiteren Öffnung von MySpace bleiben.

4.1.1.2. Facebook

Facebook ist im amerikanischen Raum als „The Facebook" gestartet und richtete sich in seinen ersten Monaten ausschließlich an Studenten. Durch den raschen Erfolg öffnete man sich Anfang 2006 ebenfalls auch für alle Nicht-Studenten. Facebook gilt durch seine Architektur (s. Kapitel 4.1.1.2.2.) als technisch innovativer Herausforderer von MySpace. Die Seite wurde von Mark Zuckerberg gegründet. 2007 kaufte Microsoft 1,6 Prozent von Facebook um die Summe von 240 Millionen USD, gleichbedeutend hat Facebook einen Marktwert von 15 Milliarden Dollar. (vgl. Welt Online, 2007a). Aktuellen Zahlen zufolge hat die Plattform rund 60 Millionen Mitglieder. Täglich kommen an die 250.000 hinzu. (vgl. Reissmann, 2008).

Ein Deutschlandstart Anfang März 2008, das Werbetool *Beacon*, die Öffnung für Applikationen von Fremdanbietern sowie die Veröffentlichung eines Instant Messaging Programs (s. Kapitel 3.2.4) brachten die Plattform in den letzten Monaten vermehrt in die Medien. Doch die Meldungen beinhalten auch oft negative Kritikpunkte, wie die fehlende Möglichkeit der Abmeldung, sowie Proteste gegeben personalisierte Werbung und Mini-Feeds.

Worum es sich bei dem Facebook Werbesystem handelt, erklärt eine Pressemeldung aus dem Jahr 2007:

> *"Facebook today announced that 12 of the world's largest brands and companies have immediately committed to using Facebook Ads, an ad system that enables people to provide trusted referrals to their friends and helps businesses to spread information through the social graph and communicate with their customers in completely new ways. With Facebook Ads, users can learn about brands and businesses through trusted referrals from their friends on Facebook. Advertisers can connect with users by creating a presence on Facebook and targeting the exact people they want"* (Facebook, 2007)

Die Idee von Facebook, Einkäufe bei den angemeldeten Partner von Benutzern aufzuzeichnen und Freunden per News Feed mitzuteilen lies Benutzer und Datenschützer aufschreien. Der Zeitpunkt der Veröffentlichung dieser Funktion war sehr ungünstig gewählt, denn Benutzer mussten mit ansehen, wie alle Bekannten per Facebook über die geheimen Weihnachtsgeschenke informiert wurden, die man sich untereinander machen wollte. (vgl. Welt Online, 2007b) Facebook hat daraufhin die Funktion zurückgezogen und sich für das Verhalten entschuldigt:

> „*Its grand attempt to redefine the advertising industry by pioneering a new approach to social marketing, called Beacon, failed completely. Facebook's idea was to inform a user's friends whenever he bought something at certain online retailers, by running a small announcement inside the friends' "news feeds". In theory, this was to become a new recommendation economy, an algorithmic form of word of mouth. In practice, users rebelled and privacy watchdogs cried foul. Mark Zuckerberg, Facebook's founder, admitted in December that "we simply did a bad job with this release" and apologised.*" (Economist, 2008)

Bereits 2006 gab es Probleme mit dem angesprochenen News Feed, der bereits damals für Datenschutzbesorgnis sorgte, da die Befürchtung, dass „Stalking" von Benutzern nun noch einfacher wäre, aufkam. Die Funktion wurde optional deaktivierbar und heutzutage ist die Aktivitätsübersicht auf Plattformen wie Facebook, MySpace und Xing Standard. (vgl. Anon, 2006) Bereits 2005 wurde die Community in mehreren kritischen Berichten auf Sicherheitsprobleme analysiert. So fanden zum Beispiel Jones und Soltren (2005, S. 25) Möglichkeiten zur Datenbankmanipulation, dem Auslesen von Passwörtern bzw. dem Umgehen der Zugriffsrechte heraus.

4.1.1.2.1. Die Eigentümerverhältnisse

Einen durchaus skeptischen Blick hinter die Kulissen warfen der Guardian und Herr Agarwala (2006). Beide untersuchten die Eigentümerverhältnisse von Facebook etwas genauer und fanden verblüffende Ergebnisse:

> *"Facebook is a well-funded project, and the people behind the funding, a group of Silicon Valley venture capitalists, have a clearly thought out ideology that they are hoping to spread around the world. Facebook is one manifestation of this ideology. Like PayPal before it, it is a social experiment, an expression of a particular kind of neoconservative libertarianism. […] the real face behind Facebook is the 40-year-old Silicon Valley venture capitalist and futurist philosopher Peter Thiel. There are only three board members on Facebook, and they are Thiel, Zuckerberg and a third investor called Jim Breyer from a venture capital firm called Accel Partners. […] On the board of such US giants as Wal-Mart and Marvel Entertainment, he is also a former chairman of the National Venture Capital Association (NVCA). Now these are the people who are really making things happen in America, because they invest in the new young talent, the Zuckerbergs and the like. Facebook's most recent round of funding was led by a company called Greylock Venture Capital, who put in the sum of $27.5m. One of Greylock's senior partners is called Howard Cox, another former*

> *chairman of the NVCA, who is also on the board of In-Q-Tel. What's In-Q-Tel? Well, believe it or not (and check out their website), this is the venture-capital wing of the CIA. In-Q-Tel's first chairman was Gilman Louie, who served on the board of the NVCA with Breyer. Another key figure in the In-Q-Tel team is Anita K Jones, former director of defence research and engineering for the US department of defence, and - with Breyer - board member of BBN Technologies."* (Hodgkinson, 2008)

Die Zusammenhänge zwischen Facebook, Thiel, Breyer, Jones und Louie zeigen enge Verbindungen zu der Central Intelligence Agency, dem Department of Defense und dem Information Awareness Office, das nach den Anschlägen des 11. Septembers gegründet wurde. Ob Facebook tatsächlich Geheimdienstorganisationen in Amerika nahe steht, oder es sich hierbei nur um einen Zufall bzw. eine Verschwörungstheorie handelt, ist nicht restlos aufklär bar. (Zukünftige) Benutzer sollten jedoch über diesen Umstand informiert werden, bevor Sie eine *Mitgliedschaft auf Lebenszeit* (s. Kapitel 4.1.4.1) bei Facebook eingehen. Denn abseits der bisherigen Datenbestände der (US-)Bürger könnte mit den Informationen aus Facebook ein detailiertes Netz an Informationen erstellt werden, das jede bisherige Ansammlung an personenbezogenen Daten bei weitem übertreffen würde. Facebook ist daher nicht nur wegen der in den Nutzungsbestimmungen definierten Regelungen, sondern auch aufgrund des unklaren Umfelds für europäische Benutzer nicht zu empfehlen.

4.1.1.2.2. Offen für fremde Applikationen

Facebook hat früh die Möglichkeiten einer Öffnung seiner Plattform für Drittanbieter erkannt. Die vorgestellte „Facebook Platform" ermöglicht das „Installieren" von Applikationen in das eigene Profil. Diese sogenannten „*Facebook Platform Applications*" werden nicht direkt von Facebook selbst, sondern von außenstehenden Firmen entwickelt. Facebook liefert dazu eine Dokumentation der Möglichkeiten zur Einbindung in die Community.

> *„Facebook-Anwendungen - inzwischen gibt es etwa 7000 davon - laufen aber nur innerhalb von Facebook. Einschränkend muss man sagen: Von den Tausenden von Anwendungen werden nur die wenigsten wirklich genutzt. Eine Studie des O'Reilly-Verlages ergab kürzlich: 87 Prozent der Nutzung entfällt auf nur 84 Anwendungen. Wirklich populär sind nur einige wenige, geschaffen von einer Handvoll spezialisierter Entwickler."* (Stöcker, 2007)

Zukünftig soll durch Data Portability gewährleistet werden, dass ähnliche Applikationen über die Grenzen von Social Communities entwickelt und benutzt werden können. Die Vielzahl an aktuellen Applikationen wird durch die Aussage von O'Reilly stark reduziert. In der Liste an unzähligen Zusatzfunktionen für Facebook findet man nicht immer nur nützliche Erweiterungen, sondern auch Spyware. Programme, die erst am Client installiert werden müssen, sollten daher dringlich vermieden wären, wie folgendes Zitat zeigt:

> *"Apparently, one of those annoying "who do you like" Facebook applications called Secret Crush actually downloads and installs spyware on your computer. The application appears no different from other similar ones: it appears in your profile, saying that someone has a "secret crush" on you. Eager to find out who the secret admirer is, you install it, and instead of some lovin', you get the infamous Zango spyware."* (Schroeder, 2008)

Plattformanwendungen, egal ob böswillig oder nicht, haben aus Sicht des Datenschutzes noch ein sehr großes Problem: Alle in Zusammenhang stehenden Daten werden nicht bei Facebook, sondern bei den Drittherstellern gespeichert. In den AGBs von Facebook (s. Kapitel 4.1.4) wird daher auch jede Gewährleistung auf Schutz der Daten in Zusammenhang mit den Applikationen ausgeschlossen. Benutzer müssen bei Verwendung dieser Dienste also damit rechnen, dass ihre (personenbezogenen) Daten nicht nur bei Facebook gespeichert werden.

4.1.1.3. studiVZ

Die Social Community studiVZ.net startete im Oktober 2005 und nahm sich zum Ziel eine „*Netzwerkkultur an europäischen Hochschulen zu etablieren und damit universitäre Grenzen zu überwinden*“. (Bonow, 2006). Bereits 10 Monate nach dem Start der Plattform wuchs das damalige studiVZ schneller als die Business-Plattform Xing. Aktuell hat die Plattform rund 4,8 Millionen Mitglieder.

Aktuell sind die von der studiVZ Limited betriebenen Seiten studiVZ.net und schuelervz.net die zwei größten Webseiten Deutschlands. Im internationalen Vergleich zeigt sich jedoch, dass studiVZ nicht in der gleichen Liga wie MySpace oder Facebook mitspielt.

	studiVZ	Facebook	MySpace
Benutzerzahlen	4,8 Millionen	60 Millionen	300 Millionen
Mitarbeiter	Etwa 100	Etwa 400	Etwa 300
Wachstum/Tag		+ 250.000	
Page Impressions (Dezember 2007)	5,3 Mrd.	403 Mrd.	1.178 Mrd.

Tabelle 4: Vergleich von studiVZ, Facebook und MySpace (vgl. Reissmann, 2008)

Tabelle 4: Vergleich von studiVZ, Facebook und MySpace zeigt, dass bei den Benutzer- und Mitarbeiterzahlen ein großes Ungleichgewicht zwischen studiVZ und den Branchenprimen herrscht. Während bei studiVZ 1 Mitarbeiter auf 48.000 Mitglieder kommt, ist dies bei MySpace 1 Mitarbeit auf 1 Million Mitglieder.

Im Februar dJ kam mit meinVZ.net eine dritte Community hinzu. Die Notwendigkeit zu diesem Schritt zeigt folgende Gegenüberstellung: Während es im deutschsprachigen Raum aktuell 3,6 Millionen Studenten gibt, verzeichnet die Studentencommunity bereits über 4 Millionen Mitglieder. Was als Plattform für Studenten anfing, wurde schnell von einer breiteren Bevölkerungsschicht benutzt. Um diesem Trend, der den Sinn einer Community für Studenten zerstört, entgegenzuwirken und eine größere Zielgruppe erreichen zu können, wurde daher eine dritte Community der studiVZ Ltd für alle deutschsprachigen Personen (http://meinvz.net/) geschaffen.

Die Plattformen von studiVZ sind im deutschsprachigen Raum definitiv Branchenführer. Die angebotenen Funktionalitäten und das Layout sind jedoch lediglich abgekupfert. studiVZ wurde in weiten Teilen von Facebook kopiert. Das Facebook-Blau wurde durch ein Rot, das aus dem amerikanischen bekannte „to poke“ mit dem deutschen Kunstwort „gruscheln“ (Zusammensetzung aus grüßen und kuscheln) ersetzt. Selbst der Funktionsaufwand ist in weiten Teilen ident zu dem des großen Bruders. Ende 2006 hat Michael Bumann einen Artikel verfasst, der die Gemeinsamkeiten im Layout aufzeigt. Dabei wird klar, dass studiVZ tatsächlich 1:1 von Facebook kopiert wurde. Attributnamen im HTML/CSS-Code wurden übernommen, Grafiken wurden gleich wie im amerikanischen Original genannt und das von Bumann zur Verfügung gestellte Stylesheet, das studiVZ in das bekannte Facebook Blau einfärbt, funktioniert tatsächlich 2 Jahre später, nachdem die Plattform bereits komplett neu entwickelt wurde, immer noch, wie Abbildung 8 zeigt. Eine Fehlermeldung von studiVZ im Jahr 2006 zeigte ebenfalls den Namen „Fakebook“ als Applikationsnamen.

Abbildung 8: studiVZ im Facebook-Blau (nachgestellt laut Bumann, 2006)

studiVZ ist ein Klon, der offensichtlicher nicht sein könnte. Selbst betreibt man aber eine sehr harsche Politik gegen Namensvetter. So wurden im Februar 2008 alle Webseitenbetreiber von Rechtsanwälten abgemahnt, die das Kürzel VZ (=Verzeichnis) im Domainnamen nutzen möchten. (vgl. Siebert, 2008)

Einen großen Einfluss von studiVZ auf den Alltag kann nicht abgestritten werden. Die in Österreich durchgeführte Wahl zum Wort des Jahres 2007 zeigte, dass der studiVZ Ausdruck „gruscheln“ auf Platz 2 landete. (vgl. Muhr, 2007)

Eine komplette Auflistung aller Pannen und Sicherheitsprobleme, die studiVZ in den letzten 2 Jahren hatte, würde den Rahmen der Arbeit sprengen. Es wird daher auf einige wenige Punkte eingegangen, die das Umfeld analysieren. Mit (*) markierte Termine sind aus einer Auflistung von „daburna.de“ übernommen, die alle Fehltritte von studiVZ gesammelt und historisiert hat. (vgl. Anon, 2008)

Historie
01.11.2006 (*): In einer studiVZ Fehlermeldung ist das Wort „Fakebook“ zu lesen. Es wird entdeckt, dass Dennis Bemmann die Domains unister.at und studylounge.co.uk registriert hat. Sowohl Unister als auch Studylounge sind Konkurrenzplattformen. Vorwürfe des sogenannten Domain-Grabbings seitens studiVZ kommen auf. Die Gründe für Domain-Grabbing zeigen Schumacher et al 2002 auf:

> *„Ein Fall von Domain-Grabbing liegt vor, wenn eine Domain zu dem Zweck registriert wird, einen Namens- oder Kennzeicheninhaber an der Nutzung seines Zeichens als Domain zu hindern, zumeist verbunden mit dem Ziel, ihn zur Zahlung einer Geldsumme für die Überlassung der Domain zu veranlassen.“*

studiVZ, das wie bereits beschrieben, selbst im Jahr 2008 gegen VZ Domains vorgeht, sicherte sich zum Zweck der Hinderung möglicher Konkurrenten Domains im deutsch- und englischsprachigen Raum. Ein Test des Autors für die Domain unister.at zeigt am 16.04.2008, dass die Domain nicht mehr im Besitz von studiVZ, sondern nunmehr in den Händen der Unister GmbH steht. Die Domain studylounge.co.uk ist zum heutigen Zeitpunkt immer noch im Besitz von studiVZ.

08.11.2006 (*): Es wird bekannt, dass sich Ehssan Dariani die Domain voelkischer-beobachter.de registriert hat. Die Domain ist zum Zeitpunkt des Verfassens der Arbeit immer noch auf Ehssan Dariani registriert.

> *„Nicht nur, dass der 26-jährige Startup-Gründer nächtens durch Berlin streift und bizarre Filme von Frauen veröffentlicht, zum Beispiel aus der U-Bahn oder von einer Party-Toilette (vielsagender Titel: "chick auf mitte party // WC"). Schon vor Monaten sicherte sich Dariani die Adressen voelkischer-beobachter.de und voelkischerbeobachter.de. Die Seiten wurden mit einem überarbeiteten Titelblatt der Nazi-Zeitung verziert - eine Party-Einladung sollte das sein. Immerhin thronte der Reichsadler nicht auf einem Hakenkreuz, sondern auf dem Logo von studiVZ. Die Publikation wurde "Kampfblatt der Vernetzungsbewegung Europas" genannt.“ (Meusers, 2006 und Stöcker, 2006)*

18.11.2006 (*): Angebliche Bestechungsversuche gegen einen Betreiber eines Blogs, damit dieser keine negativen Beiträge mehr verfasst.

20.11.2006 (*): Erwähnter Blogger zeigt, dass private Bilder öffentlich zugänglich sind. Der Datenschutzbeauftragte von studiVZ meldet sich zu Wort und erklärt, dass die Sicherheitsbedenken unbegründet sein.

22.11.2006 (*): studiVZ erklärt den am Vortag bekannt gewordenen Fehler einfach zum Feature.

23.11.2006 (*): Es wird bekannt, dass eine angeblich 700 Mann starke Stalkergruppe auf studiVZ existiert, die ohne dem Einverständnis der ausgewählten Frauen Miss-Wahlen veranstalten und sich gegenseitig über „interessante Frauen“ berichten. Ein Mitglied dieser Gruppe schreibt: „Und noch eine „Gruftschlampe“ diesmal ganz nah aus dem gleichen Wohnheim (leider noch vergeben) …“ Wenige Minuten später: „hab vor lauter sabbern mal wieder den namen [sic] vergessen mitzuteilen: ….“. Nachdem die ersten 2 gewählten „Miss studiVZ“ die Community verlassen haben und sich die Beschwerden bei dem studiVZ Support mehren, meldet sich dieser bei dem Gründer der Gruppe:

> *„Grundsätzlich wollen wir hier eigentlich keine Zensur betreiben, müssen aber solchen Beschwerden eben nachgehen. Zuerst, okay ich bin ein Mann – also erster Eindruck… Ne, ernsthaft: die Inhalte in deiner Gruppe sind absolut okay – es geht ja quasi nur um einen Fotocontest und nicht um irgendwelche Beleidigungen […] P.S.: Einer der Gründer (Michael B….. hätte übrigens gerne ne Einladung für die Gruppe… - ich würd mich dann da auch anschließen ;) […] post heil“* (Meyer, 2006).

Vor allem die Verabschiedung des Supports mit „post heil“ sowie die Tatsache, dass die Gruppe als „absolut okay“ deklariert wird, und man selbst dazu beitreten mag, zeigt die Unfähigkeit der Führungsmannschaft von studiVZ, Probleme innerhalb der Community zu lösen und ernsthaft zu behandeln. Bestimmungen der eigenen AGB schließen Aktionen wie das in der Gruppe praktizierte „Gruppengruscheln“ von Personen aus. Dennoch wird die Gruppe nicht geschlossen.

27.11.2006 (*): Durch eine XSS-Lücke wird studiVZ angegriffen. 32 Nutzer sind betroffen.

28.11.2006 (*): studiVZ entwickelt gemeinsam mit seinen Mitgliedern einen Verhaltenskodex. In Blogs wird beschrieben, wie die sicher scheinenden Profil-Identifikationsnummern, die aus alphanumerischen Zeichen bestehen, in einfache, aufsteigende Zahlen umgerechnet werden können.

30.11.2006 (*): Ein Fehler wird gefunden, der es ermöglicht, sich selbst in private Gruppen einzuladen. Eine weitere XSS Lücke ist entdeckt worden. studiVZ zahlt für jeden gefundenen

Fehler eine Belohnung von 256 EUR. Ein eigens dafür vorgesehenes Testsystem wird installiert.

14.12.2007 (*): Neue AGBs werden per E-Mail verschickt und beinhalten das Recht auf Nutzung aller persönlichen Daten. Es soll ebenfalls zu Werbung per SMS und Instant Messaging Programmen kommen. Nach einem großen negativen medialen Echo erklärt studiVZ, dass keine Daten von Nutzern verkauft würden.

Der Verbraucherzentrale Bundesverband hat die Betreiber 3 Monate später abgemahnt.

> *„Die Verbraucherschützer kritisieren, dass studiVZ sich die umfangreiche Erklärung zur Verwendung persönlicher Daten mit einem einzigen Klick bestätigen lässt. Dabei werde nicht hinreichend deutlich, welche Informationen das Unternehmen erhebt und wie es diese verwendet […] "Es ist zwingend erforderlich, dass die Verbraucher bei so etwas bewusst zustimmen", betonte Elbrecht. Die Juristin kritisierte zudem, dass Nutzer der Datenschutz- Erklärung zunächst zustimmen müssen und erst im Nachhinein manuell die Verwendung von Daten für Werbezwecke ablehnen können."* (Miesen, 2008).

Die AGB werden nach Protesten geändert. Die personalisierte Werbung bleibt als Passus in den AGB erhalten. Durch SMS und per Instant Messaging werden Benutzer aber keine Werbung von studiVZ erhalten. (vgl. Lischka, 2007b)

27.01.2008: Das Duell des Jahres bahnt sich an. Innerhalb von einer Woche startet die dritte studiVZ Community unter dem Namen „meinVZ.net" und der Rivale Facebook startet die deutschsprachige Version seiner Community. (vgl. Anon, 2008)

Bereits 2006, als die Stalking-Probleme aufkamen und studiVZ täglich wegen Sicherheitsproblemen in den Medien war, hat Martin Weber, ein Geschäftsführer der Holtzbrinck Ventures (Eigentümer von studiVZ) ein Interview mit Johnny Haeusler (2006) geführt. Darin sagt Weber:

> *„Ohne Frage muss StudiVZ an sich weiter arbeiten und zwar nicht nur was PR angeht sondern auch an vielen anderen Themen. […] gestern wurde ein Update der IT vorgenommen, vor einigen Tagen wurde eine erfahrene Person für das Thema Datenschutz eingestellt […]"*

Die Installation eines Datenschutzbeauftragten, sowie die Auswechslung der Unternehmensspitze führten dazu, dass studiVZ seltener (negativ) in die Schlagzeilen geriet. Doch auch die erfahrenen Manager mussten bei den Planungen zu den neuen AGB eingestehen, dass sie gegen den Unmut von Benutzern keine Chance haben. Der erste Entwurf der neuen AGB wurde überarbeitet und in einigen Bereichen abgemildert. (vgl. Kötter, 2007) Der Vergleich der allgemeinen Geschäfts- und Nutzungsbedingungen mit anderen Anbietern ergibt, dass die AGB im Gegensatz zu amerikanischen Formulieren weitaus ungefährlicher sind. (s. Kapitel 4.1.5). Medien dürften bei dem Thema vereinzelt Unwahrheiten verbreitet haben und selbst den Vergleich mit anderen Anbietern gescheut haben. Dennoch: studiVZ ist ein junges Unternehmen, das bereits für einige Datenschutz-Probleme gesorgt hat. Obwohl die Entwicklung neuer Sicherheitsmechanismen und erweiterter Privatsphäre-Einstellungen die Plattform sicherer gemacht haben, bleibt durch das unprofessionelle Umfeld und dessen Machenschaften ein fauler Beigeschmack.

Datamining und Webcrawling am Beispiel von studiVZ:
Wie einfach die Analyse einer unzureichend geschützten Community sein kann, beweist ein Student, der im Dezember 2006 innerhalb von 4 Stunden eine Million Nutzerprofile automatisiert herunterlud und statistisch unter der Adresse http://studivz.irgendwo.org/ aufbereitete. Die Ausgangsdaten können immer noch von dieser Adresse heruntergeladen werden. Die

Auswertung liefert interessante Ergebnisse für Personen, die meinen: „Was interessiert die Plattform <xxx> mein Profil? Damit kann doch nichts angefangen werden!“. Nun, im vereinzelten vielleicht (noch) nicht. Dass einzelne Profile für Mechanismen wie Targeting (s. Kapitel 3.1.6) oder Trendforschung sehr wohl wichtig sein können, beweisen nachfolgende Diagramme:

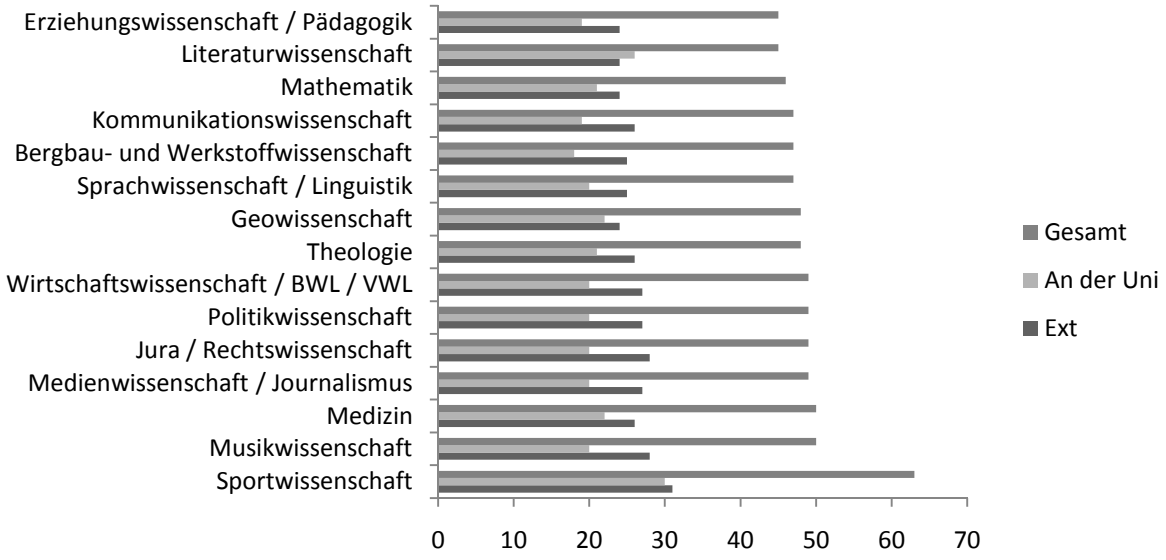

Abbildung 9: studiVZ.irgendwo.org: Freunde nach Studiengängen, adaptiert und verkürzt nach Fritsch, 2006

Wer sind die beliebtesten Personengruppen? Wer ist sozial am aktivsten? Die landläufige Meinung, dass Informatiker lieber zurückgezogen sind und wenig soziale Aktivitäten planen spiegelt sich in den Messungen aus Abbildung 9 wieder. Eine solch detailierte Aufzählung von Freunden nach Studiengängen wäre jedoch auf herkömmliche Weise durch (Telefon-)Befragungen niemals möglich. Hier sieht man, was mit der Auswertung von „user generated content“ möglich ist und wie genau Plattformen in der Lage sind, ihre Benutzer zu analysieren.

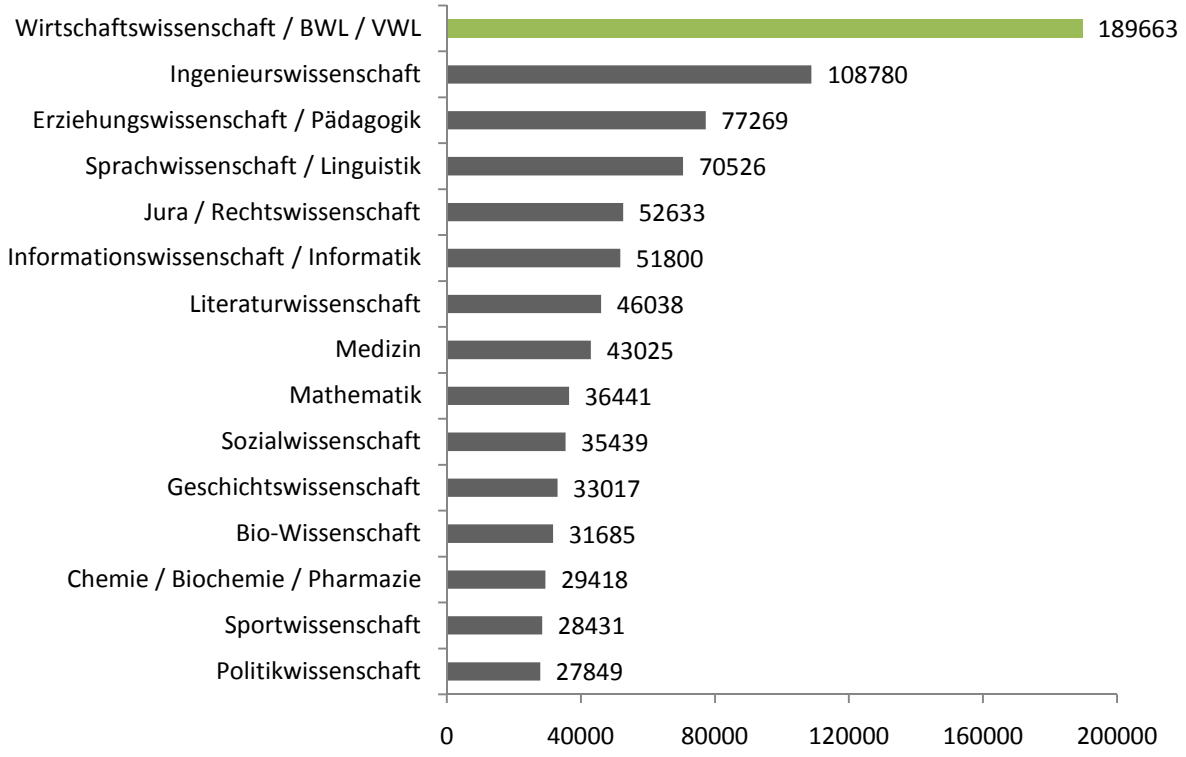

Abbildung 10: studiVZ.irgendwo.org: Mitglieder nach Studiengängen, adaptiert und verkürzt nach Fritsch, 2006

Für Werbetreibende ist diese Aussage wohl eine sehr entscheidende. Lohnt es sich, mein Produkt, das vor allem für Physiker geeignet ist, auf studiVZ zu schalten? Der Gesamtanteil an Physikstudenten auf studiVZ ist schwindend gering. Zielt man auf die Gruppe von Wirtschaftsstudenten ab, dann ist studiVZ die geeignete Wahl. *(*vgl. Otto, 2007*,* Fritsch*,* 2006*)*

4.1.1.4. kaioo

Anfang des Jahres 2008 startete ein neuer Anbieter am deutschen Markt. Durch Medien und geschicktes (virales) Marketing machte Sich kaioo rasch den Namen für Datenschutz und –sicherheit zu stehen. Neue Hoffnung bei den Benutzern, die von studiVZ enttäuscht waren, kam auf. kaioo nimmt das Wort „Social" Community ernst und ist als staatlich anerkannte gemeinnützige Organisation eingetragen. Es handelt sich um keine kommerziell geführte Plattform, sondern um ein Spendenportal; Werbeeinnahmen werden zu 100% von kaioo gespendet. In Zukunft können Benutzer der Plattform karitative Projekte vorschlagen und per Votum selbst entscheiden, an welche Projekte die Einnahmen fließen. Bis zum heutigen Zeitpunkt wird die Plattform einzig durch Spenden von Sony BMG und der Familie Schmidt-Holtz betrieben.

Bereits auf der Startseite bekommen (zukünftige) Benutzer die Garantie, dass gesammelte Benutzerdaten nicht an Dritte weitergegeben werden.

- *„Als gemeinnützige Organisation finanziert sich kaioo wie Wikipedia durch Spenden und Sponsoren: es gibt also keine Investoren, die ein Interesse am Verkauf Deiner Daten haben.*
- *kaioo ist und bleibt unabhängig von politischen, religiösen, kommerziellen und anderen Organisationen, so dass keine Abhängigkeitsverhältnisse bestehen, die den Schutz Deiner Daten gefährden könnten." (kaioo, 2008)*

Die Benutzerstatistiken zeigen, dass es sich bei kaioo aktuell höchstens um einen Nischenspieler handelt. Während auf Webseiten wie MySpace oder Facebook täglich 250.000 neue Profile erstellt werden, sind es auf kaioo gerade 1500. Anfang Februar hatte die Community 32.000 Profile. (vgl. Soltau, 2008 & Jacquemain, 2008) Das gemeinnützige Netzwerk ist daher ein Beispiel für die im Kapitel 3.2.3.2 aufgestellte These, dass ohne finanzielles Budget keine kritische Masse an Benutzern erreicht werden kann. Auch nicht, wenn kreatives, virales Marketing eingesetzt wird:

Stasido MC
Was machen Community-Betreiber, wenn konventionelle Werbeformen nicht mehr reichen, um ein neues Projekt erfolgreich zu machen? Virales Marketing ist die Antwort. Das Video von Stasido MC könnte solch eine virale Marketingkampagne darstellen, obwohl dies die Betreiber der Plattform von sich weisen.

Unter dem Spruch

> *„…Mein Profil, meine Gruppen, meine Freunde, meine Fotos, meine Hobbys, meine Daten sind weg. Meine Gedanken, mein Herz, mein Leben, meine Welt stehen nicht mehr im VZ. […] Junge, Kaioo ist erst seit ein paar Wochen am Start und hat jetzt schon bessere Features…“* (vgl. http://www.youtube.com/watch?v=B92sDagwZ1I)

versucht Stasido MC auf die Probleme bei studiVZ aufmerksam zu machen und bietet für Benutzer gleich eine Alternative: kaioo. Das kaioo über die besseren Features als studiVZ verfügt, konnte der Autor zum Zeitpunkt des Plattformvergleichs nicht erkennen (s. Kapitel 4.1.6).

Während Stasido MC am Ende des Videos scherzt: „*Oh Shit, da sind die vom stasiVZ und wollen mich einkassieren*.“, hat die Antwort von studiVZ und dessen Anwälten tatsächlich nicht lange gedauert. Eine knappe Woche später erscheint bereits der erste Presseartikel über eine mögliche gerichtliche Abmahnung des YouTube-Videos (vgl. Staedele, 2008). Während kaioo selbst mit den Worten „*Diese Art von Guerilla-Marketing passt nicht zu kaioo. Für uns ist Glaubwürdigkeit sehr wichtig, und dazu trägt das Video nicht bei*." (Jacquemain, 2008) eine virale Marketingkampagne ausschließt, entschließt sich studiVZ die Sache nicht weiter zu verfolgen, um kaioo wahrscheinlich nicht noch größere Medienpublik zu bescheren.

Die Social Community erinnert mit dem Layout und den Funktionen stark studiVZ, respektive Facebook. Das USP (Unique Selling Proposition) von kaioo bezieht sich daher lediglich auf die gemeinnützige Ausrichtung, die jedoch für die Masse an Personen zu wenig sein dürfte, wenn man ebenfalls die geringe Benutzeranzahl heranzieht. Dennoch: Die Plattform ist jung und zeigt einen alternativen Weg, den Benutzer zukünftig belohnen könnten: Die Bildung eines gemeinnützigen Vereins, der keine gewinnorientierte Ausrichtung hat. Daten scheinen in einem Verein, der nicht auf Gewinn ausgerichtet ist, weitaus sicherer.

Vom Regen in die Traufe?
kaioo wird als gemeinnütziger Verein betrieben. Doch blickt man hinter die Bühnen, so ergibt sich ein interessantes Bild. Die Nähe zu der Firmengruppe Bertelsmann ist nicht abzuweisen. Die Geschäftsführung beharrt zwar darauf, dass man selbst nichts mit Bertelsmann bzw. Sony BMG zu tun hätte; Experten sehen dies jedoch anders. In einem Artikel über kaioo zeigt Janos Balazs (2008), wie gut kaioo in das Portfolio von Bertelsmann passt und kaioo als Datenbank und Auswertungsgrundlage dienen könnte.

Alleine die Zeit wird also im Falle von kaioo zeigen, in welche Richtung sich die Plattform entwickelt und ob sie langfristig mit den großen der Branche mithalten kann.

4.1.1.5. Xing

Als OpenBC gestartet, ist Xing der einzige Anbieter einer Special Interest Community im Umfeld der durchgeführten Analyse. Die Business Community, die eingeschränkt kostenlos benutzbar ist, bietet ebenfalls die Möglichkeit einer kostenpflichtigen Premiummitgliedschaft. Aktuell hat Xing 5 Millionen registrierte Benutzer (vgl. Ihlenfeld, 2008). Wie stark die Community genutzt wird, zeigt das jährliche Xing Survey. Die erhobenen Zahlen zeigen, dass in Ländern wie USA, China, Türkei und Teilen Europas die Relevanz, Networking online zu betreiben, (signifikant) höher ist, als es bei dem altmodischen bei Offline Veranstaltungen der Fall ist. Als einer der Hauptgründe wird hierbei die fehlende Hürde der Zeitzonen angegeben, da Plattformen wie Xing 24 Stunden am Tag benutzt werden können.

Der tatsächliche Nutzen der Plattform zeigt sich in den bisherigen Erfahrungen, die die Teilnehmer des Xing Survey berichteten. Durchschnittlich jeder 2. europäische Xing-Benutzer hat bereits ein Job Angebot auf Xing erhalten und fast 3 von 4 Mitgliedern haben neue und interessante Kontakte geknüpft. Deswegen überrascht es nicht, dass sich 80% der Mitglieder aus Europa zumindest einmal am Tag oder mehrmals die Woche bei Xing einloggen. Im Vergleich zu Communities zur Freizeitnutzung ist die Verweildauer jedoch eher gering (vgl. XING, 2007a und Schmidt, 2008)

Auch Xing kam in den letzten Monaten vermehrt aufgrund von Benutzerprotesten in die Medien, da die Einführung neuer personalisierter Werbebanner für Proteste sorgte:

> „*Zum geplanten Start werden zunächst ausgewählte Bereiche der Plattform für Werbung zur Verfügung stehen. Im Verlauf des kommenden Jahres wird das Volumen behutsam angepasst und mit zunehmender Relevanz für Mitglieder erweitert.*“ (XING, 2007b)

Wie auf studiVZ und Facebook waren personalisierte Werbungen auf den Mitgliederseiten geplant. Die Betreiber versprachen, dass diese Änderungen im Einklang mit den Datenschutzbestimmungen stehen würden, doch Juristen sahen diesen Schritt anders:

> *„Auch rechtlich ist die Einblendung von Werbung in den Userprofilen nicht unproblematisch. […] So ist beispielsweise einigen Berufsgruppen Werbung im Zusammenhang mit der eigenen Tätigkeit gar nicht oder nur sehr eingeschränkt erlaubt. Finden sich auf deren Selbstpräsentationen nun plötzlich Werbebanner, könnten die Betroffenen im Rahmen der Mitstörerhaftung sogar selbst für diese Angebote verantwortlich gemacht werden.“* (Heidrich, 2008)

Xing ruderte innerhalb von wenigen Wochen zurück und hat auf die Proteste der Benutzer und Juristen reagiert. Die angesprochene Rechtslage zeigt das Spannungsfeld, in dem sich Betreiber und vor allem dessen Benutzer befinden. Die Einblendung von Werbeflächen auf Profilseiten von Benutzern, denen eine Werbung untersagt wird, ist ein ernsthafter Verstoß gegen das geltende Recht. Seit Anfang 2008 sind Profilseiten von Premium-Mitgliedern wieder frei von Werbung. Xing bedauert das Vorgehen.

> *„Seit Samstag, den 05. Januar 2008, sind die Profilseiten von Premium-Mitgliedern generell frei von Werbung. Wir reagieren damit auf das anhaltende Feedback, wonach die Mehrheit unserer Premium-Mitglieder keine Werbung auf ihren Profilseiten für Basis-Mitglieder wünscht. Wir bedauern es sehr, dass wir die Situation falsch eingeschätzt haben. Dafür möchten wir uns bei Ihnen entschuldigen.“* (XING, 2008)

4.1.2. Methodik

Um die Plattformen auf den gelebten Datenschutz hin zu vergleichen, wurden folgende Kriterien definiert, die auf jeder der fünf Plattformen getestet wurden:

- Welche Felder müssen bei der Registrierung unbedingt angegeben werden?
- Gibt es eine definierte Mindestlänge für Passwörter?
- Welche Mechanismen der automatisierten Anmeldung durch Bots wurden getroffen?
- Werden die AGB und Datenschutzbedingungen bei der Registrierung verlinkt?
- Ist eine Anmeldung ohne Zustimmung der AGB und Datenschutzbedingungen möglich?
- Wie erfolgt der Registrationsprozess?
- Welche datenschutzrechtlichen Mechanismen bietet die Plattform für angemeldete Benutzer?
- Ist eine Abmeldung von der Plattform möglich?
- Welche Fragen werden bei der Abmeldung gestellt?
- Wie lang dauert eine Abmeldung und welche Inhalte eines Benutzers werden gelöscht?

Der Vergleich der Plattformen wurde am 22. März 2008 um 18:00 Uhr durchgeführt. Die Auswertung ist für dieses Datum gültig. Nachfolgende Änderungen an den Systemen können daher nicht in die Auswertung einfließen. Die einzelnen Schritte wurden per Screenshot dokumentiert und liegen der Arbeit im Anhang bei.

Die Anmeldung wurde in allen Fällen als „Test Person“ durchgeführt. Lediglich Facebook erkannte diesen Namen als ungültig (s. Kapitel 4.1.4.2). Für die Angabe einer E-Mail-Adresse wurde der Service 10minutemail.com genutzt, der es ermöglicht, gratis für 10 Minuten willkürliche E-Mail-Adressen einzurichten. Nach Ablauf von 10 Minuten werden diese wieder gelöscht. So weit dies die Plattformen zuließen, wurden die Profile nach Beendigung der Auswertung gelöscht. 18 Stunden nach Abmeldung in den Plattformen wurde noch einmal nach den gelöschten Profilen gesucht um feststellen zu können, ob die Daten tatsächlich gelöscht wurden.

Da mehrere Fragen auf allen Plattformen gleich beantwortet werden können, werden diese bei den Detailauswertungen nicht aufgeschlüsselt.

Die Frage nach den Mechanismen zur Abwehr von automatisierten Anmeldungsversuchen kann allgemein beantwortet werden. Jede der getesteten Plattformen benutzte ein CAPTCHA (s. Kapitel 3.1.7.5). Der Anmeldeprozess erforderte ebenfalls bei jeder Community die Beantwortung einer Bestätigungs-E-Mail. Diese Abläufe dürften sich als defacto Standard im Internet entwickelt haben, die zwar den Anmeldeprozess für den Benutzer verlangsamen, dafür eine Hürde für automatisierte Anmeldeprogramme oder Webcrawler (s. Kapitel 3.1.7.4) deutlich erhöhen.

Die AGBs und Datenschutzbestimmungen werden bei jeder Registrierung verlinkt und müssen ebenfalls akzeptiert werden. Hier heben sich die professionellen Plattformen deutlich von den privat betriebenen Plattformen ab, in denen AGBs oder Datenschutzbestimmungen oftmals gänzlich fehlen. Die Rechtsabteilungen der Betreiber wissen also genau, wofür/wogegen sie sich absichern müssen. Das sowohl AGB als auch Datenschutzbestimmungen vorhanden sind, ist in erster Linie positiv zu beurteilen, da potentielle Benutzer von vornherein wissen, an welche Vertragsrichtlinien sie sich im Zweifelsfall durch die Zustimmung gebunden haben.

Interessant ist festzustellen, dass jeder der Betreiber bei der Löschung der Profile die eigenen größten Problematiken der Seite selbst anspricht und den Benutzer mit Hilfestellungen hierzu versucht von der Löschung abzubringen.

4.1.3. Auswertung Myspace.com

Welche Felder müssen angegeben werden?
E-Mail-Adresse, Passwort, Anzeigename, Vorname, Nachname, Land, Region, Postleitzahl, Geburtsdatum, Geschlecht, Lieblingsseite & Sprache, CAPTCHA zum Bestätigen des Vorgangs

Gibt es eine definierte Mindestlänge der Passwörter?
Mindestens 6 Zeichen, mindestens eine Zahl oder ein Sonderzeichen

Welche datenschutzrechtlichen Mechanismen bietet die Plattform?
Es kann definiert werden, ob

- das Feature „Jetzt online“ de-/aktiv ist. Standard: aktiv.
- der Geburtstag für Freunde angezeigt wird: Standard: Ja.
- das Profil für jeden, jeden über 18, nur für Freunde sichtbar ist. Standard: Jeden.
- Fotos veröffentlicht oder ge-emailt werden können. Standard: Ja.
- Benutzer unter 18 ermöglicht sind, Personen zu kontaktieren. Standard: ja.
- einzelne Benutzer gesperrt wurden, dass Profil einzusehen.

Zusätzlich zu den allgemeinen Datenschutzfunktionen können auf MySpace ebenfalls Spam-Einstellungen getroffen werden. So können Benutzer selbst entschieden, wann CAPTCHA Abfragen erforderlich sind, und welche Personen Benutzer zu Gruppen und Events einladen dürfen. Es gibt ebenfalls eine Unterteilung von Personengruppen, die Freundesanfragen tätigen können. Bands, Filmemacher und Komödianten können, so fern sie sich als diese Personengruppen outen, am Hinzufügen von Freundanfragen gehindert werden.

Standardmäßig sind die Spameinstellungen auf „benutzerdefiniert“, obwohl sie vom System so vorgegeben werden. Die CAPTCHA-Eingabe ist nicht zwingend erforderlich, dafür dürfen nur Freunde Gruppen- und Eventeinladungen verschicken. Sowohl Bands, Filmemacher als auch Comedians dürfen im *benutzerdefinierten* Modus Freundesanfragen stellen. Ob dies tatsächlich die von den Benutzern gewünschte Einstellung ist, ist fraglich. Wären CAPTCHAs standardmäßig erforderlich, wären die eigens konfigurierbaren Spameinstellungen, die sonst keine der untersuchten Plattformen hat, weitestgehend vernachlässigbar. Bei Personen unter 16 Jahren werden die Standardeinstellungen deutlich restriktiver gesetzt. (vgl. Poulsen, 2008a).

Ist eine Abmeldung möglich?
Ja.

Welche Fragen werden bei der Abmeldung gestellt?
Ein genereller Kommentar zur Abmeldung kann eingegeben werden, dieser ist jedoch nicht zwingend notwendig.

Wie lang dauert eine Abmeldung und welche Inhalte eines Benutzers werden gelöscht?
Eine Abmeldung erfolgt in mehreren Schritten. Nach Angabe eines optionalen Beweggrundes zur Löschung des Profils wird eine E-Mail an die angegebene Adresse geschickt, um den Vorgang zu bestätigen. In dem E-Mail ist ein Link zu einer weiteren Bestätigungsseite. Nach nochmaliger Bestätigung ist das „Löschen des Accounts geplant“ (s. Anhang MYSPA-

CE1). Das Profil wird innerhalb der nächsten 48 Stunden gelöscht. Nach Erscheinen des geplanten Löschvorgangs war ein Einloggen immer noch möglich. Die Überprüfung am nächsten Tag ergab, dass das Profil zu diesem Zeitpunkt bereits gelöscht war.

Welchen AGBs und Datenschutzbestimmungen[12] stimmt der Benutzer zu?
Die zum Zeitpunkt der Auswertung gültigen AGB und Datenschutzbestimmungen sind 12 Seiten lang und liegen in deutscher Sprache vor. Die als „MySpace Services" definierten Dienstleistungen werden in den Vereinigten Staaten betrieben. Die AGB gelten sowohl **für Gäste** als auch für angemeldete Mitglieder. Ist man mit diesen nicht einverstanden, muss die "*MySpace Webseite umgehend verlassen*" werden. MySpace behält sich das Recht vor, die AGB ohne Vorankündigung zu verändern:

> *„MySpace kann diesen Vertrag zu gegebener Zeit ändern. Diese Änderungen treten dann in Kraft, sobald sie von MySpace auf der MySpace Webseite bekannt gegeben werden. Wenn Sie die MySpace Services nach Bekanntgabe des geänderten Vertrags durch MySpace weiterhin benutzen, erklären Sie sich dadurch mit dem geänderten Vertrag einverstanden. Deshalb ist es wichtig, dass Sie sich diesen Vertrag regelmäßig durchlesen und immer auf dem neuesten Stand sind."*

Ohne das Wissen der Benutzer kann MySpace die Bestimmungen ändern – sobald die Benutzer die Webseite benutzen stimmen sie automatisch den neuen Bestimmungen zu. Da die AGB nur auf den MySpace Seiten veröffentlicht sind, müsste theoretisch jeder Benutzer den AGBs zustimmen, sobald er sich diese durchlesen möchte. Berechtigt zum Verwenden der Seite sind ausschließlich Personen, die mindestens 14 Jahre alt sind. Der mit MySpace geschlossene Vertrag „*bleibt selbst nach der Beendigung der Mitgliedschaft in Kraft*".

In Bezug auf das Urheberrecht der veröffentlichten Inhalte hält MySpace fest:

> *„MySpace beansprucht keinerlei Eigentumsrechte an Texten, Dateien, Bildern, Fotos, Videos, Sounds, Musikwerken, urheberrechtlich geschützten Werken, Anwendungen oder sonstigen Materialen […]. Nach der Veröffentlichung von Inhalt über MySpace Services behalten Sie vorbehaltlich der hier geltenden beschränkten Lizenz weiterhin alle Rechte, die Sie an Ihrem Inhalt haben. Mit der Anzeige oder Veröffentlichung („Einstellen") von Inhalt auf den oder über die MySpace Services erteilen Sie MySpace eine beschränkte Lizenz, den Inhalt lediglich auf den oder über die MySpace Services zu nutzen, zu modifizieren, zu löschen, dazu hinzuzufügen, öffentlich darzubieten, zu reproduzieren und zu verbreiten. […] Wenn Sie Ihren Inhalt von der MySpace Webseite entfernen, versuchen wir, die Verbreitung so bald als möglich einzustellen. Zu dem Zeitpunkt, zu dem die Verbreitung aufhört, verfällt auch die Lizenz. […] Bei der Lizenz, die Sie MySpace gewähren, handelt es sich um eine einfache […], unentgeltliche und gebührenfreie (das bedeutet, dass MySpace keine Gebühr für die Nutzung des von Ihnen veröffentlichten Inhalts auf den MySpace Services zahlt), weiterlizenzierbare […] und weltweite Lizenz"*

MySpace ist der Ansicht, dass zum Betrieb der Services keinerlei Eigentumsrechte beansprucht werden und eine beschränkte Lizenz notwendig ist. Im Gegensatz zu dem Vertrag, der ebenfalls nach Beendigung der Mitgliedschaft bestehen bleibt, gilt die Lizenz an den Inhalten ausschließlich während diese veröffentlicht auf den Seiten öffentlich zugänglich sind.

Die Haftungsbedingungen schließen MySpace von der teilweisen Haftung aus. Bei Streitigkeiten gilt ausschließlich das geltende Recht des Bundesstaates New York:

[12] AGB: http://www.myspace.com/index.cfm?fuseaction=misc.terms, Stand: 28.02.2008
Datenschutzbestimmungen: http://www.myspace.com/index.cfm?fuseaction=misc.privacy, Stand: 28.02.2008

> *„MySpace ist unter keinen Umständen Ihnen oder Dritten gegenüber haftbar für indirekten, folge-, verschärften, beiläufig entstandenen, konkreten oder Strafschadenersatz, einschließlich eines Schadenersatzes für entgangenen Gewinn im Zusammenhang mit der Nutzung von MySpace Services […] Der Vertrag unterliegt und wird ausgelegt entsprechend den Gesetzen des US-Bundessstaates New York […]. Sie und MySpace unterwerfen sich der ausschließlichen Zuständigkeit der Gerichte im US-Bundesstaat New York zwecks der Beilegung von Streitigkeiten."*

Im Kapitel 4.3.3 wird diese Einschränkung des geltenden Rechts mit einem Rechtsexperten diskutiert.

Die Datenschutzbestimmungen weisen explizit darauf hin, dass sich Personen, die sich außerhalb der Vereinigten Staaten befinden, mit der Übermittlung Ihrer Daten in die USA zustimmen. Im Gegensatz zu den AGB wird in den Datenschutzbestimmungen erklärt, dass es sich bei den MySpace Webseiten um Seiten handelt, die nicht bewusst Daten von Kindern erheben, die unter **13 Jahre** alt sind. Hier herrscht eine Diskrepanz, da bei den AGB die Nutzung für Personen unter *14 Jahren* ausgeschlossen wird.

Bezüglich Werbung halten die Datenschutzbestimmungen fest, dass MySpace Profilinformationen und sonstige verbundene Daten dazu verwendet werden können, „*um die Online-Werbung so auf Sie zuzuschneiden, dass sie unserer Meinung nach Ihren Interessen entsprechen.*" Die Datenschutzbestimmungen beinhalten in der gültigen Fassung einen Hinweis darauf, dass diese Form der Werbung deaktivierbar ist.

Externe Anwendungen können in die Seite integriert werden. MySpace weist ausdrücklich darauf hin, dass es sich hierbei jedoch um Anwendungen externer Entwickler handelt und keine personenbezogenen Daten übermittelt werden sollten. Die Nutzungsbestimmungen regeln darüberhinaus ebenfalls die Verwendung eines Rights Management Tools, das zur Überprüfung von Audio- und audiovisuellem Inhalt herangezogen wird und Inhalte sperren kann.

> *„MySpace kann das Tool außerdem gelegentlich zur Prüfung von Inhalt heranziehen (einschließlich der Profilinformationen in privaten Profilen), um festzustellen, ob ein Inhalt vorliegt, der einem Inhalt entspricht, für den die Inhaber von Urheberrechten Content Identifier zur Verfügung gestellt haben. […] Die Inhaber von Urheberrechten haben beim Betrieb des Tools möglicherweise Zugriff auf bestimmte verbundene Daten und Profilinformationen, jedoch nicht auf PII[13], wenn keine ausdrückliche Erlaubnis des Mitglieds vorliegt."*

Die gelegentliche Prüfung von Inhalten der Mitglieder zeigt die Gefahr, die von der Nutzung sozialer Netze ausgehen kann. Niemand kann genau wissen, welche Daten zu welcher Zeit überprüft werden. Das verwendete Tool, das urheberrechtliche Verletzungen aufspüren soll, könnte auch für weitere Datamining Aktivitäten herangezogen werden, über die Benutzer nicht informiert sind.

MySpace sichert sich das Recht zu, dass bei einer Veräußerung des Unternehmens die Datenbestände auf den neuen Eigentümer übertragbar sind und versichert, dass PII, sollte MySpace zur Löschung dieser aufgefordert wird, bis auf diejenigen PII gelöscht werden, die zur Erfüllung geltender gesetzlicher Bestimmungen notwendig sind.

[13] Personally Identifiable Information (vollständiger Name, E-Mail-Adresse, Postanschrift, Kreditkartennummer)

Welche Besonderheiten gibt es in der SC in Bezug auf Datenschutz?
Im Gegensatz zur überladenen und sehr undurchsichtigen Plattform selbst ist die Anmeldemaske sehr benutzerfreundlich. Prominent platzierte Fehlerboxen zeigen, welche Fehleingaben gemacht wurden und geben Tipps zu den einzelnen Feldern. MySpace achtet auf sichere Passwörter und verlangt als einziger der untersuchten Anbieter ein starkes Passwort aus mindestens 6. Zeichen und einem Sonderzeichen oder einer Zahl. Es wird ebenfalls auf der ersten Seite darauf hingewiesen, dass es sich bei MySpace um einen amerikanischen Anbieter handelt, und daher die Daten, die in den USA gespeichert werden, auch diesem Recht unterliegen. (s. Kapitel 3.1.5)

Nach erfolgter Registrierung steht man auf MySpace nicht alleine da. Man ist automatisch Freund des MySpace-Teams sowie des Gründers von MySpace, Tom Anderson. Durch diese Aktion dürfte Tom Anderson die Person mit den meisten Freunden weltweit sein. Zum Stichtag 23. März 2008 hat er 229.628.403 Freunde, zumindest auf MySpace (vgl. http://www.myspace.com/tom).

Eine Funktion, die im Vergleich einzigartig war, ist die Tatsache, dass bei MySpace sowohl HTML als auch CSS bei den Eingaben im Benutzerprofil erlaubt ist. Während dem Test der Plattform stieß der Autor auf ein Profil, dass durch HTML Code so stark verändert wurde, dass eine komplett andere Seite im Browser geladen wurde – obwohl in der Adressleiste immer noch eine MySpace.com Adresse aufschien.

Unerklärlich erscheinen ebenfalls die Absenderadressen von automatisch generierten E-Mails von MySpace, wie der Screenshot aus Abbildung 11 zeigt:

Abbildung 11: Absenderadressen bei MySpace E-Mail-Nachrichten

Zufällig generierte alphanumerische Zeichenfolgen als Absender zu gebrauchen, ohne einen Absendernamen zu definieren, fördert Phishing-Attacken, da Benutzer den Unterschied von „richtigen“ und „falschen“ Absendern nur sehr schwer erraten können. Wenn es möglich ist, durch die Eingabe von HTML Code, beliebige Seiten über ein bestehendes Profil zu laden, kann ein Phishing Versuch auch von Profis nicht mehr erkannt werden.

Ebenfalls gefährlich erscheint die Tatsache, dass Benutzer bei MySpace eine eigene MySpace-URL im Format myspace.com/<<Benutzereingabe>> auswählen können. Die potentiell sehr gefährliche Eingabe von „adminteam“ wird mit einem „*Gut gemacht*“ (s. Anhang MYSPACE2) belohnt.

4.1.4. Auswertung Facebook.com

Welche Felder müssen bei der Registrierung unbedingt angegeben werden?
Die Felder der Registrierung hängen bei Facebook von dem ausgewählten Personentyp ab. Als Student hat man die Felder Vollständiger Name, Schulstatus, Abschlussjahr, Geburtsdatum, E-Mail, Passwort, CAPTCHA zum Bestätigen des Vorgangs einzugeben.

Facebook unterscheidet zwischen Studenten, arbeitenden Personen, Schülern und „Nichts davon“. Für Firmen oder Bands gibt es eine eigene Registrierungsseite. Dieses Feature ist innerhalb des Vergleichs einzigartig.

Gibt es eine definierte Mindestlänge der Passwörter?
Mindestens 6 Stellen

Welche datenschutzrechtlichen Mechanismen bietet die Plattform für angemeldete Benutzer?
In den Kontoinformationen können für jede Applikation (s. Kapitel 4.1.1.2.2.) Einstellungen getroffen werden. Für die Applikation „Facebook" an sich ist es möglich, E-Mail-Benachrichtigungen für jeden erdenklichen Event (Benutzer wird auf Foto markiert, anderer Benutzer antwortet auf einen Beitrag in einer Gruppe, Benutzer wird als Freund hinzugefügt, …) zu definieren. Standardmäßig sind hier alle Optionen auf E-Mail erhalten eingestellt, außer der Event des „angestupst" Werdens. (vgl. studiVZs *gruscheln*).

Ist eine Abmeldung von der Plattform möglich?
Nein, das Profil kann nur deaktiviert werden. (s. Anhang FACEBOOK1)

Welche Fragen werden bei der Deaktivierung gestellt?
Eine erforderliche Selektion eines Deaktivierungsgrundes ist notwendig. Es kann ebenfalls entschieden werden, ob man weiterhin E-Mails von Facebook bekommen möchte, oder nicht.

Wie lang dauert eine Deaktivierung und welche Inhalte eines Benutzers werden gelöscht?
Die Deaktivierung des Profils erfolgt sofort. Es werden jedoch keine Profildaten gelöscht.

Welchen AGBs und Datenschutzbestimmungen stimmt der Benutzer zu?
Die AGB und Nutzungsbestimmungen[14] liegen sowohl in deutscher als auch englischer Sprache vor. Der Umfang der Bestimmungen variiert daher. Bei den deutschen Richtlinien handelt es sich lediglich um Übersetzungen, die rein informativen Charakter haben. Lediglich die englische Version des jeweiligen Dokuments ist rechtlich bindend. Zu den deutschen Dokumenten ist generell zu sagen, dass diese äußerst schwach übersetzt sind. Nicht beendete Sätze, englische Passagen sowie Sätze, die grammatikalisch komplett falsch sind hinterlassen ein sehr getrübtes Bild von Facebook. Die Richtlinien selbst sind sehr strikt und dürften einige Überraschungen für Benutzer bereithalten. Es dürfen sich nur Personen über 13, bzw. Studenten über 18 Jahren registrieren.

Wie bereits bei MySpace gelten die AGB von Facebook ebenfalls sowohl für Besucher als auch für Mitglieder der Seite. Regelungen können ebenfalls zu jeder Zeit von Facebook verändert werden. Die Änderung der Richtlinien wird durch das Datum der letzten Veränderung verdeutlicht. Eine Benutzung der Seite nach der Änderung der AGB führt auch hier zu einer Zustimmung der neuen Regelungen. Alle Daten, die von Facebook verarbeitet und den Benutzern bereitgestellt werden, werden in den USA gespeichert.

Die Regelung der Nutzungsbestimmungen wird bei Facebook jedoch anders gehandhabt:

> *„When you post User Content to the Site, you authorize and direct us to make such copies thereof as we deem necessary in order to facilitate the posting and storage of the User Content on the Site. By Posting User Content to any part of the Site, you automatically grant, and you represent and warrant that you have the right to grant, to the Company an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to use, copy, publicly perform, publicly display, reformat, translate, excerpt (in whole or in part) and distribute such User Content for any purpose, commercial, advertising, or otherwise, on or in connection with the Site or the promotion thereof, to prepare derivative works of, or incorporate into other works, such User Content, and to grant and authorize sublicenses of the fore-*

[14] Nutzungsbedingungen: https://login.facebook.com/terms.php, Stand: 15. November 2007
Privacy Policy: https://login.facebook.com/policy.php, Stand: 6. Dezember 2007

> *going. You may remove your User Content from the Site t any time. If you choose to remove your User Content, the license granted above will automatically expire, however you acknowledge that the Company may retain archived copies of your User Content."*

Facebook sichert sich das Recht zu, dass die Inhalte auch für (kommerzielle) Werbezwecke verwendet werden dürfen und archivierte Kopien aufgehoben werden dürfen.

Der Passus bezüglich der bereits angesprochenen „Platform Applications" (s. Kapitel 4.1.1.2.2. beinhält den Verweis auf eigene Nutzungsbedingungen der installierten Programme. Weder die Applikationen selbst, noch die vertraglichen Richtlinien werden von Facebook überprüft.

> *„Platform Applications have not been approved, endorsed, or reviewed in any manner by Facebook, and we are not responsible for your use of or inability to use any Platform Applications, including the content, accuracy, or reliability of such Application and the privacy practices or other policies of Developers. YOU USE SUCH PLATFORM APPLICATIONS AT YOUR OWN RISK. If you, your friends or members of your network use any Platform Applications, such Platform Applications may access and share certain information about you with others in accordance with your privacy settings as further described in our Privacy Policy. Platform Developers are required to agree to restrictions on access, storage and use of such information. However, while we have undertaken contractual and technical steps to restrict possible misuse of such information by such Platform Developers, we do not screen or approve Developers, and we cannot and do not guarantee that all Platform Developers will abide by such restrictions and agreements."*

Die Installation von Platform Applications stellt nicht nur für den Benutzer selbst, sondern auch für dessen bestätigte Kontakte ein potentielles Sicherheitsproblem dar. Den Entwicklern der Mini-Anwendungen wird ermöglicht auf Daten zuzugreifen und ebenfalls selbst Daten über Personen zu speichern. Somit entstehen entfernte Datenbestände über Facebook-Benutzer, die im schlimmsten Fall nicht mehr gelöscht werden können. Facebook stellt fest, dass die Verwendung der Applikationen ein eigenes Risiko darstellt und man selbst keine Überwachung durchführt.

Die Haftungsbeschränkung wird wie bei MySpace sehr eng gehalten und darüberhinaus wird geregelt, dass Facebook in keinem Fall zu mehr als 1000 US Dollar haftet. Es gelten die Gesetze des Staates Kalifornien.

4.1.4.1. Profil auf Lebenszeit

Die Kündigung des Vertrags (gleichbedeutend der Löschung eines Profils) ist einzig durch den Betreiber möglich:

> *„The Company may terminate your membership, delete your profile and any content or information that you have posted on the Site or through any Platform Application and/or prohibit you from using or accessing the Service or the Site or any Platform Application […] When we are notified that a user has died, we will generally, but are not obligated to, keep the user's account active under a special memorialized status for a period of time determined by us to allow other users to post and view comments."*

Die Mitgliedschaft bei Facebook reicht nicht nur auf Lebenszeit, sondern auch darüber hinaus. Facebook erlaubt sich das Profil bei Bekanntgabe des Ablebens eines Nutzers weiterhin, unter einem besonderen Status, aufrechtzuerhalten. Ein vergleichbarer Passus findet

sich in keinen der untersuchten Regelungen anderer Betreiber. Elegant schweigt Facebook über die Tatsache, dass keine Abmeldung durch den Benutzer möglich ist. Bereits Anfang des Jahres wurden Medien auf diesen Umstand aufmerksam. derStandard (2008c) berichtete damals über eine „*Verpflichtung auf Lebenszeit*" für Mitglieder von Facebook. Von einer Deaktivierung des Profils, wie es Facebook definiert, kann dabei jedenfalls keine Rede sein. Es ist Freunden weiterhin möglich deaktivierte Profile zu neuen Events einzuladen, oder diese auf Fotos zu verlinken. Personen haben keine Kontrolle über ihre Daten.

Die geltenden Privacy Policies erklären, dass Facebook auf zwei Grundprinzipien basiere:

- *„Du solltest [sic] Kontrolle über deine persönlichen Informationen haben.*
- *Du sollst Zugriff auf Informationen haben, die andere mit dir teilen möchten."*

Es dürfte sich wohl um einen Übersetzungsfehler handeln, der von den Facebook Mitarbeitern noch nicht entdeckt wurde. Oder handelt es sich bei „Du *solltest* Kontrolle haben" um einen Hinweis, dass dies bei Facebook nicht der Fall ist? Die hier beschriebenen Grundprinzipien stehen auf jeden Fall im direkten Gegensatz zu den AGB, in denen keine Kündigung der Mitgliedschaft durch den Benutzer erwähnt bzw. ermöglicht wird.

Damit noch nicht genug, sichert sich Facebook auch die Möglichkeit zu, dass Daten für einen angemessenen Zeitraum gespeichert werden, die verändert oder gelöscht wurden:

> *„Wenn du Informationen aktualisierst, behalten wir normalerweise eine Sicherungskopie der vorherigen Version für einen angemessenen Zeitraum, um die Rückkehr zur vorherigen Version dieser Informationen zu ermöglichen. […] Gelöschte Informationen können in backup [sic] Kopien für eine gewissen Zeitraum erhalten bleiben, sind aber nicht für Facebook Mitglieder einzusehen."*

Benutzen Mitglieder der Seite den Einladungs-Service, um Freunde auf die Seite aufmerksam zu machen, werden die Daten des möglichen zukünftigen Benutzers gespeichert. Facebook hat allerdings kein Interesse daran diese Daten freiwillig wieder zu löschen:

> *„[…] Wir werden deinem Freund automatisch eine einmalige Email oder eine Sofortnachricht schicken um ihn oder sie auf unsere Seite einzuladen. Facebook wird diese Informationen speichern um diese einmalige Nachricht zu schicken, um eine Freundschafts-Verbindung anzulegen, sofern deine Einladung angenommen wird, und um den Erfolg unseres Empfehlungssystems zu verfolgen. Dein Freund kann uns per info@facebook.com kontaktieren um diese Informationen aus unserer Datenbank entfernen zu lassen."*

Eine Überprüfung dieses Dienstes durch den Autor hat ergeben, dass bei dem versendeten E-Mail kein Hinweis darauf besteht, dass die Daten der geworbenen Person im System gespeichert bleiben. Es besteht jedoch die Möglichkeit zukünftige E-Mails durch Facebook zu blockieren.

Die Krönung der Privacy Policy stellt folgende Aussage dar:

> *„Facebook kann ferner Informationen über Dich aus weiteren Quellen sammeln, hierzu gehören unter anderem Zeitungen, Blogs, Instant Messaging Dienste und die Aktionen anderer Facebook Nutzer (z.B. Foto-Tags), um Dich mit mehr nützlichen Informationen und personalisierten Angeboten zu versorgen."*

Was wird Facebook in Zukunft über seine Benutzer (und eingeladenen Personen) speichern? Sollte Facebook tatsächlich Informationen über Mitglieder sammeln und dabei auf Zeitungen und Blogs zurückgreifen, wäre der Datenbestand von unheimlich großem Wert für

Werbetreibende und Investoren. Facebook hat deswegen bereits vorgesorgt und weist in den Nutzungsbedingungen auf eine mögliche Veräußerung hin:

> *„Wenn die Eigentumsverhältnisse am gesamten oder nahezu gesamten Facebook-Unternehmen oder an einzelnen Unternehmenseinheiten der Facebook Inc. Ändern, können deine Nutzerdaten auf den neuen Eigentümer übertragen werden, damit der Betrieb der Seite weitergeführt werden kann. Im Falle einer solchen Übertragung von Nutzerdaten unterliegen diese weiterhin dem Schutz jeder zuvor bestehenden Datenschutzvereinbarung.“*

Es beruhigt auf den ersten Blick, dass die Nutzerdaten weiterhin den zuvor bestehenden Datenschutzvereinbarungen unterliegen. Den Schutz, den diese aktuell unterliegen, ist jedoch äußerst niedrig. Keine Nutzungsbedingungen im durchgeführten Vergleich bieten dem Betreiber so viele Möglichkeiten, wie es bei Facebook der Fall ist.

4.1.4.2. Sicherheitsprobleme bei der Anmeldung

Während der Anmeldung fand der Autor ein Schlupfloch bei der Anmeldung, durch das es möglich ist, automatisiert Benutzerprofile auf der Plattform einzurichten. Dieses Vorgehen ist normalerweise durch das CAPTCHA nur bedingt lösbar. Gibt ein potentieller neuer Benutzer jedoch einen Namen ein, den Facebook als ungültig erkennt (in diesem Fall: Test Person), erscheint kein CAPTCHA mehr. Selbst wenn zuvor ein falscher Wert für das CAPTCHA eingegeben wurde fehlt diese Überprüfung. Nach Eingabe eines Namens, der vom System nicht als falsch erkennt wurde, erfolgt eine Registrierung und eine E-Mail mit Bestätigungslink wird verschickt. Der Autor hat Facebook über das bereitgestellte Kontaktformular am 24. März 2008 auf diese Sicherheitslücke aufmerksam gemacht.

Bis zum 14. Mai 2008, dem Tag der Abgabe der vorliegenden Arbeit, bekam der Autor keine Antwort auf die gefundene Sicherheitslücke. Eine nochmalige Überprüfung an diesem Tag ergab, dass Facebook das Problem jedoch behoben hatte. Es war nicht mehr möglich, sich mit einer 10minutemail Adresse zu registrieren. Darüberhinaus musste das CAPTCHA immer richtig ausgefüllt werden um zum nächsten Schritt zu kommen. Einzig die Überprüfung auf den Namen „Test Person“ ist gleich geblieben. Das System informiert den Benutzer weiterhin darüber, dass diese Eingabe unzulässig ist, wie Abbildung 12 erkennen lässt.

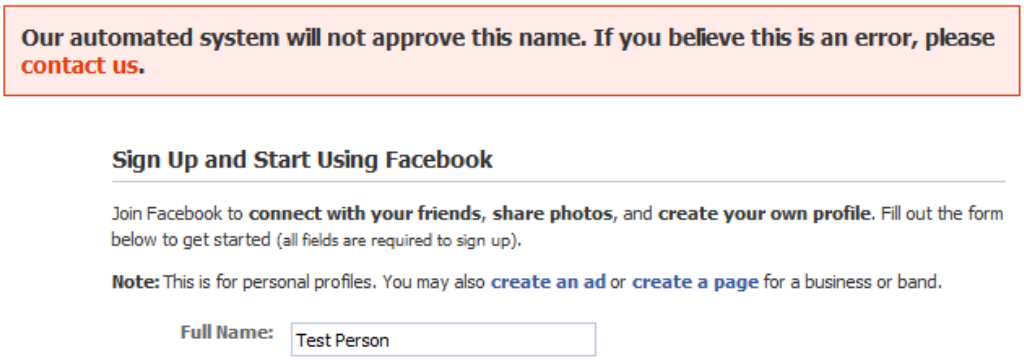

Abbildung 12: Test Person ist als Eingabe bei der Registrierung bei Facebook ungültig. (vgl. http://register.facebook.com/r.php)

4.1.5. Auswertung studiVZ.net

Welche Felder müssen bei der Registrierung unbedingt angegeben werden?
Vorname, Nachname, Geburtstag, Geschlecht, Hochschule, E-Mail, Passwort, CAPTCHA zum Bestätigen des Vorgangs

Gibt es eine definierte Mindestlänge der Passwörter?
Mindestens 6 Zeichen

Welche datenschutzrechtlichen Mechanismen bietet die Plattform für angemeldete Benutzer?
Die Privatsphäre-Einstellungen sind Anfang 2008 deutlich verbessert worden. Man kann nun sehr gezielt Einstellungen über die Profildaten, den Nachrichtenverkehr sowie weiteren Features auf der Seite treffen. Darüberhinaus kann man ebenfalls entscheiden, ob man personalisierte Werbung akzeptiert oder nicht. Standardmäßig ist dieser Wert gesetzt. Seit dem Launch von meinVZ.net ist ebenfalls eine Unterscheidung der Privatsphäre-Einstellungen für Benutzer dieser Plattform in studiVZ integriert. Standardmäßig können Benutzer der neuen Plattform Personen im studiVZ jedoch nicht finden, der Benutzer muss selbst das Profil „verbinden" – dieser Schritt ist nicht mehr rückgängig machbar.

Ist eine Abmeldung von der Plattform möglich?
Eine Abmeldung ist möglich.

Welche Fragen werden bei der Abmeldung gestellt?
Die Abmeldung bei studiVZ ähnelt sehr stark der von Facebook. Es handelt sich hierbei jedoch um eine richtige Abmeldung und keine Deaktivierung. Es wird jedoch ebenfalls nach dem Grund des Verlassens gefragt und die Antwortmöglichkeiten zeigen, warum studiVZ zu Recht als Facebook-Klon tituliert wird.

Wie lang dauert eine Abmeldung und welche Inhalte eines Benutzers werden gelöscht?
Eine Abmeldung dauert wie bei MySpace rund 48 Stunden, die Überprüfung nach 18 Stunden hat jedoch ergeben, dass das Profil nicht mehr erreichbar war. Es werden sowohl die Profilseite, als auch die Freundschaften gelöscht. Kommentare und Forenbeiträge bleiben anonym erhalten.

Welchen AGBs und Datenschutzbestimmungen stimmt der Benutzer zu?
Die Regelungen von studiVZ sind im Vergleich zu den anderen Anbietern die umfassendsten. Es gibt allgemeine Geschäftsbedingungen, einen Verhaltenskodex, eine Datenschutzerklärung sowie -informationen[15]. Durch das große mediale Echo auf den Wechsel der AGB hat studiVZ sehr viele Hilfestellungen zu den Regeln online gestellt, die aktuell etwas über das Ziel hinausschießen. Der Umfang an Informationen ist sehr hoch. Selten werden Benutzer tatsächlich die Zeit haben, um sich wirklich alle Informationen durchlesen zu können. Dennoch sind die Bemühungen sehr lobenswert. Ebenfalls Positiv anzumerken ist, dass studiVZ als einziger Anbieter im Feld ebenfalls die alten Datenschutzerklärungen auf der Webseite verlinkt hat. Die Datenschutz-Information kann als Handbuch für studiVZ benutzt werden und beinhält eine genaue Aufgliederung der angebotenen Funktionen. Hierin werden auch alle Funktionen zur Privatsphäre und dem Datenschutz erklärt.

Die Verwendung von studiVZ ist nur volljährigen Personen erlaubt. Dabei ist „die Angabe von Künstlernamen, Pseudonymen oder sonstigen Phantasiebezeichnungen" nicht gestattet. Das heißt, dass studiVZ ausschließlich mit dem richtigen Namen verwendet werden darf.

Das Löschen des Accounts kann jederzeit ohne Angaben von Gründen erfolgen. Die Löschung kann sowohl auf der Webseite als auch per E-Mail erfolgen. Die AGB klären, was mit den bisher gespeicherten Daten geschieht:

[15] AGB: http://www.studivz.net/l/terms, Stand: 20.12.2007
Verhaltenskodex: http://www.studivz.net/l/rules/
Datenschutzerklärung: http://www.studivz.net/l/policy/declaration/, Stand: 20.12.2007
Datenschutzinformation: http://www.studivz.net/l/policy/info/, Stand: 20.12.2007

> *„Mit der erfolgreichen Exmatrikulation (Löschung, Anm. des Autors) wird der Account des Nutzers und alle personenbezogenen Daten des Nutzers dauerhaft gelöscht. Diejenigen Beiträge, die der Nutzer vor der Exmatrikulation über das studiVZ-Netzwerk öffentlich zugänglich gemacht hat [...], bleiben nach der erfolgten Deaktivierung weiterhin abrufbar - dies jedoch ohne Angabe des Namens und mit dem Hinweis, dass der Beitrag von einem inzwischen gelöschten Nutzer stammt."*

Interessanterweise ändert studiVZ während der Erklärung den Begriff von „Exmatrikulation (Kündigung)" auf Deaktivierung. Dennoch ist der Passus im Gegensatz zu Facebook deutlich freundlicher formuliert.

Die AGB klären weiter auf, dass studiVZ nicht dazu verpflichtet ist, die gespeicherten Daten zu überwachen oder Nachforschungen, *„die auf rechtswidrige Tätigkeit hinweisen*", zu unternehmen.

Änderungen an den AGB werden Nutzern spätestens zwei Wochen vor Inkrafttreten per E-Mail zugeschickt. In diesem E-Mail muss „*gesondert auf die Bedeutung der Zweiwochenfrist*" hingewiesen werden. *„Widerspricht der Nutzer der Geltung der neuen AGB nicht innerhalb von zwei Wochen nach Empfang der E-Mail, gelten die geänderten AGB als angenommen."* Der deutsche Branchenprimus ist bei der Änderung der geltenden Regelungen deutlich benutzerfreundlicher als die amerikanischen Kontrahenten. Obwohl auch studiVZ bei der letzten AGB-Änderung wegen der Zustimmungsproblematik negativ in die Medien kam, kann hier klar von einer faireren Lösung gesprochen werden. Dennoch ist bei der Änderung der AGB generell noch einiges mehr an Benutzerfreundlichkeit zu verlangen.

Auch studiVZ, dass bereits vom Holtzbrinck Verlag aufgekauft wurde, hat einen entsprechenden Passus zur Übernahme durch Dritte:

> *„Anstelle von studiVZ können Dritte in die sich aus diesem Vertrag für studiVZ ergebenden Rechte und Pflichten ganz oder teilweise unter Einhaltung einer Vorankündigungsfrist von einem Monat eintreten. Der Nutzer ist befugt, sich in einem solchen Fall durch Kündigung des Vertragsverhältnisses gegenüber studiVZ ohne Angabe von Gründen von dem Vertrag zu lösen […]."*

Auch hier gilt eine Vorankündigungsfrist, die es dem Benutzer ermöglicht sein Konto zu löschen. Als ausschließliches Recht wird in den AGB das Recht der Bundesrepublik Deutschland vereinbart.

In der Datenschutzerklärung, die Nutzer während der Registrierung zustimmen müssen, wird das Bereitstellen von personalisierter Werbung geregelt und technisch näher erklärt:

> *„Dem Nutzer können so über das studiVZ-Netzwerk mit der erklärten Einwilligung Werbung und/oder besondere Angebote und Services präsentiert werden, deren Inhalt auf den im Zusammenhang mit der Clickstream-Analyse erlangten Informationen basiert. […] Ich nehme zur Kenntnis, dass ich, falls eine solch personalisierte Werbung von mir nicht mehr erwünscht ist, diese ablehnen und der Nutzung meiner Daten jederzeit widersprechen kann. […] Ich willige ein, dass studiVZ die von mir bei der Registrierung mitgeteilten Daten […], die von mir freiwillig innerhalb meines eigenen Profils („Meine Seite") eingetragenen Daten […] sowie meine Mitgliedschaft in Gruppen („Meine Gruppen") dazu nutzt, um mir gezielt personalisierte Werbung und/oder besondere Angebote und Services über das studiVZ-Netzwerk zu präsentieren bzw. präsentieren zu lassen […]"*

Die Regelungen erlauben dem Betreiber, nach Zustimmung, die standardmäßig aktiv ist, personalisierte Werbung zu schalten. Dabei werden nicht nur Profildaten genutzt, sondern auch Gruppenzugehörigkeiten analysiert.

Der Verhaltenskodex soll das Verhalten der Benutzer untereinander regeln. Vor allem zwei Passagen dürften sich nicht immer bis zum eigenen Support der Plattform durchgesprochen haben:

> *„Kein wiederholtes Zusenden von Nachrichten oder Gruscheln, wenn die Empfängerin oder der Empfänger mitgeteilt hat, dass dies nicht erwünscht ist. Ebenso ist Massengruscheln bei einer Person untersagt, wenn diese dazu kein Einverständnis gegeben hat. […] Rassistische, gewalttätige, politisch extremistische, sexistische, diskriminierende oder sonst anstößige Veröffentlichungen, sowie solche, die andere Personen, Volksgruppen oder religiöse Bekenntnisse beleidigen, verleumden, bedrohen oder verbal herabsetzen, sind nicht gestattet."*

Der in Kapitel 4.1.1.3 beschriebene Fall der Stalker-Gruppe, die Frauen „Massengegruschelt" hat und durch eine sehr fragwürdige Antwort des Supportmitarbeiters in die Schlagzeilen geriet, hätte basierend auf dem Verhaltenskodex anders geregelt werden müssen. Schließlich behält sich studiVZ das Recht bei Verstößen gegen diesen Kodex vor, Profile oder ganze Gruppen ohne Ankündigung zu löschen.

Welche Besonderheiten gibt es in der SC in Bezug auf Datenschutz?
studiVZ rüstet auf. Während es noch vor wenigen Wochen nur bedingt möglich war, spezielle Daten für Personen(-gruppen) sichtbar/unsichtbar zu schalten, wurde für diesen Zweck deutlich auf die Konkurrenz aufgeschlossen.

Die Abmeldung hat sich ebenfalls an den Kontrahenten Facebook angenähert. War es früher noch möglich, ohne Angabe von Gründen die Plattform zu verlassen, ist dies seit neuestem auch nicht mehr möglich. Darüberhinaus werden Freunde präsentiert, die den Benutzer vermissen werden. Eine Form des Social Engineerings zum Abschied. (vgl. Lüpke-Naderhaus, 2008)

4.1.6. Auswertung kaioo.com

Welche Felder müssen bei der Registrierung unbedingt angegeben werden?
Vorname, Nachname, Geschlecht, Geburtstag, Land, Region, Sprache, Personentyp, Ort, E-Mail, Passwort, CAPTCHA zum Bestätigen des Vorgangs

Gibt es eine definierte Mindestlänge für Passwörter?
Nein, auch Passwörter mit einem Buchstaben werden akzeptiert.

Welche datenschutzrechtlichen Mechanismen bietet die Plattform für angemeldete Benutzer?
kaioo wird in den Medien als studiVZ Ablöse gehandhabt. Viele Benutzer erhoffen sich bei kaioo den besseren Datenschutz, weil die Plattform gemeinnützig geführt wird. Dennoch: Bei den Privatsphäre-Einstellungen hinkt kaioo deutlich hinterher. Funktionen wie die generelle Profilsichtbarkeit, die Sichtbarkeit von Kontaktdaten sowie Freundschafts- und Besucheinstellungen sind sehr viel oberflächlicher konfigurierbar. Obwohl auch kaioo die Standardwerte bei neuen Profilen sehr offen ansetzt und damit Profil, Freundesdaten und Neuigkeiten über das eigene Profil bei Freunden angezeigt werden, sind Kontaktdaten immer nur für die definierten Freunde sichtbar.

Ist eine Abmeldung von der Plattform möglich?
Eine Abmeldung ist möglich.

Welche Fragen werden bei der Abmeldung gestellt?
Keine. Es wird lediglich das Passwort verlangt.

Wie lang dauert eine Abmeldung und welche Inhalte eines Benutzers werden gelöscht?
Das Profil wird sofort nach der Benutzer-Interaktion gelöscht. Vorbildlich ist der Hinweis (siehe Abbildung 13), was genau mit den Profildaten passiert:

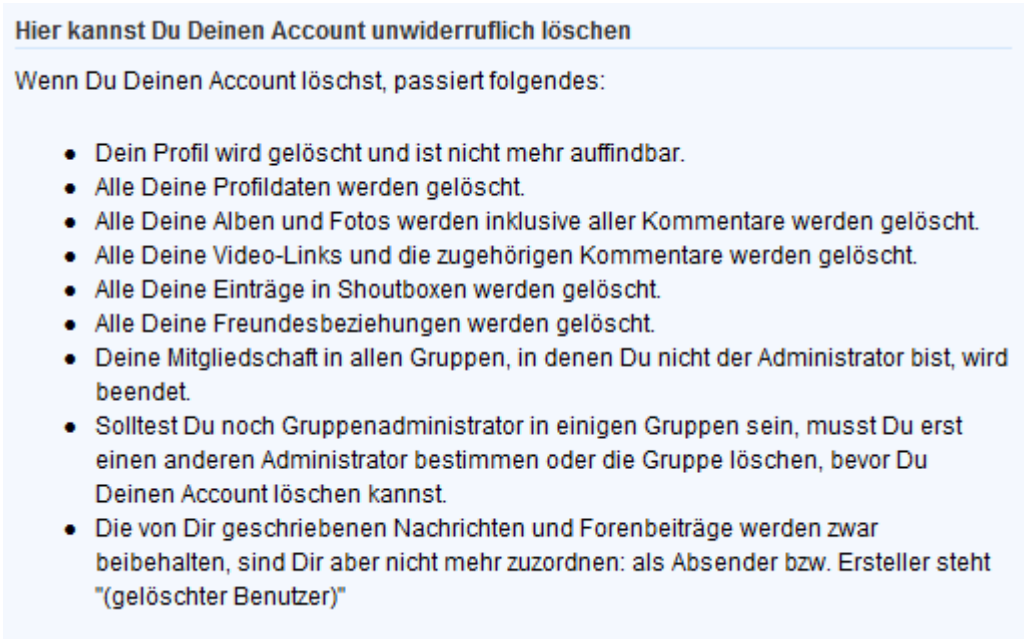

Abbildung 13: Was passiert mit den Profildaten nach ihrer Löschung auf kaioo?

Welchen AGBs und Datenschutzbestimmungen stimmt der Benutzer zu?
Die AGB und Datenschutzbestimmungen[16] von kaioo sind im Gegensatz zu den anderen Betreibern sehr gering und beinhalten insgesamt fünf Seiten. In den AGB werden „besonders heikle“ Stellen mit Kommentaren kombiniert, um die gewählten Begrifflichkeiten verständlicher zu machen.

Benutzer von kaioo müssen mindestens 14 Jahre alt sein. Eine Kündigung der Mitgliedschaft kann von beiden Seiten durchgeführt werden. kaioo spricht von einer „Deaktivierung des Profils“:

> *„Nach einer Deaktivierung des Accounts können die Daten des Nutzers nicht mehr abgerufen werden. Es kann aufgrund der im Zwischenspeicher (Cache) vorgehaltenen Daten vorkommen, dass die Daten des Mitglieds nach Deaktivierung des Accounts aus technischen Gründen noch kurzzeitig verfügbar sind. kaioo behält sich vor, bei berechtigtem Interesse (z.B. zur Durchsetzung von Schadenersatzansprüchen bei einem Verstoß) die Daten vorerst weiter zu speichern.“*

kaioo nimmt die Kündigungsklausel sehr ernst und erklärt die technischen Umstände, warum Daten auch noch nach der Kündigung sichtbar sein können. Es wird ebenfalls im Kommentar zur Regelung darauf hingewiesen, dass versendete Nachrichten anonymisiert im System verbleiben.

[16] AGB: http://www.kaioo.com/kaioo.html?locale=de#info.terms, Stand: 05.11.2007
Datenschutzbestimmungen: http://www.kaioo.com/kaioo.html?locale=de#info.data_protection

Wie auch alle anderen Anbieter im Feld sichert sich kaioo Nutzungsrechte an den veröffentlichen Inhalten seiner Benutzer, „*insbesondere zur Vervielfältigung, Änderung, Verbreitung und Veröffentlichung*“. Als Rechtfertigung für diesen Schritt wird das Beispiel herangezogen, dass Benutzer andere Foren-Beiträge zitieren möchten, und dies ohne die Nutzungsrechte nicht rechtens wäre.

Die Nutzungsbedingungen beinhalten einen Vermerk zur Analyse von personenbezogenen Daten:

> *„kaioo kann das Verhalten seiner Nutzer analysieren, um das inhaltliche Angebot besser auf die Bedürfnisse der Nutzer abstimmen zu können. Die Daten werden jedoch nicht personenbezogen verarbeitet, sondern die Identität des Nutzers bleibt anonym.“*

Auch in diesem Fall kommentieren die Eigentümer von kaioo bereits vor Protesten die Klausel und begründen diese mit der Verbesserung angebotener Funktionen und schließen personalisierte Werbung explizit aus. Daten werden nicht an Dritte weitergegeben, außer es besteht „*eine gesetzliche Verpflichtung*“ dazu.

Als Gerichtsstand gilt Deutschland. Die Nutzungsbedingungen unterliegen dem Recht der Bundesrepublik Deutschland. Eine Änderung der Datenschutzbestimmungen kann laut kaioo „*von Zeit zu Zeit*“ notwendig werden. Die aktuell gültige Fassung befindet sich auf der Webseite abrufbar. Durch die knappe Formulierung dieser Klausel entfallen kritische Aussagen, wie diese bei den amerikanischen Plattformen vorhanden sind. Im Gegensatz zu studiVZ und XING hat kaioo hierbei eine benutzerunfreundliche Passage weitestgehend durch gekonnte Formulierung verschwiegen.

4.1.7. Auswertung Xing.com

Welche Felder müssen bei der Registrierung unbedingt angegeben werden?
Anrede, Vorname, Nachname, Benutzername, Passwort, E-Mail, CAPTCHA zum Bestätigen des Vorgangs, Status, Firma, Position, Branche, Land/Region Geschäftlich, Bundesland Geschäftlich, Ort Geschäftlich

Gibt es eine definierte Mindestlänge für Passwörter?
Mindestens 4 Zeichen

Welche datenschutzrechtlichen Mechanismen bietet die Plattform für angemeldete Benutzer?
Datenschutzeinstellungen werden bei Xing groß geschrieben. Es können sowohl generelle Privatsphäre-Einstellungen getroffen werden, die über die Funktionen der anderen getesteten Plattformen hinausgehen, als auch auf *Personenebene* definiert werden, welche Daten sichtbar sind. Als Business Netzwerk versteht Xing die Bedürfnisse seiner Benutzer am besten und überlässt hier nichts dem Zufall.

Ist eine Abmeldung von der Plattform möglich?
Eine Abmeldung ist möglich, jedoch nur sehr schwer auffindbar. Es gibt weder in den Einstellungen, noch in der Konto-Übersicht einen Menüpunkt, der auf eine Abmeldung hindeuten würde. Erst in den Hilfeseiten unter dem Punkt „Mitgliedschaft & Rechnung“ ist als Antwort auf die Frage „Wie kann ich die kostenlose Mitgliedschaft kündigen/meinen Account löschen?“ ein Link auf die tatsächliche Seite. (s. Anhang XING1)

Welche Fragen werden bei der Abmeldung gestellt?
Es werden keine Fragen gestellt, es ist jedoch möglich, einen Grund anzugeben.

Wie lang dauert eine Abmeldung und welche Inhalte eines Benutzers werden gelöscht?
Die Löschung des Profils erfolgt sofort. Während auf der ersten Seite aufgelistet wird, welche Daten des Profils gelöscht werden, wird nach Beendigung der Löschung sogar angezeigt, wie viele Datensätze pro Bereich tatsächlich gelöscht wurde, wie Abbildung 14 verdeutlicht:

Ihre Mitgliedschaft bei XING wurde soeben beendet.
In der unten stehenden Liste sehen Sie einen Überblick über die Daten, die durch die Beendigung Ihrer Mitgliedschaft gelöscht wurden:

		Datenlöschung
Profil	Ihre Businessdaten	1 gelöscht
	Ihre Kontaktdaten	1 gelöscht
	Ihre Fotos	--- keine ---
	Ihre "Über mich"-Seite	--- keine ---
	Einträge in Ihrem Gästebuch	--- keine ---
Private Nachrichten	in Ihren Postfächern	1 gelöscht

Abbildung 14: Überblick über die Daten, die bei Xing gelöscht wurden

Welchen AGBs und Datenschutzbestimmungen stimmt der Benutzer zu?
Die AGB und Datenschutzbestimmungen[17] von Xing beinhalten 12 Seiten. Eine Teilnahme bei XING ist prinzipiell erst ab der Volljährigkeit möglich. Bei der Registrierung dürfen keine Pseudonyme oder Künstlernamen verwendet werden. Profilfotos dürfen laut AGB nicht älter als fünf Jahre alt sein und keine Firmenlogos beinhalten. Mitglieder dürfen nicht einer Sekte oder in Deutschland umstrittenen Glaubensgemeinschaft angehören. XING darf die AGB jederzeit ändern, verpflichtet sich jedoch Benutzer über diesen Schritt zu informieren und eine zweiwöchige Frist zur Akzeptanz der neuen Regelungen einzuräumen.

Als Business-Netzwerk beinhalten die AGB und Datenschutzbestimmungen im Gegensatz zu den anderen verglichenen Plattformen teilweise stark differenzierende Formulierungen, wie die folgende Klausel zeigt:

> *„Sofern die Nutzer über die XING-Websites Verträge untereinander schließen, ist XING hieran nicht beteiligt und wird daher kein Vertragspartner. Die Nutzer sind für die Abwicklung und die Erfüllung der untereinander geschlossenen Verträge allein verantwortlich. XING haftet nicht, falls über die XING-Websites im Zusammenhang mit einem solchen Vertrag kein Kontakt zwischen den Nutzern zustande kommt."*

XING stellt eine Business-Plattform zur Verfügung. Die Geschäfte, die über die Plattform geschlossen werden, sind für die Betreiber tabu. Bei der Beendigung des Vertrags zwischen XING und dem Benutzer wird auf das Kontaktformular verwiesen. Die angebotene Funktion zur Kündigung des Kontos wird nicht erwähnt. Die Kündigung der unentgeltlichen Mitgliedschaft ist jederzeit möglich. Bei der Kündigung der entgeltlichen Mitgliedschaft kommt es zu Fristen von 14 Werktagen.

Als anwendbares Recht definiert XING sowohl das deutsche Datenschutzgesetz, europäische Datenschutzrichtlinien und „jedes andere anwendbare Datenschutzrecht". Dies ist im Gegensatz zu allen anderen Anbietern im Vergleich einzigartig.

[17] AGB: https://www.xing.com/app/user?op=tandc.popup;what=tandc, Stand:

Wie alle anderen Anbieter sichert man sich das Nutzungsrecht an Inhalten seiner Benutzer. Dieses beschränkt sich jedoch lediglich auf Beiträge in Foren. Für Benutzer selbst ist die Vervielfältigung oder Speicherung von jeglichen Inhalten der XING Websites nicht gestattet.

Die Grundprinzipien von XING beinhalten den Schutz personenbezogener Daten:

> *„In keinem Fall wird XING Ihre personenbezogenen Daten zu Werbe- oder Marketingzwecken Dritten zur Kenntnis geben oder diese sonst wie an Dritte weitergeben. Mit Ausnahme einiger genereller Angaben über ihren beruflichen Status entscheiden Sie selbst, welche der von Ihnen bei XING eingegebenen personenbezogenen Daten durch andere XING-Mitglieder eingesehen werden können"*

Der Betreiber kommt damit den Geschäftskunden entgegen, denen der Schutz ihrer Daten sehr wichtig ist. Den Ausschluss von personenbezogener Werbung in die Datenschutzbestimmungen zu definieren lässt eine offene Firmenpolitik vermuten. Die Firma strahlt Seriosität aus. Während XING die flexibelsten Privatsphäre-Einstellungen im getesteten Umfeld aufweist, werden Angaben wie Name, beruflicher Status, Firmenname, Position, Branche und der Ort des Unternehmens fix für alle Mitglieder zugänglich gemacht. Alle anderen, freiwilligen Angaben sind standardmäßig nicht sichtbar.

Aktivitäten von Benutzern werden auf XING als sogenannter „Klickpfad" gespeichert und Premium-Mitgliedern zur Verfügung gestellt. XING verweist auf die Wichtigkeit dieser Funktion und nennt es ein „*zentrales Element des Kontaktmanagements*". Aus diesem Grund sei es nicht deaktivierbar. Jeder, der sich mit der Speicherung des Klickpfads nicht einverstanden erklärt, wird gebeten die Dienste von XING nicht zu nutzen. Aufzeichnungen über den Pfad werden nach Ablauf einer Woche durch den Betreiber gelöscht.

Welche Besonderheiten gibt es in der SC in Bezug auf Datenschutz?
Als Benutzer eines kostenlosen Profils sind viele Funktionalitäten der Plattform eingeschränkt. Die letzten Besucher des Profils werden zum Beispiel angezeigt, jedoch fehlt hierbei die Namensgebung und die Möglichkeit das Profil zu besuchen. Bei der Suche hat man ebenfalls deutlich eingeschränkte Optionen.

4.1.8. Gesamtbeurteilung der Anbieter

Die Auswertung zeigt, dass es sehr große Unterschiede bei der Handhabung des Datenschutzes in sozialen Netzwerken gibt. Alle Anbieter setzen zwar auf ähnliche Funktionen, um die Privatsphäre der Benutzer zu schützen. Die Ausprägung dieser Einstellmöglichkeiten ist jedoch sehr verschieden. Während bei MySpace, Facebook, studiVZ und kaioo bestimmten Kontakt-Gruppen eher der Zugriff auf Profilinformationen entzogen werden kann, ist der Ansatz bei Xing genau umgekehrt. Kontakte können erst nach manueller Kontaktaufnahme und Eingriff beider Benutzer granularen Zugriff auf Profilinformationen des anderen erlangen.

Das Medienkulturzentrum Dresden e.V. hat vier der fünf hier analysierten Plattformen Anfang des Jahres verglichen. Die Ergebnisse der Auswertung wurden in Tabelle 5 zusammengefasst. Bei dem Punkt Datenschutz schneiden alle Plattformen laut dem Kulturzentrum „gut" ab. Einzig bei der Nutzerfreundlichkeit bekommt Facebook nur eine „schlechte" Beurteilung. (vgl. Medienkulturzentrum, 2008b)

	Datenschutz	Transparenz	Nutzerfreundlichkeit
Myspace	****	***	****
SchuelerVZ/studiVZ	****	***	****
Facebook	****	***	**

	Datenschutz	Transparenz	Nutzerfreundlichkeit
kaioo	****	*****	****

Tabelle 5: Datenschutz-Einstufung von Medienkulturzentrum Dresden e.V. (verkürzt)

Die eigene Analyse ergab ein sehr differenziertes Bild. Eine Klassifizierung der jeweiligen Plattformen fällt schwer und ist auch nur wenig hilfreich. Communities werden nicht aufgrund ihrer Datenschutzbemühungen verwendet, sondern aufgrund der bereits angemeldeten Freunde. Eine Reihung der Plattformen ist daher nicht notwendig. Die nachfolgende Bewertung resultiert auf einem subjektiven Eindruck, gestützt auf die Ergebnisse der Analyse sowie den im Rahmen der Arbeit recherchierten Pressemeldungen:

MySpace:
MySpace ist ein amerikanischer Anbieter und daher bereits aufgrund der geltenden Rechtslage für deutschsprachige Benutzer nicht unbedingt zu empfehlen, da Daten immer in den USA gespeichert werden. Positiv hervorzuheben ist, dass MySpace diese Tatsache bereits während der Registrierung hervorhebt. MySpace verfolgt eine Passwortrichtlinie, die ebenfalls zu einer besseren Sicherheit führt. Die Notwendigkeit von eigenen SPAM Einstellungen ist ein Indiz dafür, dass es vermehrt zu ungewünschten (Werbe-)Nachrichten kommt. CAPTCHAs können benutzerdefiniert auf der eigenen Profilseite eingeführt werden. Eine Abmeldung von der Seite ist möglich und erfolgt innerhalb von 48 Stunden. Dabei werden jene Daten gespeichert, die für die Erfüllung von gesetzlichen Bestimmungen notwendig sind. Auch nach Löschung des Profils bleibt der Vertrag zwischen MySpace und dem Benutzer gültig.

Die Verwendung von MySpace ist für Neulinge sehr unintuitiv; das Layout der Seite führt oftmals zu Verwirrung. Vermehrte Phishing-Angriffe sowie die fragwürdige Funktion der Benutzernamen ohne Überprüfung auf gefährliche Wörter verdeutlichen das negative Bild in Bezug auf Datenschutz und Informationssicherheit.

Die AGBs und Datenschutzbestimmungen dürfen jederzeit ohne Vorankündigung durch MySpace verändert werden. Benutzer akzeptieren Änderungen an den AGBs automatisch durch die Nutzung der Plattform. Der Betreiber behält sich das Recht vor Daten an Dritte zur Überprüfung der Nutzungsbestimmungen zu übermitteln. Prinzipiell wird personalisierte Werbung durch die AGB erlaubt, eine Möglichkeit zur Deaktivierung ist vorhanden. Vertraglich wird die Überprüfung von veröffentlichten Daten durch den Nutzer durch ein Software-Tool geregelt. In erster Linie wird dies für die Aufdeckung von Urheberrechtsverletzungen verwendet.

Unter dem Strich ist die größte Social Community der Welt nicht zu empfehlen und eine Verwendung aufgrund der AGB und Probleme, die in Vergangenheit mit der Sicherheit der Benutzerdaten auftraten, nicht ratsam.

Facebook:
Facebook ist ebenfalls ein amerikanischer Anbieter, bei dem alle Daten in Amerika gespeichert werden. Facebook weist auf diese Tatsache nicht explizit beim Registrierungsprozess hin. Es besteht eine einfache Passwortrichtlinie. Als einziges System überprüft Facebook sowohl den eingegebenen Namen sowie die E-Mail-Adresse auf Gültigkeit. Eine Registrierung mit den meisten Fake-E-Mail-Adressen-Services ist daher nicht möglich. Da Facebook die Möglichkeit zur „Installation“ von fremden Applikationen innerhalb der Community erlaubt, müssen für jede dieser Applikationen, sowie für Facebook selbst Privatsphäre-Einstellungen getroffen werden. Dabei ist zu beachten, dass die *Facebook Platform Applications* von fremden Entwicklern erstellt werden, die selbst Datenbestände über Facebook Nutzer speichern können. Eine Abmeldung von Facebook ist nicht möglich. Auch nach einer Deaktivierung des Profils ist der Benutzer auf Fotos verlinkbar.

Die AGB, die sowohl in englischer als auch deutscher Sprache vorliegen, sind lediglich in englischer Ausführung gültig. Facebook kann jederzeit ohne Vorankündigung die AGB ändern. Benutzer akzeptieren Änderungen an den AGBs automatisch durch die Nutzung der Plattform. Facebook erlangt nicht-exklusive, weltweite Rechte an den veröffentlichen Inhalten seiner Benutzer. Der Betreiber behält sich das Recht vor Kopien der aktuellen und ehemaligen Benutzerinhalte anzufertigen und für eine angemessene Zeit zu speichern. Facebook darf weitere Informationen über seine Benutzer in Zeitungen, Blogs und weiteren definierten Medien sammeln, die für personalisierte Werbung herangezogen werden dürfen. Facebook darf Daten an Dritte weitergeben. Auch nach dem Ableben von Benutzern behält der Betreiber die Daten seiner Benutzer im System online.

Das Umfeld von Facebook in Bezug auf die Nähe zu amerikanischen Geheimdienstorganisationen ist ebenfalls fragwürdig, auch wenn es sich hierbei um eine mögliche Verschwörungstheorie handeln könnte. Der Autor rät jedem Benutzer **dringend Facebook** aufgrund der Regelungen **nicht zu verwenden**. Wer bereits Mitglied auf dieser Plattform ist, sollte so wenig wie möglich Informationen über sich Preis geben und keine *Platform Applications* benutzen.

studiVZ:
Der deutsche Branchenprimus hat bereits viele negative Erfahrungen mit dem Datenschutz erleben müssen. Es wurden daher in den letzten Monaten viele Änderungen an den Privatsphäre-Einstellungen und angebotenen Funktionen durchgenommen. Aktuell besteht die gleiche Passwortrichtlinie wie bei Facebook. Eine Löschung des Profils ist möglich und erfolgt innerhalb von 48 Stunden. Seit Dezember 2007 gelten neue AGB, die oftmals negativ in den Medien erwähnt wurden. Seitdem wurde viel Informationsmaterial veröffentlicht, dass den Umgang mit den Datenschutz näher erklären soll.

Die AGB selbst sind im Gegensatz zu den amerikanischen Anbietern um einiges freundlicher. Benutzer müssen bereits zwei Wochen vor einer möglichen Änderung darüber informiert werden. Benutzer müssen zumindest mit einem Klick den neuen Regelungen zustimmen, bevor diese in Kraft treten. Personalisierte Werbung wird angeboten, kann jedoch durch den Benutzer deaktiviert werden. Die Nutzung von studiVZ unterliegt deutschem Recht, das durch die europäischen Datenschutzrichtlinien in Bezug auf Datenschutz deutlich schärfer ist als das amerikanische Recht.

Vor allem die noch sehr junge Historie von studiVZ, bei der jede Menge Fehler auf der Plattform auftraten und das anfangs unseriöse Umfeld trüben das Bild nachhaltig. Die Ausschweifungen der ehemaligen Gründer sowie des Supportteams sind für den Betrieb einer Social Community inakzeptabel.

Die Nutzung von studiVZ ist nur dann ratsam, wenn alle Privatsphäre-Einstellungen zur Sicherung der Profildaten überprüft und adaptiert werden. Da vor allem Experten berechtigte Zweifel an der Sicherheit studiVZs haben, kann die Plattform daher nur sehr eingeschränkt empfohlen werden. Der Vergleich der Anbieter zeigte jedoch, dass studiVZ sich nach Jahren der Probleme am richtigen Weg befinden könnte.

kaioo:
Der gemeinnützige Verein besitzt im Allgemeinen weder Stärken, noch Schwächen. Als einziger Betreiber ist keine Passwortrichtlinie vorhanden, was bei der Fokussierung auf den Datenschutz überrascht. Ein deutlich besserer Datenschutz als bei dem großen Kontrahenten studiVZ ist nicht erkennbar. Man beschränkt sich lediglich auf die Aussage, dass man einen gemeinnützigen Verein ohne Gewinnzwang darstelle. Diese Tatsache trägt jedoch zu keiner besseren Informationssicherheit innerhalb der Plattform bei. Eine Abmeldung von der Seite ist möglich und wird sofort durchgeführt. Vorbildlich ist der Hinweis, welche Daten gelöscht werden. Als einziger Anbieter scheut man nicht vor der Information, dass Nachrichten und Forenbeiträge anonymisiert erhalten bleiben.

Die AGB und Datenschutzbestimmungen sind im Vergleichsumfeld sehr kurz. Kritische Passagen werden durch erklärende Kommentare abgemildert. kaioo behält sich zur ordnungsgemäßen Nutzung der Plattform Rechte an den veröffentlichten Inhalten der Benutzer vor. Diese dienen jedoch nur zur reibungslosen Bereitstellung von Funktionen und werden nicht dazu genutzt um Daten an Dritte weiterzugeben. Auch kaioo unterliegt wie studiVZ dem deutschen Recht. Änderungen an der Datenschutzerklärung können jederzeit vom Betreiber durchgeführt werden. Hier ist man im Gegensatz zu den Bestimmungen von studiVZ deutlich Benutzer unfreundlicher.

Prinzipiell kann die Nutzung von kaioo empfohlen werden. Benutzer müssen dennoch auf ihren Selbstschutz achten. Die Plattform ist im Gegensatz zu allen Anbietern sehr jung und beinhält wenige Funktionen. Die Informationssicherheit muss auf dieser Plattform erst langfristig überprüft und bestätigt werden. Die Nähe zum Bertelsmann-Konzern lässt auch kaioo fragwürdig erscheinen. Auf jeden Fall gilt: Nur weil Medien oder Rapper (s. Kapitel 4.1.1.4) sagen, dass kaioo um einiges sicherer ist als studiVZ sollte dies nicht immer blind geglaubt werden.

XING:
Das teilweise kostenpflichtige Business Netzwerk hat im Vergleich zu allen anderen Anbietern ein sehr ausgeklügeltes Privatsphäre-Modell. Es können sehr viele Einstellungen zu den Profildaten getroffen werden und Daten werden prinzipiell nur auf Kontaktebene freigegeben. Die Möglichkeit zur Löschung des Profils ist gegeben, befindet sich jedoch unscheinbar in den FAQs der Seite versteckt. Bei der Löschung wird vorbildlich die Menge an Datensätzen angezeigt, die durch das System gelöscht wurden. Ein Hinweis auf den Verbleib von Nachrichten in Foren fehlt.

Die Datenschutzrichtlinien beinhalten den Grundsatz, dass XING personenbezogene Daten nie für Werbe- oder sonstige Zwecke an Dritte weitergeben würde. Gäste dürfen nur diejenigen Informationen sehen, die der Benutzer freigibt. Die AGB dürfen durch den Betreiber verändert werden, man verpflichtet sich jedoch zur expliziten Bekanntgabe und der Wahrung einer zweiwöchigen Frist, in der Benutzer die Regelungen akzeptieren müssen.

Der *Klickpfad* stellt das Herzstück von XING dar und zeichnet die einzelnen Aktionen des Benutzers auf der XING Webseite auf. Diese Funktion kann nicht deaktiviert werden. XING weist selbst darauf hin, dass Benutzer, die diese Funktion nicht akzeptieren, eine andere Community benutzen sollen.

Die Seite beinhält die am weitest ausgeprägten Mechanismen zur Wahrung der Privatsphäre und des Datenschutzes. Der Autor empfiehlt daher die Nutzung von XING zur Wartung des persönlichen Business Netzwerks. Dennoch ist darauf hinzuweisen, dass auch XING durch die Schaltung von Werbung innerhalb von Profilen bereits negativ in die Schlagzeilen geriet.

4.1.8.1. Löschung od. Deaktivierung

Der Anmeldeprozess auf Social Communities ist einfach. Auch wenn viele Profilfelder eingegeben werden müssen, um ein Profil zu erstellen, wird man in den meisten Fällen mit Hilfetexten unterstützt. Denkt man jedoch daran die Plattform zu verlassen, sieht das Bild deutlich differenzierter aus. Bei MySpace, studiVZ, kaioo und Xing ist eine Löschung des Profils und der veröffentlichten Inhalte theoretisch möglich. Betreiber beziehen sich dabei jedoch ausschließlich auf das Profil des Benutzers, nicht auf alle publizierte Kommentare, Einträge in Gästebüchern oder Foren, die in den meisten Fällen, zumindest anonym, erhalten bleiben. Eine komplette Löschung aller Daten ist daher nicht möglich. Christiane Biederlack, eine Mitarbeiterin von studiVZ antwortet in einem Interview mit dem Magazin back view (Welzel, 2007) zur Fragestellung der Löschung: „*In diesem Fall werden alle Daten des Profils sofort*

und vollständig gelöscht." Der Hinweis darauf, dass alle anderen Daten bestehen bleibt, fehlt in dem Interview gänzlich. Nach der durchgeführten Löschung geben sich sowohl MySpace, studiVZ als auch kaioo wortkarg. Im Gegensatz dazu präsentiert XING eine genaue Statistik darüber, wie viele Datensätze gelöscht wurden. Die Transparenz über die gespeicherten Daten ist bei XING auch nach der Löschung vorbildlich. Anzumerken ist jedoch, dass auch XING die weitere Speicherung der Nachrichten innerhalb von Gruppenforen verschweigt.

Bei Facebook ist es als einzigem Anbieter im Feld gar nicht möglich sein Profil zu löschen. Es kann lediglich deaktiviert werden. Selbst die Deaktivierung kann erst erfolgen, wenn ein Grund für diesen Vorgang angegeben wird. Auch nach der Deaktivierung des Profils ist es (auch nach Auswahl des Benutzers, dass dies nicht erwünscht ist) möglich, Nachrichten von Facebook zu erhalten. Noch schlimmer ist die Tatsache, dass deaktivierte Profile weiterhin zu Events eingeladen und auf Fotos markiert werden können.

Benutzer, die sich für eine Registrierung bei einer Community interessieren, sei daher das Fazit der Arbeit ans Herz gelegt, in dem darauf hingewiesen wird, dass es sinnvoll ist, vorab ein Testkonto einzurichten um Probleme bereits vor dem Veröffentlichen von persönlichen Daten klären zu können.

4.2. Umfrage unter Benutzern von Social Communities

Um die Stimmung der Benutzer innerhalb der Szene näher untersuchen zu können, wurde im Zeitraum von 01.03.2008-05.04.2008 eine Umfrage zum Thema „Datenschutz in Social Communities" im Internet unter der Adresse http://datenschutz.ownz-the.eu/ durchgeführt. Als Umfragesoftware wurde die Applikation von http://www.onlineumfragen.com/ herangezogen, da diese bereits Analysen zur Erstellung von statistischen Auswertungen beinhaltet. Die Umfrage richtete sich hauptsächlich an Benutzer von sozialen Netzwerken und wurde daher ausschließlich per E-Mail, Blogeinträgen, sowie direkten Postings innerhalb von den fünf untersuchten Plattformen beworben. Der partizipative und virale Gedanken der Websphäre zeigte bei der Verbreitung der Umfrage seine Gültigkeit. Während alle namhaften Verlage, die über die Umfrage informiert wurden, (verständlicherweise ob der vielen universitären Umfragen) mit Absagen das Thema nicht in ihre Online-Angeboten aufnahmen, kam aus der Blogging-Community durchwegs positives Feedback. So gab es Personen, die selbstständig die Umfrage auf ihr Weblog übernahmen, und viele konnten sich durch eine kurze E-Mail ebenfalls dazu überreden lassen, über die Befragung zu berichten. Daraus entstanden viele Blogeinträge, die durchwegs sehr kritisch über das Vorhaben berichteten. Das Kernproblem, das schon sehr früh in der medialen Berichterstattung aufgezeigt wurde, war die nicht gegebene Repräsentanz der Befragung. Darüberhinaus wurde vermutet, dass nur jene Personen an einer Umfrage teilnehmen würden, die Interesse bzw. Vorwissen zu der Thematik hätten. (zum Beispiel: vgl. Weigert, 2008a). Dass diese Meinung teilweise bestätigt werden konnte, wird in nachfolgenden Fragestellungen bestätigt. Innerhalb des Befragungszeitraums wurde der Fragebogen 1535 Mal aufgerufen. 846 Personen nahmen an der Umfrage teil. Die durchschnittliche Ausfülldauer betrug 8 Minuten. Aufgrund der Beschaffenheit der Befragungssoftware kam es zu Teilnehmern, die nicht alle Fragen beantworteten. Die Zahl der Personen, die alle Fragen beantworteten, betrug daher lediglich 641. Als Hilfestellung wurde daher bei der Häufigkeitsverteilung die jeweilige Anzahl an teilnehmenden Personen vermerkt.

Das Angebot, die Resultate der Umfrage, zu veröffentlichen, bzw. an interessierte Personen zu verschicken, stieß auf großes Interesse. 63 Personen (circa jeder 13 Teilnehmer) kamen der Aufforderung während des Befragungszeitraums nach und zeigten Interesse an der Auswertung. Auch nach Beendigung der Befragung, in der die Webseite online blieb, meldeten sich interessierte Personen (darunter auch der studiVZ CMO, der in Kapitel 4.2.5 zu den Fragestellungen interviewt wurde).

Bevor näher auf die gestellten Fragen, bzw. die Auswertung der Teilnehmer eingegangen wird, möchte der Autor darauf hinweisen, dass es sich hierbei um eine *nicht repräsentative Befragung* handelt, die nur einen Trend widerspiegeln kann. Ein zentraler Punkt der Auswertung war, ob durch die steigende Anzahl an Berichten über Probleme mit dem Datenschutz in Social Communities vergleichbare Ergebnisse mit bereits durchgeführten Umfragen Unterschiede im Datenschutz-Bewusstsein der Benutzer zeigen würden. Generell ist jedoch darauf hinzuweisen, dass eine Umfrage, die nur das Thema des Datenschutzes behandelt, tendenziell häufiger von Personen durchgeführt wird, die zumindest ein Grundinteresse am Thema haben, bzw. Personen, die bereits durch vorherige Fragestellungen zu einem Umdenken bei möglichen Antworten verleitet wurden die tatsächliche Aussagekraft der Ergebnisse verfälschen können.

Um die Aussagekraft der Umfrage zu steigern, werden die Ergebnisse mit anderen Studien der letzten Monate verglichen. Somit werden Gemeinsamkeiten herausgefunden und Unterschiede aufgezeigt.

4.2.1. Teilnehmerübersicht

Die Auswertung der Länderverteilung (Tabelle 7) zeigt, dass der Großteil der Umfrageteilnehmer aus Österreich und Deutschland stammt. Leider konnten nur 9 Personen aus der Schweiz zur Teilnahme motiviert werden.

Land	Teilnehmerzahl	In Prozent
Österreich	357	56
Deutschland	264	41
Schweiz	9	1
Sonstige	11	2

Tabelle 6: Teilnehmer nach Ländern

Die Auswertung nach dem Geschlecht der Teilnehmer zeigt eine deutliche Mehrheit für das männliche Geschlecht. Nur 30% der Teilnehmer an der Umfrage waren weiblich.

Der aktuelle Beschäftigungsstand der befragten Nutzer war sehr stark zerstreut (s. Tabelle 8). Erfreulich ist, dass aus jeder Beschäftigungsgruppe Benutzer an der Umfrage teilgenommen haben. Studenten nahmen am häufigsten an der Umfrage teil – dieses Ergebnis war auf Grund der Aussendungen, des Umfelds des Autors und der Arbeit, bzw. dem starken Fokus auf studiVZ und Facebook bereits anzunehmen. Überraschend ist die geringe Anzahl an Schülern im Teilnehmerfeld, da diese Gruppe sehr stark in Social Communities aktiv ist.

Beschäftigungsstand	Teilnehmerzahl	In Prozent
Schüler	51	8
Lehrling	10	2
Student	277	43
Arbeiter/Angestellter	221	34
Selbstständig	64	10
Ohne Beschäftigung	8	1
Sonstiges	11	2

Tabelle 7: Teilnehmer nach Beschäftigungsfeld

Auf weitere demographische Merkmale wurde bei der Erstellung des Fragebogens verzichtet. Dies hatte mehrere Gründe. Einerseits war der Fragebogen mit 33 Fragen (abzüglich der demographischen Merkmale) für eine freiwillige Online-Umfrage bereits überdurchschnittlich

lang, andererseits wollte der Autor nicht nach weiteren Merkmalen auswerten. Überraschenderweise trat ein Teilnehmer der Umfrage auf den Autor zu, der sich Gedanken über die fehlenden demographischen Merkmale machte. Im Zeitalter von Targeting und Datamining, in dem Benutzer ihre Gedanken ausführlich in sozialen Netzwerken publizieren ist ein Kategoriedenken nicht mehr erforderlich. Erfolgreich sind Anbieter nur dann, wenn auf die Bedürfnisse der Benutzer eingegangen werden kann. Durch gezielte Auswertung der Fragen wäre es sehr leicht, passende Inhalte für Benutzer zu finden, würde es sich bei dieser Umfrage um eine Community handeln, und wäre der Autor der Arbeit ein gewinnorientiertes Unternehmen.

4.2.2. Auswertung

Die Auswertung der Umfrage gliedert sich in zwei Themenkomplexe:

- Häufigkeitsverteilung
- Erweiterte Analyse

Bei der Häufigkeitsverteilung werden die gestellten Fragen einzeln betrachtet und analysiert. Die grünen Balken zeigen jeweils die Antwort mit der meisten Zustimmung durch die Teilnehmer. N bezeichnet die Anzahl an Teilnehmern pro Frage. Gemeinsam mit den Ergebnissen von anderen namhaften Studien aus dem Bereich der Social Communities werden Feststellungen und Thesen abgeleitet, die in der erweiterten Analyse besprochen werden. Dabei werden die aggregierten Antworten von mehreren Fragen statistisch gegenüber gestellt und auf eine Signifikanz zwischen den Antworten überprüft.

4.2.3. Häufigkeitsverteilung

Bei welcher der folgenden Social Communities bist du registriert? (Mehrfachauswahl möglich, N = 837)

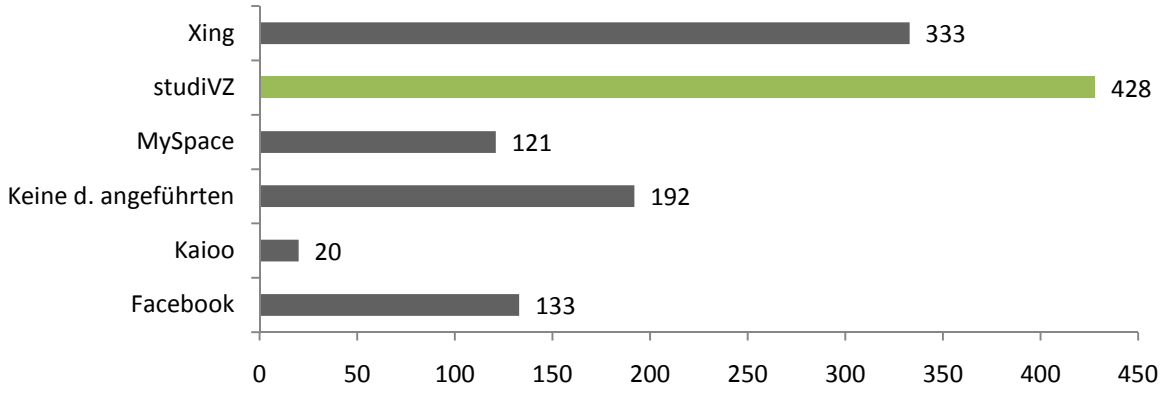

Diagramm 2: Welche, der untersuchten Communities, nutzen die Teilnehmer der Umfrage?

Knapp die Hälfte aller Teilnehmer ist bei studiVZ registriert. Die negativen Medienberichte der letzten Monate dürften studiVZ langfristig keine nennenswerten Verluste bei der Mitgliederzahl gebracht haben. Die Verteilung zeigt weiter, dass die beiden amerikanischen Plattformen, die in der vorliegenden Arbeit näher betrachtet werden, im deutschsprachigen Raum durch die klare Dominanz von studiVZ, nur wenige Mitglieder haben. Auf Platz zwei der Auswertung kommt Xing, dass als Business Netzwerk einen sehr guten Ruf genießt. Eben-

falls bemerkenswert ist das Ergebnis, dass 16% der Befragten bei keiner der fünf Communities registriert sind.

Bei wie vielen Social Communities bist du zurzeit registriert? (N = 794)

Registrierungen	Anzahl	Prozent	Prozent kumm.
0	70	8.82	8.82
1	220	27.71	36.53
2	182	22.92	59.45
3	124	15.62	75.07
4	72	9.07	84.14
5	64	8.06	92.20
6	22	2.77	94.97
7	4	0.50	95.47
8	9	1.13	96.60
9	1	0.13	96.73
10	13	1.13	98.73

Tabelle 8: Bei wie vielen Social Communities sind die Teilnehmer registriert?

Minimum: 0
Maximum: 50
Modalwert: 1
Median: 2
Arithmetisches Mittel: 2,7

Im Vergleich zur CommunityEffects Studie (Brieke, 2008) ergibt sich hier ein ähnliches Ergebnis. Die meisten Teilnehmer sind nur auf einer Plattform registriert (vgl. Modalwert). DataPortability spielt daher für den Standardbenutzer von Social Communities aktuell noch keine Rolle. Dieser Sachverhalt kann sich jedoch in Zukunft ändern, wenn immer mehr Betreiber auf DataPortability, OpenSocial oder weiteren Standards zum Austausch der Daten setzen.

Nur 70 Personen sind in keiner Social Community registriert. Mit Blick auf die Frage 1 bedeutet dies, dass viele der Teilnehme, die angegeben haben, bei keiner der fünf auswählbaren Plattformen registriert zu sein, vor allem kleine (Nischen)-Player bevorzugen.

Wie viel Zeit (in Minuten) verbringst du täglich in Social Communities? (Einfachauswahl, N = 694)

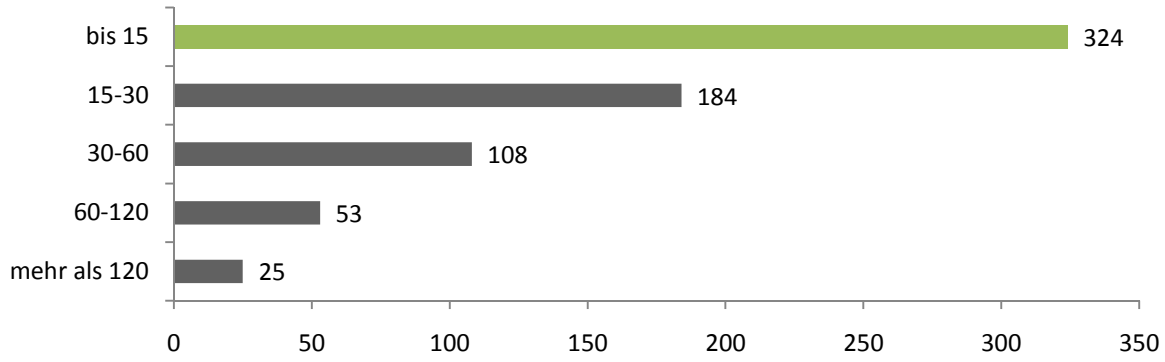

Diagramm 3: Wie viel Zeit verbringen Benutzer in Social Communities?

Die Verweildauer zeigt, dass 80% der befragten Teilnehmer täglich weniger als 60 Minuten Social Communities nutzen. Knapp die Hälfte der Teilnehmer ist weniger als 15 Minuten pro Tag online. Diese Erkenntnis deckt sich weitestgehend mit der von Nielsen Online durchgeführten Studie zur Verweildauer in Social Communities, wenn man die Werte durch Median/Arithmetisches Mittel auf einzelne Communities herunter rechnet.

Aus welchen Gründen nutzt du Social Communities?
(Mehrfachauswahl, N = 693)

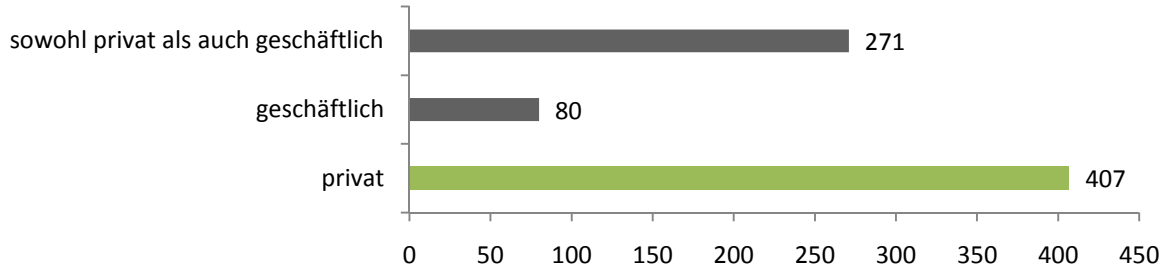

Diagramm 4: Aus welchen Gründen werden Social Communities genutzt?

Mehr als die Hälfte der Teilnehmer nützen Social Communities nur im privaten Umfeld. Auffallend gering ist die rein geschäftliche Nutzung. Daraus lässt sich die Hypothese definieren: *Xing Benutzer sind auch in anderen Communities aktiv?*

Aus welchen Gründen nutzt du Social Communities?
(Mehrfachauswahl, N = 693)

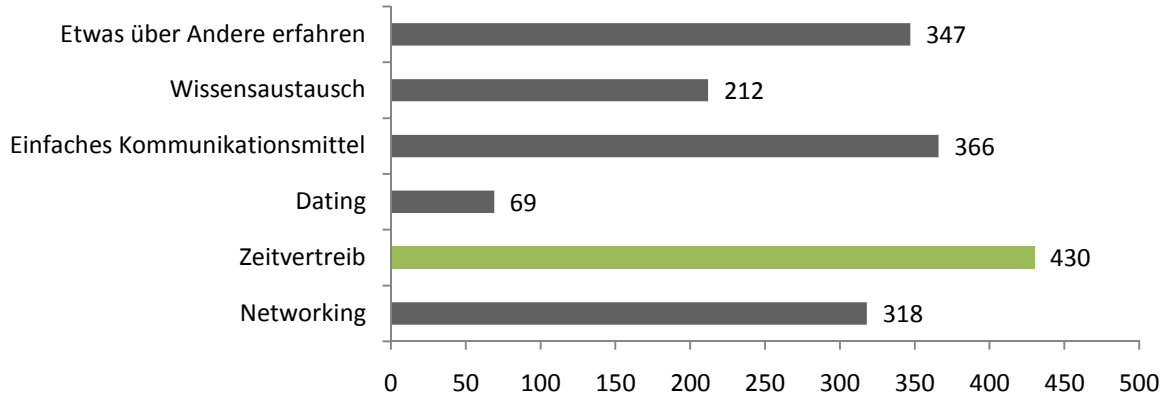

Diagramm 5: Aus welchen Gründen werden Social Communities genutzt?

Die Hauptnutzungsgründe decken sich mit den Ergebnissen des obigen Diagramms. Communities werden hauptsächlich zum Zeitvertreib und als Kommunikationsmittel benutzt. Weit abgeschlagen ist die Antwortmöglichkeit „Dating“. Communities, die die Kommunikation ihrer Benutzer noch mehr vereinfachen können liegen daher richtig. Die Einbindung eines Instant Messaging Programms in Facebook ist hierfür ein gutes Beispiel. Benutzer werden durch die Chat-Möglichkeit auf der Plattform gebunden. Die Betreiber haben mit Hilfe der neuen Funktion daher sowohl Zeitvertreib als auch Kommunikation ermöglicht. Als Nebeneffekt steigt die Verweildauer der Benutzer auf der Plattform; der Wert der Community steigt.

Hast du Bedenken, deine privaten Daten (wie Name, Adresse, E-Mail-Adresse, Telefonnummer, ...) in Social Communities zu veröffentlichen?
(Einfachauswahl, N = 726)

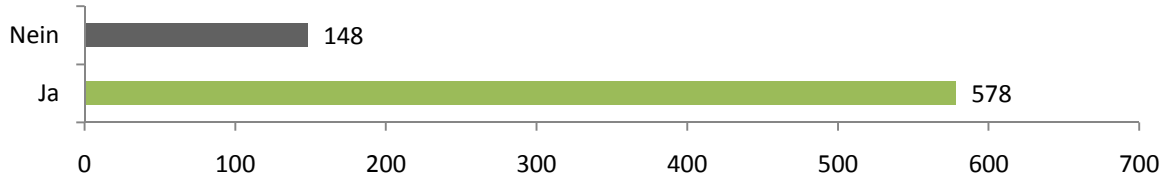

Diagramm 6: Haben Benutzer Bedenken beim Veröffentlichen von privaten Daten?

75% der Teilnehmer haben Bedenken Daten zu veröffentlichen. Das Ergebnis der Frage fällt sehr deutlich aus. Eine Vergleichsfrage zu Bedenken der Veröffentlichung von Daten im Web hätte Aufschluss darüber liefern können, ob dies ein Phänomen ist, das nur in Communities auftritt, oder ob dies generell mit dem Internet in Zusammenhang steht. Der sehr deutliche Prozentsatz zeigt auf jeden Fall, dass Datenschutz einen höheren Stellenwert einnehmen sollte. Alarmierend ist die Betrachtung, dass Personen, obwohl sie Bedenken haben, ihre Daten weiterhin veröffentlichen. Es ist davon auszugehen, dass Personen ihre eigene Privatsphäre bei der Nutzung von Social Communities als zweitrangig erachten.

Wenn Ja, worauf beziehen sich deine Bedenken?
(Mehrfachauswahl, N = 568)

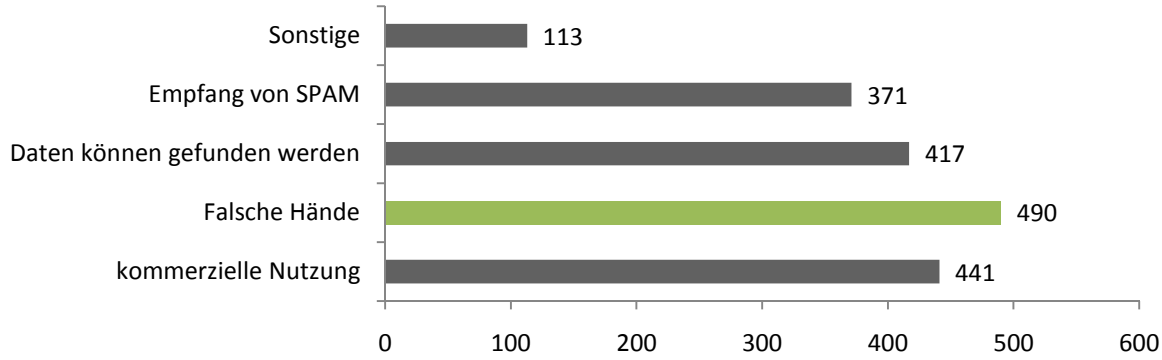

Diagramm 7: Worauf beziehen sich die geäußerten Bedenken?

Die Gründe für die Bedenken sind sehr verschieden, ein klarer Favorit kann sich nicht herauskristallisieren. Bei der Mehrfachauswahl geben mehr als 80% der Teilnehmer an, dass Daten in falsche Hände gelangen könnten, oder diese für kommerzielle Nutzung herangezogen werden. Die Bedenken des Empfangs von unerwünschten (Werbe-)Nachrichten (SPAM) sind vergleichsweise gering. Im Gegensatz zu den großen amerikanischen Anbietern wie MySpace und Facebook, bei denen die SPAM-Problematik an der Tagesordnung steht und daher umfangreiche Maßnahmen seitens der Betreiber unternommen werden, ist die Gefahr, die von SPAM ausgeht, deutlich geringer. Keine der verglichenen deutschsprachigen Communities hat eigene SPAM-Einstellungen. Dies dürfte vor allem auf die Tatsache zurückzuführen sein, dass die deutschen Anbieter im Vergleich zu den amerikanischen Communities deutlich kleiner sind.

Ist es für dich relevant, in welchem Land Daten, die du über dich veröffentlichst, gespeichert werden?
(Einfachauswahl, N = 713)

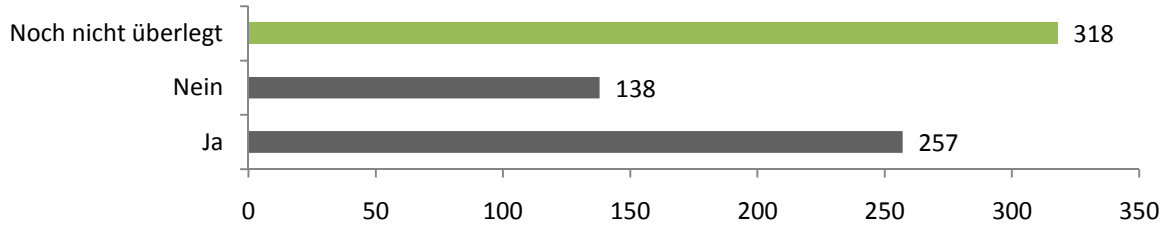

Diagramm 8: Ist der Speicherort der Daten für die Teilnehmer relevant?

Der Großteil der Leute hat sich noch keine Gedanken über dieses Thema gemacht. Dieses Thema spielt jedoch dann eine entscheidende Rolle, wenn ausländische Communities genutzt werden. Amerikanische Anbieter speichern alle anfallenden Daten in den USA, in denen gänzlich unterschiedliche Datenschutzbestimmungen gelten, wie die Ausführungen in Kapitel 3.1.5 zeigen. Es ist daher notwendig, dass Benutzer für das Bewusstsein der Datenspeicherung sensibilisiert werden. Auf Platz zwei der Auswertung landen Personen, die sich bereits über den Speicherort Gedanken gemacht haben. Dieser Umstand könnte ein Zeichen dafür sein, dass viele Experten an der Umfrage teilgenommen haben. Hierzu lautet eine These des Autors: *Je mehr man sich mit Datenschutz beschäftigt hat, desto wichtiger erachtet man den Speicherort*.

Erwartest du dir von einer geschäftlichen Community (zB: Xing) mehr oder weniger Datenschutz als von einer Plattform für Freizeitnutzung (zB: MySpace)?
(Einfachauswahl, N = 704)

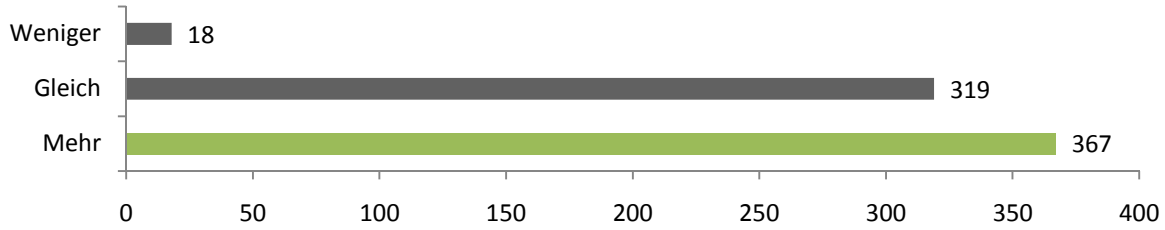

Diagramm 9: Erwarten sich Benutzer geschäftlicher Communities mehr Datenschutz als von Communities für Freizeitnutzung?

Das Ergebnis bei dieser Frage ist eindeutig. Benutzer erwarten zumindest gleich viel oder mehr Datenschutz innerhalb von geschäftlichen Communities. Betreiber von Business Netzwerken wie XING sollten daher Datenschutz ernst nehmen, um ihre Benutzer zufriedenzustellen. Der durchgeführte Vergleich der Communities kann dieses Bild bestätigen. XING hat die variabelsten Privatsphäre-Einstellungen im Feld.

Erwartest du dir von einer (teilweise) kostenpflichtigen Community (bsp: Xing) mehr oder weniger Datenschutz als von einer gratis Plattform? (Einfachauswahl, N = 703)

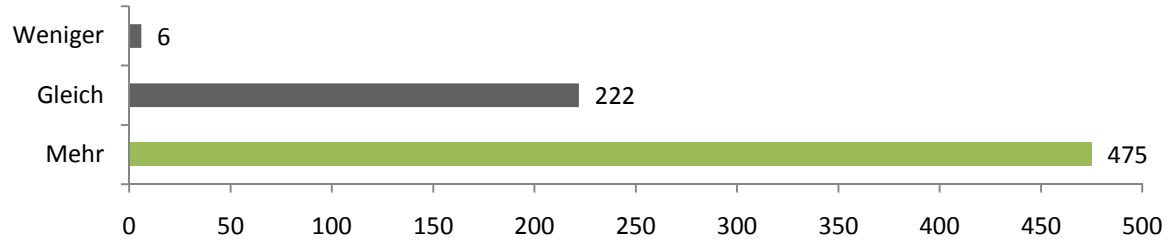

Diagramm 10: Erwarten sich Benutzer von kostenpflichtigen Communities mehr Datenschutz als von kostenlosen Communities?

Auch dieses Ergebnis war zu erwarten. Müssen Benutzer für die Nutzung einer Community bezahlen, erwarten sie sich einen höheren Datenschutz. Hier ist wieder auf das Beispiel XING verwiesen, dass nicht nur als Business Netzwerk, sondern ebenfalls als (teilweise) kostenpflichtige Community betrieben wird und den Schutz seiner Mitglieder als sehr wichtig erachtet.

Aus welchen Gründen entscheidest du dich für eine bestimmte Community? (Mehrfachauswahl, N = 673)

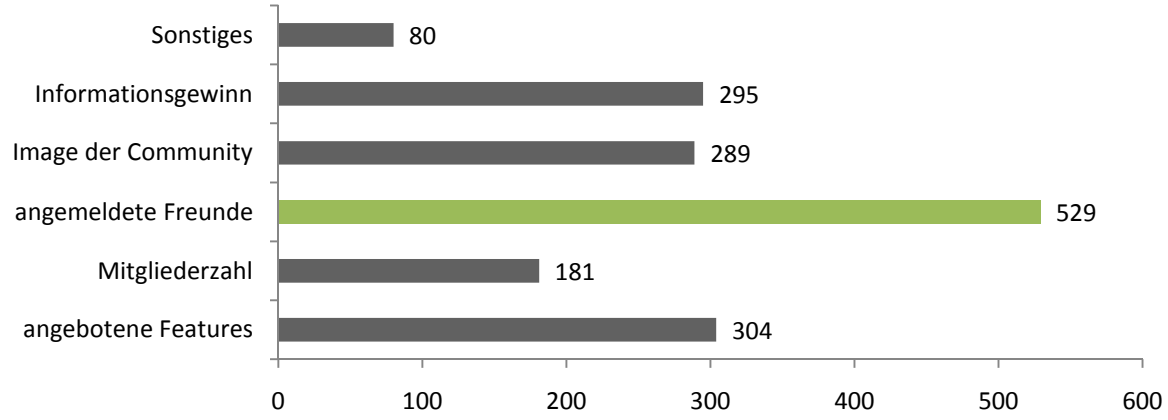

Diagramm 11: Welche Gründe sprechen für eine Registrierung bei einer bestimmten Community?

Die wenige Wochen zuvor durchgeführte SNS Umfrage zeigt ein ähnliches Ergebnis (vgl. CSCM, 2008): Benutzer registrieren sich auf Plattformen, bei denen ihre Freunde bereits angemeldet sind. Angebotene Funktionen spielen nur eine sekundäre Rolle. Hat eine Community die kritische Masse an Benutzern erreicht, ist es daher für Kontrahenten schwer Fuß zu fassen. Die angebotenen Funktionen oder ein möglicher Informationsgewinn können fehlende Kontakte nicht wettmachen. Amerikanische Plattformen, die in Deutschland Fuß fassen wollen, werden es vermutlich gegen studiVZ/meinVZ schwer haben. Wenn bereits alle Freunde in den VZ-Netzen registriert sind, besteht keine Notwendigkeit sich in anderen Netzen anzumelden. Auch die Gesamtmitgliederzahl ist im Vergleich zu den anderen Faktoren eher zweitrangig.

Hast du dich schon mal bei einer Community nicht registriert, weil du mit den AGBs nicht einverstanden warst?
(Einfachauswahl, N = 689)

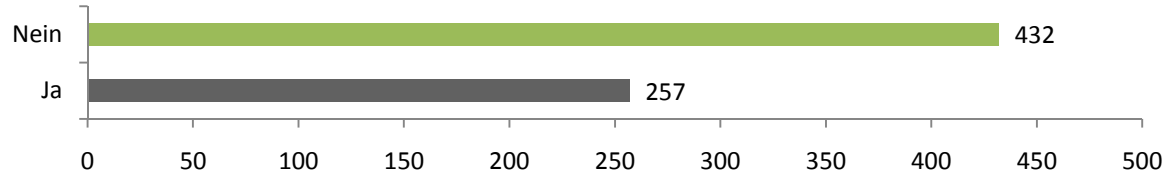

Diagramm 12: Wird die Registrierung abgebrochen, weil Benutzer mit den AGB nicht einverstanden sind?

Zwei Drittel der Teilnehmer antworten mit einem klaren Nein. Das Ergebnis lässt darauf hindeuten, dass nur wenige Teilnehmer die AGB vor der Registrierung lesen. Die Auswertung der AGB von MySpace, Facebook, studiVZ, kaioo und XING zeigen, dass AGB auf jeden Fall gelesen werden sollten, um Überraschungen zu vermeiden.

Die Zahl an Personen, die sich aufgrund der AGB nicht registriert haben, ist vergleichsweise hoch. Das heißt, dass AGB sehr wohl Klauseln beinhalten, mit denen Benutzer nicht zufrieden sind.

Vertraust du darauf, dass dich die Betreiber der Communities über die Verwendung deiner Daten informieren?
(Einfachauswahl, N = 686)

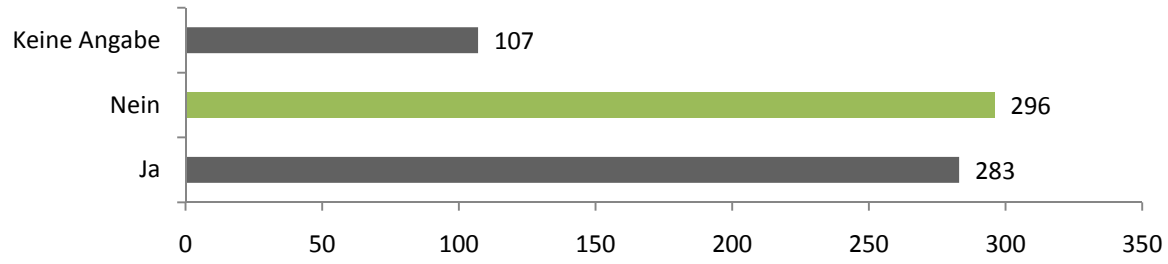

Diagramm 13: Haben Benutzer Vertrauen in die Betreiber von Communities?

Knappe 300 Personen haben kein Vertrauen in ihren Betreiber, wenn es um die Verwendung ihrer Daten geht. Weitere 100 Personen haben keine Angabe getroffen. Ein alarmierender Wert, der die bereits aufkommende Frage verdeutlicht: Warum veröffentlichen Benutzer persönliche Daten in Social Communities, wenn sie so große Bedenken dabei haben? Offen bleibt die Frage, was Betreiber in Bezug auf das Vertrauen falsch machen, beziehungsweise wie sie in Zukunft ein höheres Vertrauen seitens der Benutzer erlangen können.

Würdest du dich bei Communities registrieren, die deine Daten an Drittanbieter für Werbezwecke weitergeben?
(Einfachauswahl, N = 683)

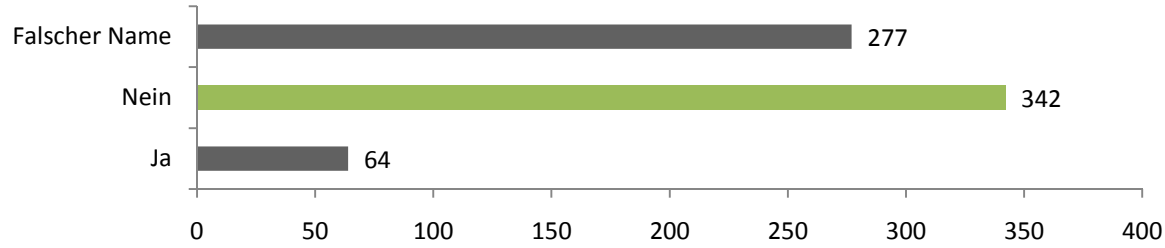

Diagramm 14: Registrieren sich Benutzer, obwohl Daten an Dritte weitergegeben werden?

Ein eindeutiges Bild bei der Frage nach der Weitergabe von Daten an Drittanbieter: 90% sprechen sich dagegen aus, wobei 40% sich dennoch, mit einem falschen Namen, registrieren würden. Nur 9% würden eine Registrierung mit dem richtigen Namen vornehmen. Wirft man einen Blick in die AGB von Betreibern und vergleicht dies mit der Zahl an Personen, die in Frage 1 angegeben haben, in Communities wie Facebook registriert zu sein, kommt man zu dem Ergebnis, dass sich nur sehr wenige Personen die AGBs vor der Registrierung durchgelesen haben. Einzelne Communities geben Daten sehr wohl („in angemessenem Rahmen“) an Dritte weiter. Desweiteren bleibt eine Frage ungeklärt: Woher wissen Benutzer, über eine Weitergabe von Daten Bescheid, wenn diese die AGBs nicht lesen? Der Fall studiVZ zeigt, dass die mediale Berichterstattung oftmals nicht objektiv genug ist: Missstände in den AGBs von studiVZ mag es geben, dennoch sind die Klauseln der amerikanischen Anbieter bei weitem gefährlicher. Diese Thematik blieb in der Berichterstattung weitestgehend unbeachtet. Das heißt, nur weil meine Community nicht negativ in die Medien gerät, heißt das nicht, dass sie keine Probleme hat.

Angenommen, du bist bei mehreren Communities registriert. Möchtest du, dass deine Daten von einer zur anderen Community automatisch mitgenommen werden können?
(Einfachauswahl, N = 676)

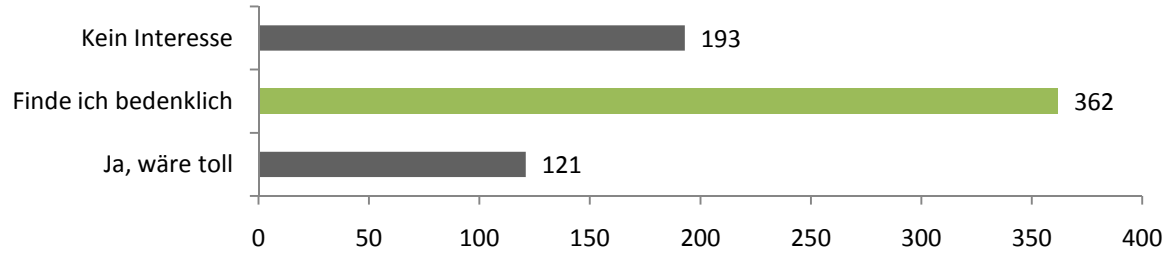

Diagramm 15: Besteht ein Interesse an DataPortability?

Lediglich jeder fünfte Teilnehmer der Umfrage begrüßt den Schritt zur Öffnung von Plattformen durch DataPortability oder OpenSocial. Jeder Zweite hält diesen Schritt eher für bedenklich. Das heißt: Auch wenn das Verfahren bald technisch realisierbar ist und sich einzelne Communities öffnen, gehört bei diesem Thema noch viel über das Vertrauen und den Datenschutz geredet. Eine Recherche zu diesem Thema ergab, dass vor allem der internationale nicht eindeutige Datenschutz bei weltweiten Netzen eine Hürde darstellen könnte (s. Kapitel 3.2.5).

Wenn ja, welche Daten möchtest du zu anderen Communities mitnehmen können? (Mehrfachauswahl, N = 119)

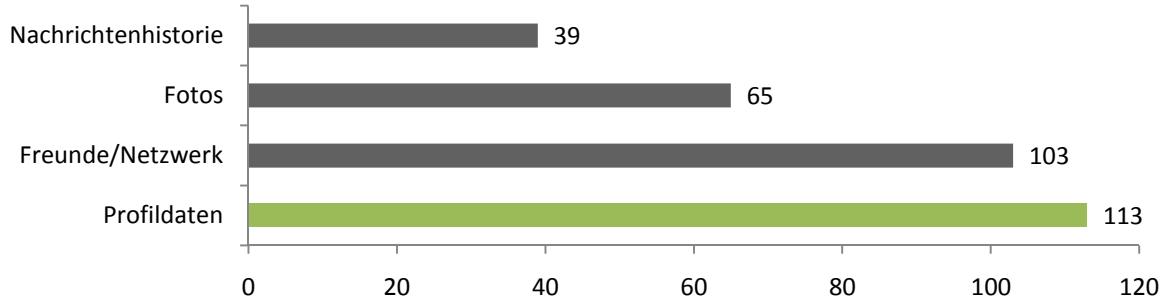

Diagramm 16: Welche Daten sollen austauschfähig werden?

Stimmt man für die Data Portability, dann ist der Hauptgrund die „Mitnahme“ der Profildaten, dicht gefolgt von dem eigenen Netzwerk. Die Teilnehmer hoffen darauf, dass die mehrfache Verwaltung redundanter Daten in Zukunft ausbleibt. Aus Sicht der Datenschützer bleibt jedoch noch die Frage nach der sicheren Realisierung dieses Vorhabens. Wer ist in Zukunft für die Daten verantwortlich? Wo werden diese gespeichert? Communities, deren Wert sich ausschließlich über die gespeicherten Daten errechnet, werden die Hoheit der Datenspeicherung wohl kaum aus der Hand geben.

Das Austauschen von Nachrichten über die Community Grenzen hinweg ist nur für 12 % der Personen interessant. Im Gegensatz zu Instant Messaging oder dem Versand von E-Mails, bei denen „Inselsysteme“ schon sehr früh aufgelöst wurden, ist die Benutzung von Social Communities für die Benutzer noch immer sehr auf das Networking und den Zeitvertreib reduziert.

Registrierst du dich mit deinem richtigen Namen in Communities? (Einfachauswahl, N = 672)

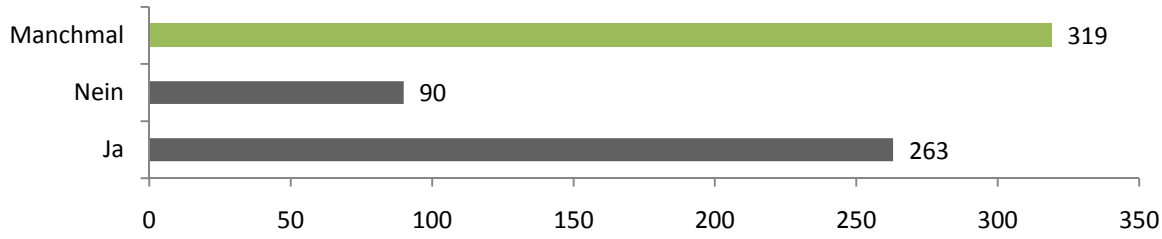

Diagramm 17: Registrieren sich Benutzer mit dem richtigen Namen?

40% der Teilnehmer geben an, sich mit dem richtigen Namen in Communities zu registrieren. Nur 13% der Befragten geben an, dass sie sich nicht mit ihrem richtigen Namen registrieren würden. Die vorliegende Fragestellung wurde sehr offen formuliert. Natürlich gibt es bei der Registrierung bei diversen Social Communities Unterschiede. Die Tatsache, dass lediglich 90 Personen (von 672 Teilnehmern) noch nie ihren eigenen Namen verwendet haben, ist beachtlich. Denn obwohl Betreiber in den AGBs Pseudonyme oder Fantasienamen ausschließen wollen, besteht kein Grund zur Akzeptanz dieser Klauseln. Communities, die sich aufgrund ihrer Mitgliederzahlen definieren, würden nur in den wenigsten Fällen Personen löschen, die Pseudonyme verwenden. Zum Beispiel verlangt studiVZ die Angabe des realen Namens. Seit den Problemen mit den AGBs im Dezember letzten Jahres haben sich

einige Personen umbenannt. Diese werden vom Betreiber nicht gelöscht – vermutlich wäre eine neuerliche mediale Berichterstattung die Folge.

Die Verwendung vom richtigen Namen sollte daher tatsächlich nur dann stattfinden, wenn persönliches Networking betrieben werden, oder die Person als „Marke“ etabliert werden soll (s. Kapitel 4.3.1). Zum Zeitvertreib ist die Angabe eines Pseudonyms ausreichend.

Welchen Anteil der Profilfelder, bei einer Registrierung in einer Community füllst du aus?
(Einzelauswahl, N = 664)

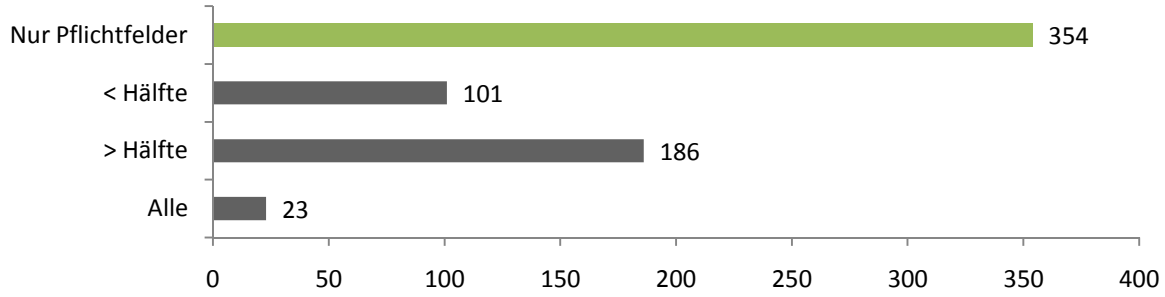

Diagramm 18: Wie viele Felder werden bei der Registrierung ausgefüllt?

Jeder zweite befragte Teilnehmer füllt bei der Registrierung nur die Pflichtfelder aus. Nur 3 % füllen alle vorgeschlagenen Felder aus. Das hier erzielte Ergebnis ist zeigt, wie wichtig die Wahl der Pflichtfelder durch den Betreiber ist. Die Auswahl von Pflichtfeldern sollte nicht leichtfertig getroffen werden und immer mit (externen) Datenschützern abgesprochen werden. Da die Hälfte der Benutzer nur die aller notwendigsten Daten ausfüllen, muss dafür gesorgt werden, dass Profile hiermit genügend Informationen zu bieten haben. Im Gegensatz dazu ist eine zu große Auswahl an Pflichtfeldern kontraproduktiv. Personen, die falsche oder keine Angaben zu einem Merkmal treffen wollen, würden bei der Registrierung falsche Daten eingeben, somit den Zweck der Plattform nicht erfüllen, oder im schlimmsten Fall die Registrierung abbrechen.

Die Auswertungen von studivz.irgendwo.org aus dem Jahr 2006 zeigen, dass von 28 ausfüllbaren Profilfeldern nur jeder zweite Benutzer mehr als die Hälfte ausgefüllt hat. (vgl. Fritsch, 2006) Der Registrierungsprozess sollte sich daher auf die unbedingt notwendigen Felder reduzieren.

Gibst du bei Registrierungen in Social Communities immer das gleiche Passwort an?
(Einfachauswahl, N = 661)

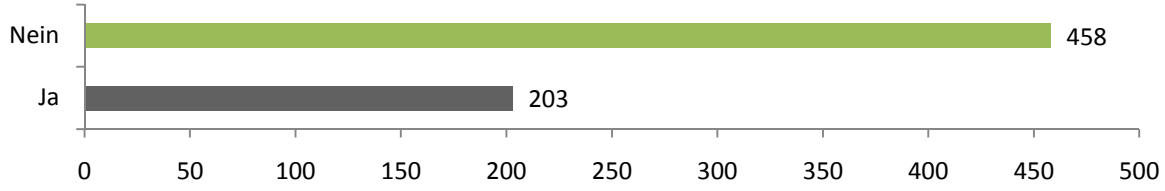

Diagramm 19: Werden unterschiedliche Passwörter in verschiedenen Communities verwendet?

2/3 der teilnehmenden Personen geben an, dass sie verschiedene Passwörter in Communities benutzen. Ein richtiger Schritt in die Richtung Datensicherheit. Dennoch benutzt jeder 3. Benutzer immer das gleiche Passwort. Dies stellt eine große Gefahr dar, sollte es Angreifern möglich sein auf die Daten zuzugreifen.

Gibst du bei Registrierungen in Social Communities immer die gleiche E-Mail-Adresse an? (Einzelauswahl, N = 656)

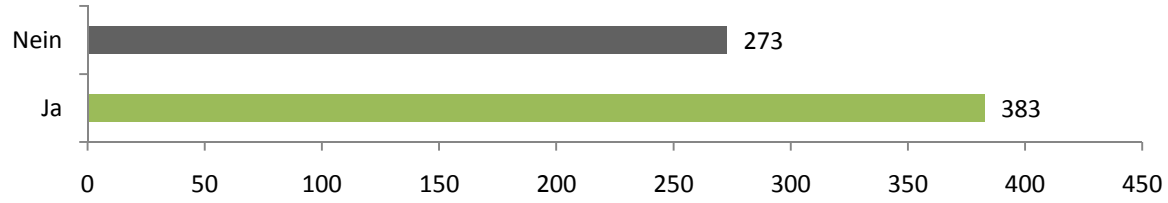

Diagramm 20: Werden unterschiedliche E-Mail-Adressen in verschiedenen Communities verwendet?

Ein Umgekehrtes Bild zeigt sich bei der Angabe von E-Mail-Adressen. Zwei von drei der befragten Personen verwenden immer die gleiche Adresse. Die Verwendung mehrerer E-Mail-Adressen dürfte für die Mehrzahl an Benutzern ein zu großes administratives Aufkommen bedeuten. Die Angabe der gleichen E-Mail-Adresse bedeutet jedoch ebenfalls potentielle Gefahr für den Benutzer, da diese als eindeutiges Erkennungsmerkmal über Plattformgrenzen hinweg betrachtet werden kann.

Bezugnehmend auf die letzten beiden Fragestellungen kommt der Autor zu folgender Hypothese: *Personen, die die gleiche E-Mail-Adresse verwenden, verwenden ein identes Passwort.*

Welche E-Mail-Adressen verwendest du bei der Registrierung in einer Social Community? (Mehrfachauswahl, N = 656)

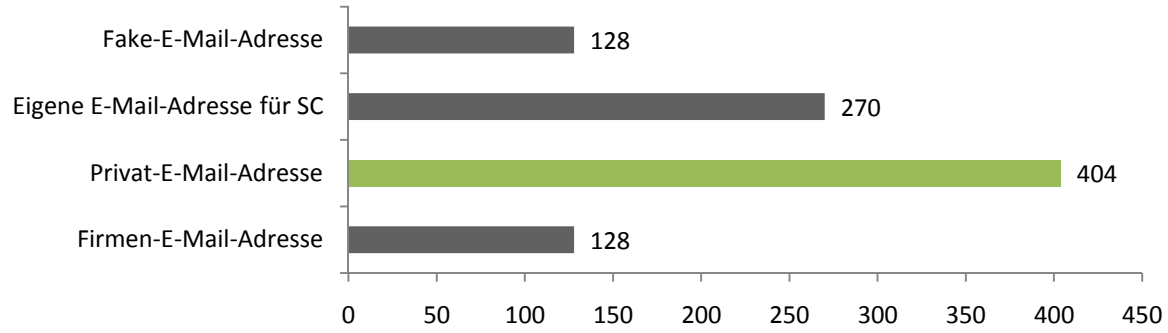

Diagramm 21: Welche E-Mail-Adressen verwenden Benutzer bei der Registrierung in einer Social Community?

Auf Platz 1 der E-Mail-Adressen-Typen landet die private E-Mail-Adresse. Erstaunlich ist, dass bereits auf Platz 2 der Antwortmöglichkeiten eine eigens für Social Communities verwendete E-Mail-Adresse liegt. Der Autor hofft, dass diese Zahl in Zukunft noch größer wird. Eine Abschottung der Community Tätigkeiten von privaten oder Firmen-E-Mail-Adressen ist eine wichtige Selbstschutzmaßnahme. Abgeschlagen auf dem letzten Platz liegen ex aequo die Firmen- sowie die Fake-E-Mail-Adressen. Auch die Verwendung von temporären Fake-Adressen stellt eine gute Möglichkeit zum Selbstschutz dar.

Communities bieten oftmals die Möglichkeit zur variablen Festlegung deiner Privatsphäre (Wer darf welche Teile deines Profils sehen?) für definierte Personengruppen. Findest du, diese Möglichkeiten ....
(Einfachauswahl, N = 649)

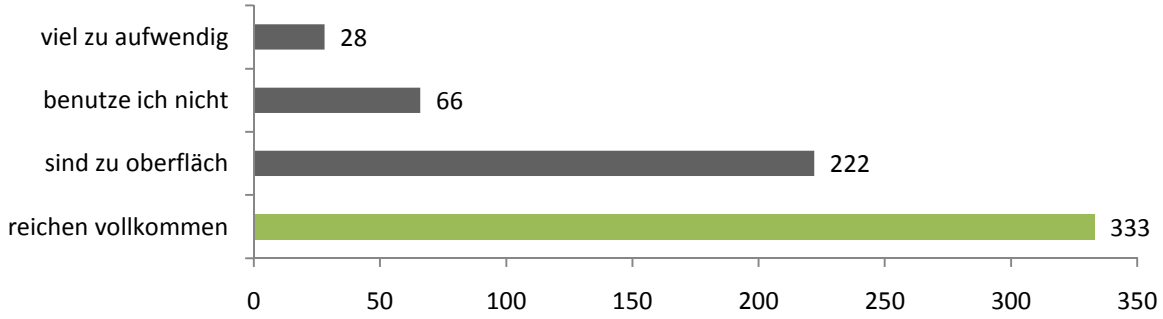

Diagramm 22: Wie empfinden Benutzer die aktuell angebotenen Privatsphäre-Einstellungen?

Die Hälfte der befragten Teilnehmer ist mit den aktuell angebotenen Privatsphäre-Einstellungen zufrieden. Jeder Zehnte nutzt diese jedoch gar nicht, dh. er vertraut auf die Standardeinstellungen, die durch den Betreiber definiert werden. Wie im Falle der Pflichtfelder bei der Registrierung ist auch hier die Rolle des Betreibers für erfolgreichen Datenschutz entscheidend. Betreiber, die standardmäßig alle Profildaten auch für Nicht-registrierte Mitglieder der Seite öffentlich zugänglich machen, sollten durch Benutzer gemieden werden. Lediglich ein Drittel der Teilnehmer möchte ausgereiftere Privatsphäre-Optionen. Die Thematik der Privatsphäre-Einstellungen wird im Experteninterview mit Herrn Weigert (s. Kapitel 4.3.1) näher analysiert.

Wenn du Bedenken bezüglich der Sicherheit deiner Daten (bsp: Zugriff durch unbefugte Dritte) hättest, welche Schritte würdest du unternehmen?
(Mehrfachauswahl, N = 653)

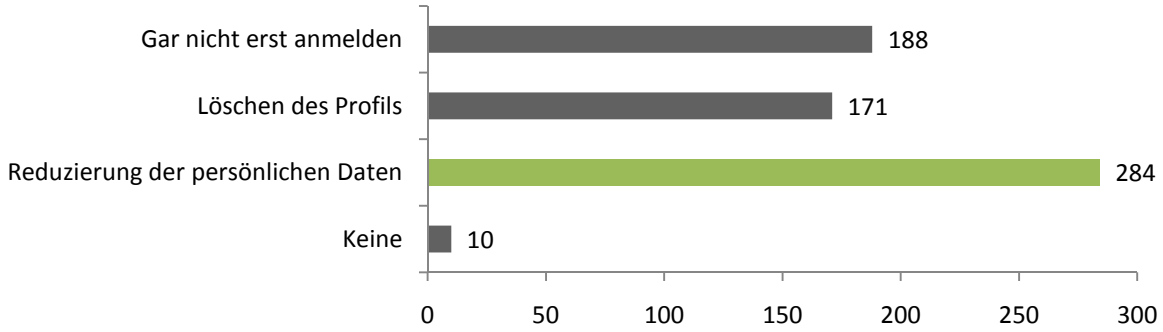

Diagramm 23: Welche Schritte würden unternommen werden, wenn Bedenken bezüglich der Sicherheit existieren?

Knapp die Hälfte der Teilnehmer würde bei datenschutzrechtlichen Bedenken die Menge an veröffentlichten Daten reduzieren. Hier liegt das Problem jedoch in den Verträgen mit den Betreibern. Im Falle von Facebook erlaubt man dem Betreiber archivierte Kopien auch von bereits veränderten Daten speichern zu dürfen. Die Reduktion der Daten funktioniert also nur

dann, wenn diese für die Öffentlichkeit nicht mehr sichtbar sein sollen. Hat man Bedenken gegenüber den Betreiber ist die Reduktion/Löschung des Profils oftmals wirkungslos.

Beunruhigend ist die Tatsache, dass lediglich jeder vierte sein Profil tatsächlich löschen würde, sollte es zu Bedenken bezüglich der Sicherheit auf der Plattform kommen. Dieses Ergebnis zeigt ebenfalls deutlich, dass der Schutz von den eigenen Daten bei der Verwendung von Social Communities keine primäre Rolle spielt.

Sprichst du mit Freunden über etwaige Bedenken im Bezug auf die Verwendung deiner Daten in Social Communities?
(Einfachauswahl, N = 645)

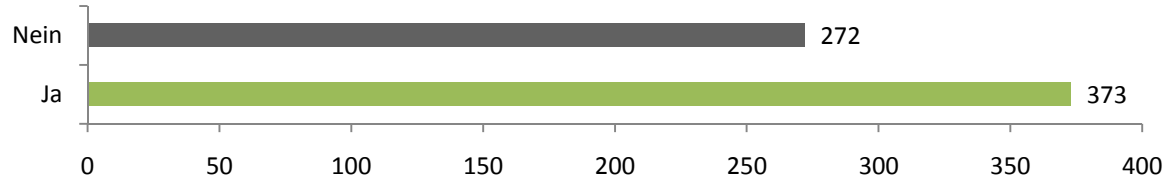

Diagramm 24: Sprechen Benutzer von Social Communities mit ihren Freunden über Datenschutz?

Zwei von drei teilnehmenden Personen sprechen mit Freunden über den Datenschutz in Social Communities. Die Zahl, die aufgrund der vielen Berichterstattungen in namhaften Medien in den letzten Wochen sicher angestiegen ist, zeigt, dass das Thema bereits „Mainstream"-Charakter bekommen hat. In Zukunft muss versucht werden, durch Berichte und weiterer Vorsprache, diese Zahl noch mehr zu steigern und das gegenseitige Bewusstsein für Datenschutz zu steigern. Vor allem der Bekanntenkreis von Benutzern ist für die nachhaltige Bewusstseinsbildung wichtig, da man den eigenen Freunden oftmals mehr glaubt als Experten.

Über welche Dienste suchst du aktiv nach Bekannten/Freunden im Internet? (Mehrfachauswahl, N = 649)

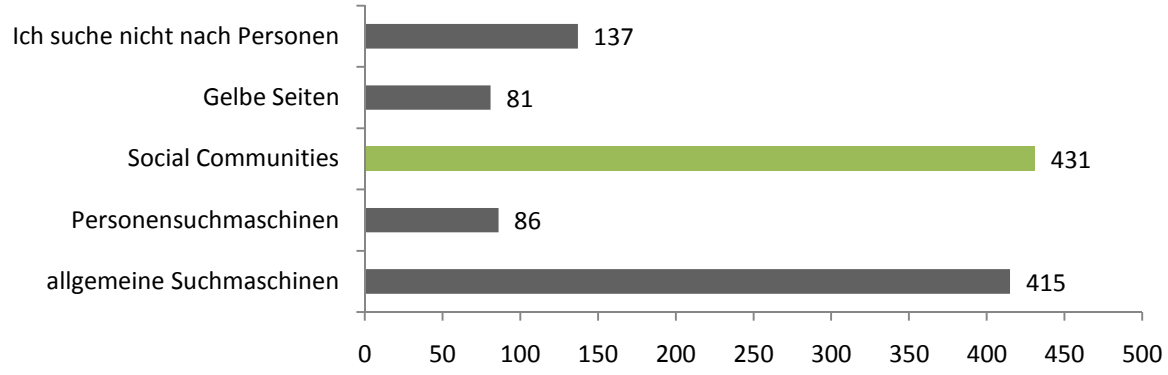

Diagramm 25: Über welche Dienste suchen Benutzer nach Bekannten/Freunden im Internet?

Social Communities sind die Recherchequelle, wenn Benutzer über Bekannte oder Freunde im Internet suchen wollen. Dichtgefolgt von allgemeinen Suchmaschinen wie Google. Weit abgeschlagen liegen Personensuchmaschinen. Dennoch werden diese in Zukunft wichtiger:

> „*Das in Wien entwickelte Portal durchsucht in Echtzeit Soziale Netzwerke, andere Suchmaschinen, auf Bilder oder Kurztexte spezialisierte Portale wie Flickr und Twitter, die Online-Enzyklopädie Wikipedia und Telefonbücher nach öffentlich verfügbaren Informationen über eine Person. […] Einnahmen generiert die Suchmaschine derzeit über die Weiterleitung an andere Portale, etwa Soziale Netzwerke*.“ (Haddad, 2008)

Die Suchmaschine 123people.com, die Anfang 2008 startete, setzt bereits jetzt auf ein Geschäftsmodell, das die Kooperation mit Social Communities forciert. Zukünftig könnte eine noch engere Kooperation sowie Mechanismen wie DataPortability oder OpenSocial dazu führen, dass Personensuchmaschinen zur ersten Anlaufstelle im Web2.0 werden, um Personen zu finden. Für alle beteiligten Parteien wäre dies eine Win-Situation. Suchmaschinenbetreiber verdienen am Weiterleiten zu den Communities, die Plattformbetreiber selbst könnten neue Mitglieder gewinnen. Für Benutzer des Social Webs bietet sich erstmals die Möglichkeit, dass gezielt nach *Personen* mit definierbaren Kriterien oder Namen im Internet gesucht werden kann. Hierbei ist jedoch das Thema des Datenschutzes nicht außer Acht zu lassen. Spezialisierte Suchmaschinen, die über jeden Menschen Informationen sammeln und bereitstellen ist für aktuell gültige Datenschutzbestimmungen einiger Länder unvereinbar. (vgl. Schormann, 2007)

Welche Teile von Social Communities benutzt du?
(Mehrfachauswahl, N = 614)

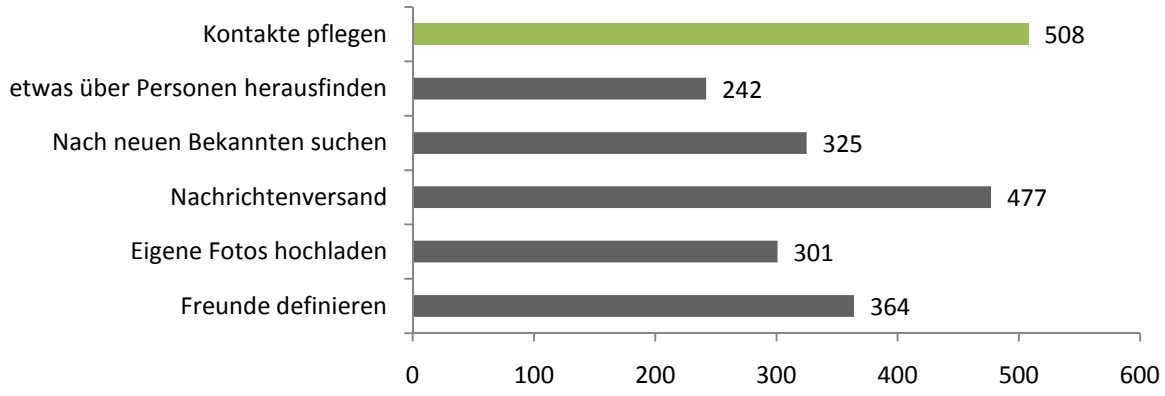

Diagramm 26: Welche Teile von Social Communities werden benutzt?

8 von 10 befragten Teilnehmern pflegen Kontakte und versenden Nachrichten. Facebook liegt daher mit seiner neuesten Entwicklung, einem Chat auf der Plattform, im Trend. Instant Messaging und E-Mails werden zwar mittelfristig nicht verschwinden, allerdings durch Social Communities harte Konkurrenz erhalten. Schon jetzt gilt die Kontaktpflege über E-Mails als zeitaufwendig (vgl. Kapitel 4.3.1). Das Hochladen von Fotos, das Suchen nach neuen, sowie verlinken mit alten Bekannten benutzt jeder zweite Benutzer. Generell gibt es keine Auswahlmöglichkeit im Test, die nicht oder nur sehr wenig genutzt wird. Die angebotenen Funktionen von Social Communities ähneln sich oftmals und man kann daher bei den hier angeführten Antworten als „Standardfunktionssammlung“ von Communities sprechen.

Wurden schon einmal (vielleicht Jahre später) Daten von dir im Internet gefunden, die dir unangenehm waren?
(Einfachauswahl, N = 642)

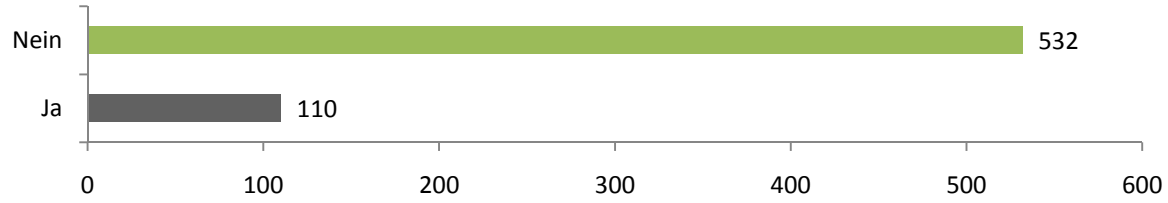

Diagramm 27: Kamen Benutzer bereits in unangenehme Situationen aufgrund veröffentlichter Daten?

80% der Teilnehmer haben bis jetzt noch keine unangenehmen Situationen erlebt, in denen kompromittierende Daten über den Teilnehmer gefunden wurden. Die breite Nutzung von Communities steckt aktuell noch in den Kinderschuhen, daher ist diese Zahl nicht wirklich überraschend. Dennoch mussten bereits 110 Teilnehmer negative Erfahrungen machen.

These: *Jemand, über den bereits unangenehme Daten gefunden wurden, löscht seine Daten (Profil), wenn diese nicht mehr relevant sind.*

Löschst du dein Profil, wenn du nicht mehr in der Community aktiv bist?
(Einfachauswahl, N = 638)

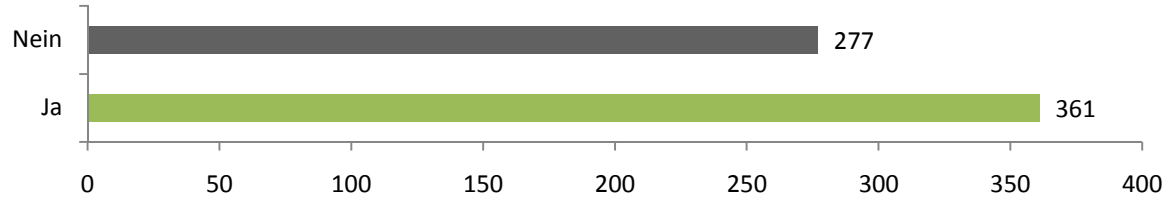

Diagramm 28: Löschen Benutzer ihre Profile, wenn kein Interesse mehr besteht?

Nur 57% der befragten Teilnehmer löschen ein Profil, wenn sie nicht mehr in der Community aktiv sind. Das heißt, dass in Zukunft Mitgliederzahlen von Plattformen kritischer betrachtet werden müssen, da einige der ausgewiesenen Profile nicht mehr verwendet werden. Bisher gibt es Statistiken über den monatlichen Zuwachs von Benutzern, aber nur vereinzelt Studien darüber, wie viele der registrierten Benutzer tatsächlich aktiv sind und bleiben.

Für Datenschützer ist diese Aussage nur schwer zu verstehen. Viele Benutzer verzichten auf die Löschung ihrer Daten, die ungeachtet vom Benutzer weiterhin für eine Vielzahl an Personen zur Verfügung stehen. Auch wenn man sich selbst nicht mehr daran erinnern kann, kann es sein, dass veröffentlichte Daten Jahre später auftauchen. Sei es bei einem Bewerbungsgespräch oder bei der Recherche von Zeitungen über die eigene Person. Die Bedrohungsszenarien sind hier schier unendlich.

Aus welchen Gründen würdest du dein Profil in Social Communities löschen? (Mehrfachauswahl, N = 641)

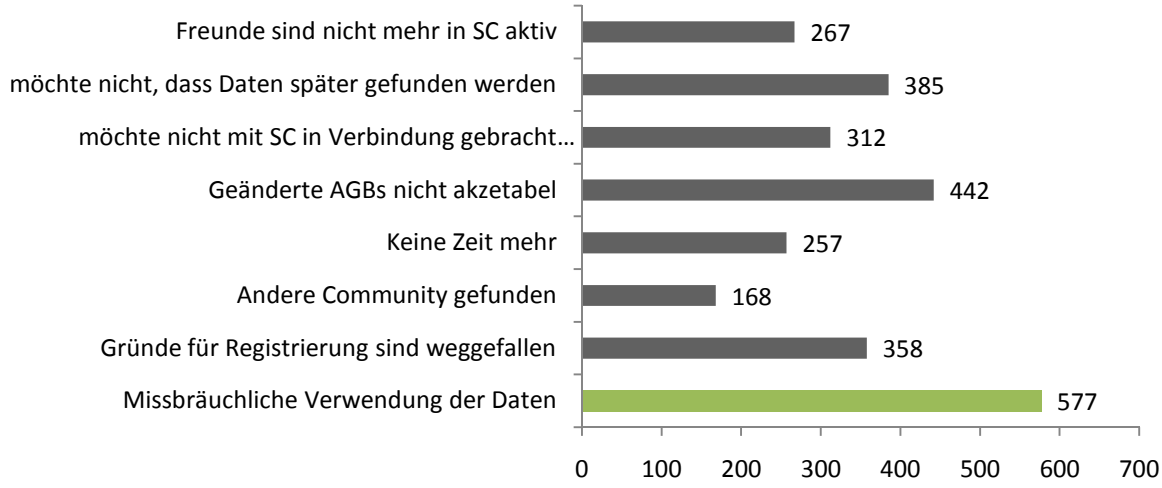

Diagramm 29: Weshalb würden Profile in Social Communities gelöscht?

90% der Teilnehmer würden ihr Profil sofort löschen, wenn es zu einer missbräuchlichen Verwendung ihrer Daten käme. Im Vergleich zur Fragestellung, welche Schritte unternommen werden würden, wenn es datenschutzrechtliche Bedenken gibt, ist hier ein deutlicher Unterschied zu erkennen. Ebenfalls 70% würden ihr Profil löschen, wenn die geänderten AGBs nicht akzeptabel wären.

Eine logische Schlussfolgerung dieses Ergebnisses ist daher, dass die von studiVZ neu entworfenen AGB trotz der lauten Kritik in den Medien für viele Benutzer dennoch akzeptabel sind (s. Kapitel 4.2.5) . 90% aller Benutzer haben den neuen Bestimmungen zugestimmt. Ein Unternehmenssprecher von studiVZ sagte in einem Interview, dass gemessen an der Mitgliederzahl die Proteste der Änderungen sehr gering waren. (vgl. Welzel, 2007)

Ebenfalls noch 6 von 10 Personen geben an, das Profil löschen zu wollen, damit Daten in Zukunft nicht mehr gefunden werden könnten. Obwohl angemeldete Freunde das Top Argument für eine Registrierung in einer Social Community sind, würden nur 4 von 10 Personen ihr Profil löschen, wenn ihre Freunde ebenfalls nicht mehr in der Community aktiv wären.

Findest du es selbstverständlich, dass bei dem Löschen deines Profils alle Daten tatsächlich gelöscht werden?
(Einfachauswahl, N = 648)

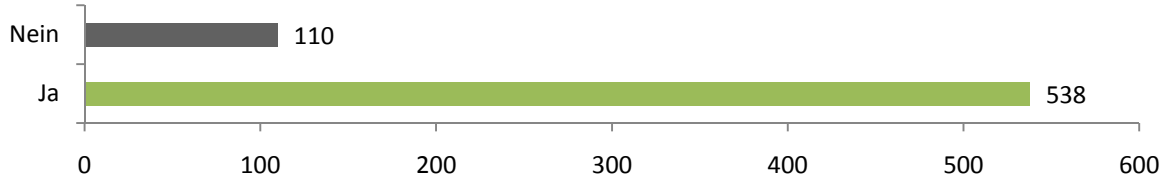

Diagramm 30: Finden es Benutzer selbstverständlich, dass alle Daten gelöscht werden?

Ein klares Bild: 83% finden es selbstverständlich, dass alle Daten tatsächlich gelöscht werden. 17% finden diesen Schritt nicht selbstverständlich. Die Realität zeigt, dass die tatsächliche Menge, die bei einer Profilkündigung gelöscht wird, sehr variiert. Da bei Facebook ledig-

lich eine Deaktivierung des Profils möglich ist, dürfte dies bei einigen Benutzern für Verärgerung führen, wenn diese Tatsache bekannt wird. Auch wenn eine Änderung der Firmenrichtlinien nicht auszuschließen ist, sollte daher vor der Registrierung bei einer Social Community immer ein Testkonto eingerichtet werden um zu überprüfen, dass eine Löschung des Profils möglich ist.

Wie genau hast du dich bereits mit dem Thema Datenschutz auseinander gesetzt? (Einfachauswahl, N = 648)

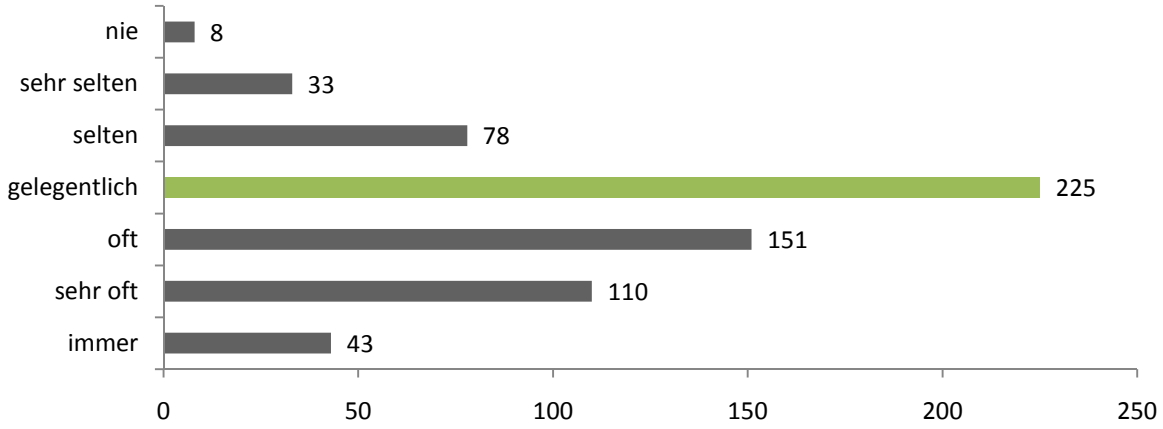

Diagramm 31: Wie genau haben sich Teilnehmer bisher mit dem Datenschutz auseinander gesetzt?

Ein Drittel der befragten Teilnehmer hat sich bereits gelegentlich mit dem Thema auseinander gesetzt. Das Diagramm zeigt, dass insgesamt mehr Personen an der Umfrage teilgenommen haben, die bereits öfters mit dem Thema in Berührung gekommen sind. Die Befürchtung, dass die unerfahrenen Benutzer nicht erreicht werden können, ist also eingetroffen. Die damit verbundenen Ergebnisse der Umfrage erlangen allerdings durch diese Tatsache einen noch größeren Stellenwert, da durch die bisherigen Fragestellungen eindeutig hervorgeht, dass der Schutz von Daten bzw. Reaktionen auf Probleme des Datenschutzes oder der Informationssicherheit nur sehr gering ausfallen. .

Welche der folgenden Aussagen machen eine Community im Bezug auf datenschutzrechtliche Aspekte deiner Meinung nach am effektivsten "sicher"? (max. 4, N = 635)

Auf Platz 1 der wichtigsten Faktoren, warum eine Community als „sicher“ erachtet wird, liegt die Aussage, dass Daten wirklich gelöscht werden. Dicht gefolgt von der Aussage: „*Daten werden nicht an Dritte weitergegeben.*“ Für die Hälfte der Teilnehmer ist eine Verschlüsselung von Daten sowie die Einhaltung von gesetzlichen Datenschutzbestimmungen ebenfalls wichtig.

Das heißt:
Wenn Betreiber sich nur an gesetzliche Datenschutzbestimmungen halten, ist dies nicht ausreichend. Betreiber müssen als „good will“ gewährleisten, dass Daten glaubhaft nicht an Dritte weitergegeben werden und auch tatsächlich gelöscht werden, wenn dies der Benutzer möchte.

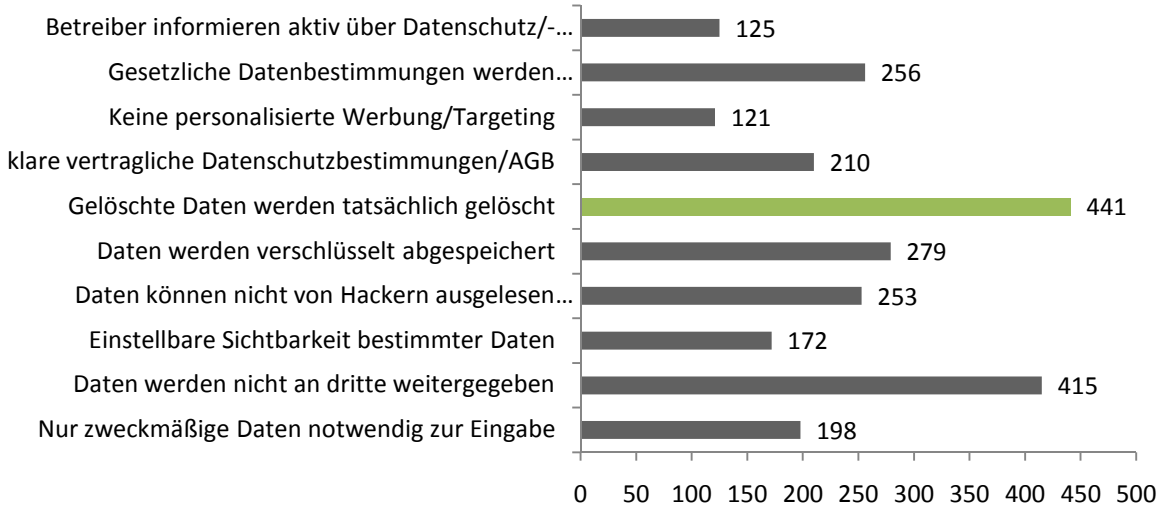

Diagramm 32: Welche der folgenden Aussagen machen eine Community im Bezug auf Datenschutz am effektivsten?

Nur für jeden fünften Teilnehmer ist die personalisierte Werbung ein Thema. Das Interesse an aktiven Informationen zu Datenschutz- und Informationssicherheitsthemen durch die Betreiber ist ebenfalls vergleichsweise gering. Datenschutz und Informationssicherheit ist daher ein passives Thema, das Benutzer voraussetzen. Demnach ist aktiver Datenschutz als USP für eine Plattform nicht geeignet (s. Kapitel 4.3.2).

Glaubst du, dass deine Daten in den Social Communities "sicher" sind? (Einfachauswahl, N = 641)

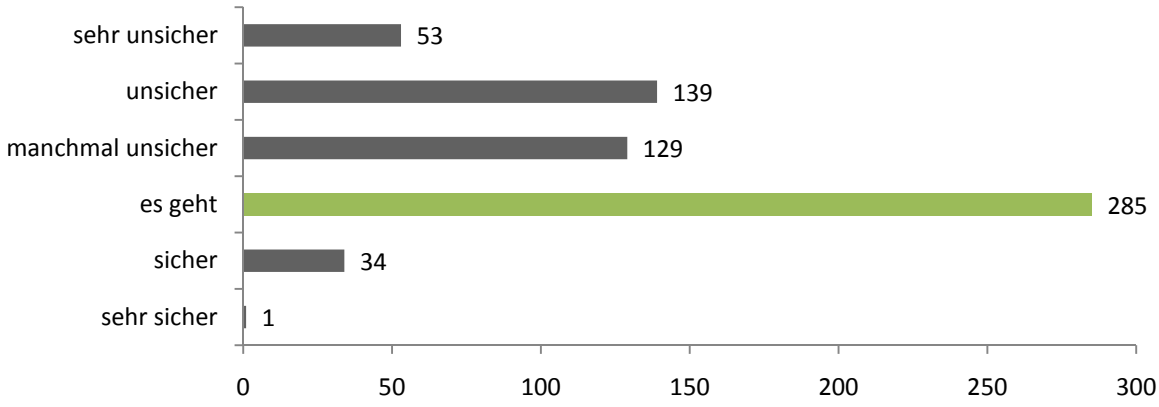

Diagramm 33: Glaubst du, dass deine Daten in den SC sicher sind?

44% der befragten Personen findet, dass die Daten nur durchschnittlich „sicher“ sind. Jeder zweite Teilnehmer der Umfrage gibt an, dass er das Gefühl hat, dass Daten zumindest manchmal unsicher sind. Lediglich eine Person im Umfeld hat den Glauben daran, dass Daten wirklich „sehr sicher“ in Social Communities aufgehoben sind. Die Wichtigkeit der Berichterstattung über Social Communities und die Schulung von Benutzern ist daher wichtig. Zusammengerechnet haben 50% der befragten Teilnehmer Probleme mit der Sicherheit ihrer Daten. Dieses Ergebnis ist äußerst beunruhigend und wird im weiteren Verlauf im Fazit näher behandelt.

4.2.4. Erweiterte Analyse

Nachdem die Fragestellungen einzeln betrachtet wurden, zeigt die folgende erweiterte Analyse statistische Zusammenhänge zwischen den einzelnen Fragestellungen. Im letzten Kapitel wurden sechs Thesen definiert, die mit Hilfe des sogenannten Chi-Quadrat-Tests beantwortet werden. Dabei werden jeweils zwei Fragen gegenübergestellt und die Antworten miteinander verglichen. Ist eine statistische Signifikanz vorhanden, dann darf die These als gültig betrachtet werden. Gibt es keine Signifikanz, muss die These verworfen werden. Zur Berechnung der Auswertung wurden die internen statistischen Berichte der Fragebogensoftware (vgl. 4.2) herangezogen. Tabelle 9 zeigt die Signifikanzwerte, die den statistischen Zusammenhang definieren.

Wert	Signifikanz
> 0,05	Nicht signifikant
< 0,05	Signifikant
< 0,01	Sehr signifikant
< 0,001	Höchst signifikant

Tabelle 9: Signifikanzskala

These 1:
Xing Benutzer sind ebenfalls auch privat in anderen Communities aktiv.

Fragestellung 1:
Bei welcher der folgenden Social Communities bist du regelmäßig aktiv?

Fragestellung 2:
Aus welchen Gründen nutzt du Social Communities?

Ergebnis:
$x^2 = 336,64$
$p = 0$ = Höchste Signifikanz

229 Teilnehmer der Umfrage geben an auf XING angemeldet zu sein und Communities sowohl privat als auch geschäftlich zu nutzen. ($p < 0$) Es besteht höchste Signifikanz. Interessant sind hierbei auch die weiteren Ergebnisse für XING Benutzer, die ebenfalls eine höchste Signifikanz zu der Antwort „*Zeitvertreib*“ ($p < 0,0001$) aufweisen. Die Antwort „*einfaches Kommunikationsmittel*“ ist sehr signifikant ($p < 0,0012$). 133 Teilnehmer, die auf studiVZ registriert sind, nutzen die Communities ebenfalls privat als auch geschäftlich. Auch hier besteht eine höchste Signifikanz ($p < 0,0001$).

Die These kann bestätigt werden.

Diskussion:
Der Zusammenhang zwischen XING und der Nutzung anderer privater Communities überrascht, da das Zielpublikum von XING durchaus älter ist als das der anderen Communities. Leider kann aufgrund der Fragestellungen nicht ermittelt werden, ob XING als Haupt-Community benutzt wird, oder selbst nur als Lückenfüller für andere Communities herrscht. Die Bestätigung der These zeigt jedoch, dass XING durch den Beitritt zu OpenSocial den richtigen Weg einschlägt. (vgl. Hüsing, 2008)

These 2:
Personen, die sich mit Datenschutz auskennen, veröffentlichen weniger Inhalte über sich selbst:

Fragestellung 1:
Wie genau hast du dich bereits mit dem Thema Datenschutz auseinander gesetzt?

Fragestellung 2:
Welchen Anteil der Profilfelder, bei einer Registrierung in einer Community füllst du aus?

Ergebnis:
$x^2 = 13,69$
$p = 0,7485$ (keine Signifikanz)

Die These muss verworfen werden.

Diskussion:
Durch die Verwerfung dieser These kristallisiert sich ein Hauptergebnis der Arbeit heraus. Obwohl Personen Bescheid wissen, füllen diese nicht signifikant mehr oder weniger Profilfelder bei der Registrierung einer Community aus. Der Autor, der lange Zeit mit einem Zusammenhang zwischen den beiden Fragen überzeugt war, wurde jedoch im Laufe der Arbeit durch vergleichbare Ergebnisse (vgl. Merschmann, 2006 und Govani & Pashley, 2005) konfrontiert. Daher ist auszugehen, dass die These tatsächlich verworfen werden muss. Das Bewusstsein für Datenschutz reicht also nicht aus, um die Datenflut zu minimieren.

These 3: Personen benutzen ebenfalls die gleiche E-Mail-Adresse, wenn diese das gleiche Passwort benutzen.

Fragestellung 1:
Gibst du bei Registrierungen in Social Communities immer das gleiche Passwort an?

Fragestellung 2:
Gibst du bei Registrierungen in Social Communities immer die gleiche E-Mail-Adresse an?

Ergebnis:
$x^2 = 50,8329$
$p = 0$ (höchste Signifikanz)

Höchst signifikant ist der Zusammenhang zwischen den beiden „Ja“ antworten. 159 Personen gaben an, dass sie sowohl eine gleiche E-Mail-Adresse als auch ein gleiches Passwort für mehrere Communities benützen würden. ($p < 0,0001$)

Ebenfalls sehr signifikant ist der Zusammenhang zwischen den beiden „Nein“ antworten. Das bedeutet, dass 230 Teilnehmer sowohl unterschiedliche Passwörter als auch E-Mail-Adressen verwenden. ($p < 0,0025$)

Die These kann bestätigt werden.

Diskussion:
Die Verwendung von gleicher E-Mail-Adresse und dem gleichen Passwort stellt ein Sicherheitsrisiko für den Benutzer dar. Sobald ein Angreifer Informationen über einen Benutzer erlangt hat, kann dieser auch auf anderen Communities Informationen finden. Sollte das verwendete Passwort ebenfalls zur Absicherung des E-Mail-Kontos benutzt werden, wäre ein kompletter „Identitätsraub“ möglich.

These 4:
Personen, die bereits durch frühere Informationen kompromittiert werden, veröffentlichen weniger Informationen über sich selbst

Fragestellung 1:
Wurden schon einmal (vielleicht Jahre später) Daten von dir im Internet gefunden, die dir unangenehm waren?

Fragestellung 2:
Welchen Anteil der Profilfelder, bei einer Registrierung in einer Community füllst du aus?

Ergebnis:
$x^2 = 1,834$
$p = 0,6073$ (keine Signifikanz)

Die These muss verworfen werden.

Diskussion:
Personen, die bereits durch ihre eigenen Daten kompromittiert wurden, veröffentlichen nicht weniger Informationen. Das heißt, es ist festzustellen, dass Personen aus ihren bisherigen Fehlern nicht lernen.

These 5:
Der Speicherort von Daten spielt für Personen, die sich mit Datenschutz auseinander setzen, eine Rolle.

Fragestellung 1:
Ist es für dich relevant, in welchem Land Daten, die du über dich veröffentlichst, gespeichert werden?
Fragestellung 2:
Wie genau hast du dich bereits mit dem Thema Datenschutz auseinander gesetzt?

Ergebnis:
$x^2 = 105,33$
$p = 0$ (höchste Signifikanz)

62 Teilnehmer haben angekreuzt, dass sie sich bereits sehr oft mit Datenschutz auseinander gesetzt haben und den Speicherort ihrer Daten für relevant empfinden ($p < 0,0006$).

Diskussion:
Vor allem Laien wissen nicht über die Bedeutung des Speicherorts Bescheid. Die Teilnahme an ausländischen Communities kann jedoch Gefahren beinhalten, die einem erst zu spät bewusst werden. Werden Daten außerhalb der EU, zum Beispiel in Amerika, gespeichert und kommt es zu einem Problem, gilt amerikanisches Datenschutzrecht. Durch die AGB sichern sich die Betreiber ebenfalls zu, dass lediglich amerikanisches Recht gilt. Käme es jedoch in einem europäischen Land zu Problemen, könnte man auf europäisches, bzw. österreichisches Recht zurückgreifen.

4.2.5. Gespräch mit dem CMO von studiVZ

Nicht nur während der laufenden Befragung stieß die durchgeführte Umfrage auf Interesse. Auch nach der Beendigung der Umfrage erhielt der Autor E-Mails bezüglich der Ergebnisse. Darunter fand sich auch eine E-Mail des CMO (Chief Marketing Officer) von studiVZ. Herr Cherdron hatte die Umfrage selbst leider verpasst, zeigte sich aber an den Ergebnissen

interessiert. Diesen Umstand wollte der Autor nutzen und Herrn Cherdron für ein Gespräch gewinnen und über die Fragestellungen, Antworten des CMO und die Ergebnisse der Auswertung zu diskutieren. Per E-Mail wurden ausgewählte Fragen, die in der Umfrage behandelt wurden noch einmal gestellt und von Herrn Cherdron beantwortet. Im Anschluss daran wurden die Antworten Cherdrons mit denen der Benutzer verglichen.

Nachfolgend sind die wichtigsten Aussagen des Gesprächs (vgl. Cherdron, 2008), das im Anhang beiliegt, zusammengefasst:

Fragestellung:
Hast du Bedenken, deine privaten Daten (wie Name, Adresse, E-Mail-Adresse, Telefonnummer, ...) in Social Communities zu veröffentlichen?

Bei dieser Frage konnte der CMO nicht explizit mit Ja oder Nein antworten. Selbst benutzt er lediglich Communities, bei denen er keine Bedenken hat. Generell sieht er jedoch keine Bedenken, wenn sein Name in Social Communities erscheint. Der Befragte weist darauf hin, dass es die meisten Nutzer ähnlich betrachten würden, da man nur mit der Angabe des Namens von alten Bekannten gefunden werden könne. Darüberhinaus sorgt der richtige Namen für zivilisierteren Umgang miteinander, da man sich nicht hinter einem Pseudonym verbergen könne. Angesprochen auf die Ergebnisse der Auswertung, in der 75% der Teilnehmer Bedenken haben, meint Cherdron, dass dies als Indiz für ein grundsätzliches Bewusstsein der Benutzer gegenüber Datenschutz aufgefasst werden kann:

> *„Für Social Communities im Allgemeinen kann ich nicht sprechen, höchstens für studiVZ. Und da kann ich dir versichern, dass die Bedenken der Nutzer keinesfalls ignoriert werden. […] Ein gewisses Maß an Grundbedenken gegen eine wahllose Veröffentlichung ist ja gerade die Voraussetzung dafür, dass die Nutzer diese Einstellungen[18] sinnvoll vornehmen."*

Natürlich stimmt der Autor der Aussage zu, dass ein gewisses Maß an Grundbedenken zum Schutz beiträgt, dennoch ist der sehr hohe Prozentsatz von 75% ein Zeichen dafür, dass Plattformen zukünftig mehr zum Datenschutz und der Informationssicherheit beitragen müssen.

Fragestellung:
Vertraust du darauf, dass dich die Betreiber der Communities über die Verwendung deiner Daten informieren?

Cherdron kann hierbei keine allgemeingültige Antwort geben, verweist jedoch darauf, dass das Vertrauen in studiVZ absolut gerechtfertigt ist und in Zukunft vermehrt Aufklärungsarbeit geleistet werden müsse.

Vergleicht man die Werte der durchgeführten Umfrage zum Vertrauen der Teilnehmer insgesamt und stellt diese mit dem Vertrauen gegenüber, dass Personen haben, die auf studiVZ registriert sind, erhält man ein überraschendes Ergebnis:

	Ja	Nein
Allgemeinschnitt	48%	51%
Schnitt der studiVZ Benutzer	51%	48%

Tabelle 10: Vertrauen der Benutzer in die Communities, unter Missachtung der Antwortmöglichkeit „Keine Angabe"

[18] Privatsphäre-Einstellungen, Anmerkung des Autors

Obwohl studiVZ vermehrt wegen Datenschutzproblemen in die Schlagzeilen geriet, haben Benutzer von studiVZ, die an der Umfrage teilnahmen, ein höheres Vertrauen in den Betreiber. Cherdron: „*Wir haben in dieser Hinsicht absolut nichts zu verbergen und sind überzeugt, dass wir faktisch viel besser dastehen als andere.*“ Diese Aussage dürfte nicht von der Hand zu weisen sein. Die genauen Hilfestellungen bezüglich der angebotenen Funktionen zur Privatsphäre, die in Kapitel 4.1.5 besprochen werden, könnten tatsächlich zu einem höheren Vertrauen gegenüber dem Betreiber beitragen.

Fragestellung:
Aus welchen Gründen würdest du dein Profil in Social Communities löschen?

Der Befragte gibt an, dass alle Gründe zu einer Löschung des Profils führen können. Nach der Bekanntgabe der Auswertung stellt er eine rhetorische Frage auf: *„Heißt dass, das immerhin 10% auch bei Datenmissbrauch bei ihrem SN bleiben würden und 30% inakzeptable AGBs akzeptieren würden?“* Der Gedankengang stellt eine spannende Frage in den Raum, die leider nicht eindeutig beantwortet werden. Da es sich bei der Beantwortung der Frage um eine Mehrfachauswahl handelte und Benutzer tatsächlich alle Gründe für eine Löschung anführen konnten, könnte dieser Umkehrschluss theoretisch gezogen werden.

Fragestellung:
Findest du es selbstverständlich, dass bei dem Löschen deines Profils alle Daten tatsächlich gelöscht werden?

Cherdron antwortet ganz klar mit „Ja“ und bekräftigt das die Löschung der Profildaten ein äußerst wichtiger Punkt für die meisten Nutzer darstellt. Angesprochen auf die Firmenpolitik von Facebook, die eine Löschung des Profils unmöglich macht, sagt Cherdron, dass diese Methode nicht dem Verständnis von studiVZ vom Umgang mit den Nutzerdaten entspreche. Das Verständnis studiVZs sieht jedoch lediglich die Löschung von Profildaten vor. Dies beinhält alle Daten des Profils, Fotoalben und Freundschaftsbeziehungen. Nachrichten, die an andere Personen verschickt wurden, oder auf Pinnwänden hinterlassen wurden „gehören“ jedoch den Empfängern, wie dies auch bei normalem E-Mail-Verkehr der Fall ist. Dennoch wird bei diesen Nachrichten der Name durch „Gelöschte Person“ ersetzt. Daten bleiben, im besten Falle, anonym erhalten. Dieses Vorgehen deckt sich mit allen anderen Betreibern, die im Testumfeld verglichen wurden.

Fragestellung:
Welche der folgenden Aussagen machen eine Community im Bezug auf Datenschutz rechtliche Aspekte deiner Meinung nach am effektivsten "sicher"? (max. 4)

Cherdron gibt folgende vier Antwortmöglichkeiten an, die laut ihm „unverzichtbar“ sind:

- Gesetzliche Datenbestimmungen werden eingehalten
- Gelöschte Daten werden tatsächlich gelöscht
- Daten können nicht von Hackern ausgelesen werden
- Daten werden nicht an Dritte weitergegeben.

Der CMO von studiVZ ist dabei sehr ähnlicher Meinung wie die Teilnehmer der durchgeführten Umfrage. Bis auf die Antwort „Daten werden verschlüsselt gespeichert“ wählt Cherdron die gleichen Antworten als wichtig und meint: „*Man muss nur mal die Gegenprobe machen und sich vorstellen, dass eine davon nicht erfüllt ist.*“

Die einleitenden Kapitel über die in der Arbeit verglichenen Communities zeigen, dass in der Vergangenheit oftmals Missstände in der Informationssicherheit sehr wohl zu Problemen durch bestehende Sicherheitslücken führten. Die Datenschutz rechtlichen Aspekte werden zwar von den Betreibern erkannt, jedoch nicht immer in angemessenem Rahmen behandelt.

Cherdron gibt zu, dass studiVZ in den letzten Jahren wegen (Sicherheits-)Problemen in die Medien kam, kann jedoch keine Zahlen darüber Preis geben, wie viel Budget/Arbeitszeit bei der studiVZ-Entwicklung in Datenschutz und Informationssicherheit investiert wird. Die Fragestellung, ob studiVZ mit dem vor wenigen Wochen eingeführten Applikationskern eine solide Basis geschaffen hat, um in Zukunft gegen Angriffe gefeit zu sein, bleibt offen. Die Beantwortung der nächsten Frage dürfte zumindest ein Indiz dafür sein, dass die Sicherheit gegenüber früher verbessert wurde.

Fragestellung:
Glaubst du, dass deine Daten in den Social Communities „sicher" sind?

Der Befragte sagt, dass er auf diese Frage allgemein mit „Nein" antworten müsste. Er ist sich allerdings sicher, dass seine Daten auf studiVZ „sicher" sind.

Abschließend wurde Cherdron über die Zukunft von Communities, im speziellen die von studiVZ, und dem Datenschutz innerhalb von sozialen Netzen befragt:

> *„Communities wird es auch in 10 Jahren noch geben. Wenn man das einmal kennt, ist es etwas völlig Natürliches und Elementares wie E-Mail. Was den Datenschutz angeht: Das ist eine grundsätzliche Frage im Internet, kein spezielles Problem von Communities. studiVZ hält sich an die deutschen Datenschutzbestimmungen, die deutlich strenger sind als die vieler anderer Länder. […] Technische Möglichkeiten (im Gegensatz zu dem aktuellen USP studiVZs, dass die frühe Erschließung des deutschen Markts darstellt, Anm. des Autors) sind eine Sache. Eine andere ist, ob man eine Minderheit von Technik- und spielbegeisterten Nutzern glücklich macht oder die große Mehrheit, der Übersichtlichkeit und intuitive Nutzung wichtiger ist als die 51. Variante, Freunde mit Schafen zu bewerfen. Ein wesentlicher Wert eines SN, der häufig unterschätzt wird, liegt in der Koordination möglichst vieler Nutzer in meinem Umfeld auf einfache, allgemein verständliche Kommunikationsstandards."*

Das Interesse seitens studiVZ an der durchgeführten Umfrage und den daraus erzielten Ergebnissen, sowie die sehr ausführlichen Antworten auf die Fragestellungen des Autors durch den CMO sind generell sehr positiv zu betrachten. Im Gegensatz zu den vielen negativen Schlagzeilen, die in der noch jungen Firmengeschichte durch die Medienlandschaft aufkamen, ist ein Bemühen zu erkennen, zukünftig Dinge sorgfältiger und überlegter zu planen. Als deutlicher Marktführer im deutschsprachigen Raum wird es auch zukünftig zu gezielten (Negativ-)Schlagzeilen kommen. Ob studiVZ zu empfehlen ist oder nicht kann die vorliegende Arbeit nicht restlos klären. Zumindest der Vergleich der AGB und Nutzungsbestimmungen zeigte, dass studiVZ den amerikanischen Communities klar vorzuziehen ist. Für alle (zukünftigen) Benutzer sei das Interview mit Professor Speck (s. Kapitel 4.3.1) über die Sicherheit von Benutzerdaten in Social Networks und die vom Autor aufgestellten Richtlinien zur Benutzung von Social Communities (s. Kapitel 5.4) zu empfehlen.

4.3. Experteninterview zu den Ergebnissen

Die Umfrage im deutschsprachigen Raum hat das Bild der Benutzer von Netzwerken aufgenommen. Um das Thema jedoch ganzheitlich betrachten zu können ist eine weit differenziertere Sichtweise erforderlich. Aus diesem Grund werden die Ergebnisse der Umfrage sowie der gesamten Arbeit abschließend mit drei Experten besprochen. Es handelt sich dabei um Martin Weigert, Professor Hendrik Speck sowie Mag. Gregor Ribarov. Die Interviews wurden sowohl per Skype als auch per E-Mail geführt. Der vorhandene E-Mail-Schriftverkehr liegt der Arbeit im Anhang bei. Die wichtigsten Aussagen und Antworten aus den drei Gesprächen werden nachfolgend zitiert und vom Autor kommentiert.

4.3.1. Interview mit Martin Weigert (Web2.0 Experte)

Martin Weigert ist Betreiber eines der bekanntesten Blogs zum Thema Web2.0 im deutschsprachigen Raum. Sein Blog rangiert aktuell auf Platz 21 der deutschen Blogcharts[19]. Die Webseite www.zweinull.cc war die erste von zahlreichen, die über die durchgeführte Umfrage des Autors berichtete. Weigert beschäftigt sich sehr detailiert mit der Szene und diskutiert die wichtigsten Ereignisse sowie aufstrebende Startup-Applikationen. Der Autor hat Herrn Weigert daher gebeten eine Reihe an Fragen aus Sicht des Web2.0 Experten zu beantworten:

Fragestellung 1:
In Ihren Blogbeiträgen analysieren Sie das Web2.0 Geschehen und scheuen auch nicht davor Kritikpunkte zu äußern. Alles in allem: Empfinden Sie das Social Web als positiv oder negativ?

> *„Ich empfinde das Web2.0 beziehungsweise Social Web auf jeden Fall als positiv. Es bietet mir die Möglichkeit das zu machen, was ich heute mache. Früher wollte ich ebenfalls Texte verfassen – es gab jedoch noch keine Möglichkeiten und Akzeptanz dafür. Jeder hätte sich gefragt: Wer ist dieser Mann? Warum macht er das? Ist er eine kleine Zeitung? Heutzutage ist dies anders. Es ist selbstverständlich, dass einzelne Personen Inhalte erstellen. Blogger werden ernst genommen."*

Der Autor ist der gleichen Meinung wie Weigert. Das Web2.0 hat die Medienlandschaft und die Nutzung des Internets nachhaltig verändert. Benutzer sind nicht mehr nur stille Endverbraucher von starren Inhalten, sondern kreieren gemeinsam viele neue Inhalte. Durch die Vernetzung mit anderen Personen werden die Nutzer langfristig reifer. Dennoch können die meisten mit der neu gewonnenen Macht noch nicht umgehen.

Fragestellung 2:
Fast keine der Web2.0 Applikationen schreibt aktuell schwarze Zahlen. Können das Web2.0 und damit eingeschlossen Social Communities langfristig Erfolg haben?

> *„Ich denke ja, denn nichts mehr ist heute Web1.0. In diesem Jahr wird sich das Web2.0 als allgegenwertige Plattform präsentieren. So gut wie keine Webseite kann heutzutage ohne Social Media Komponenten auskommen. Ich hoffe auf Umsatzsteigerungen und Gewinne durch Startups, da diese verschiedene Geschäftsmodelle verfolgen können. Das häufigste Modell der Applikationen ist die Werbefinanzierung. Es ist ganz klar erkennbar, dass Werbebudgets von Firmen, die früher in klassische Medien investiert haben, in Richtung Web schwenken. Zukünftig wird es keine werbetreibende Firma geben, die sich nicht im Web vermarktet. Ein zweites Geschäftsmodell stellen kostenpflichtige Dienste dar, die ich persönlich als sehr wichtig erachte, da Qualität im Netz momentan oftmals gratis angeboten wird. Zukünftig kann also davon ausgegangen werden, dass Anbieter mit kostenpflichtigen Mehrwertdiensten Umsätze erzielen können, wenn der Mehrwert für den Benutzer entsprechend gegeben ist. Als drittes Geschäftsmodell sehe ich das Shopping im Internet, egal ob von echten oder virtuellen Gütern wie Musik oder Filmen. Facebook zeigt vor, wie das virale Marketing in Social Communities genutzt werden kann, um Güter zu vermarkten. Benutzer müssen sich jedoch erst an diese neuen Formen von Werbung gewöhnen."*

Weigert prognostiziert Erfolg für Web2.0 Applikationen und Social Communities. Seiner Einschätzung nach gibt es noch mehr Geschäftsmodelle, als das reine Banner basierende. Vor

[19] Vgl. http://www.deutscheblogcharts.de/

allem kurzfristig haben kleine Anbieter jedoch keine andere Wahl als auf eben diese zu setzen. Kein Benutzer ist bereit für kostenpflichtige Inhalte in kleinen Applikationen zu zahlen; die aktuellen Bezahlformen sind ebenfalls noch zu intransparent und kompliziert, um das Bezahlen von geringen Beträgen zu ermöglichen (vgl. Weigert, 2008b). Andererseits gibt es noch keine standardisierten Schnittstellen, um Funktionen wie Facebook Beacon (s. Kapitel 4.1.1.2) auch in anderen Communities einzubinden. Wer bekommt jedoch Firmen wie Coca Cola oder McDonalds dazu, Kooperationen mit diesen Communities einzugehen? Sobald es Intermediäre wie im Falle von Google und dem Google Adsense Modell auch für ähnliche Funktionalitäten wie Facebooks Beacon gibt, kann sich diese Form des Geschäftsmodell auch in der breiten Masse der Applikationen durchsetzen.

Fragestellung 3:
Sie bloggen über das Web2.0 Geschehen unter Ihrem echten Namen. Gezielt, um die Person "Martin Weigert" im Internet bekannter zu machen? Was würden Sie Personen raten, die ebenfalls häufig im Netz interagieren? Pseudonym oder realer Name?

> *„Es ist tatsächlich ein positiver Nebeneffekt. Nach und nach erkennt man, dass man sich als „Marke“ etabliert. Es bringt viel. Es hat meine persönliche Entwicklung im Internet nachhaltig verändert und mir Türen geöffnet. Gleichzeitig erfordert die Bekanntgabe des Namens allerdings auch Vorsicht. Alles was ich schreibe, wird ewig im Netz vorhanden sein. Man darf daher keine Texte schreiben, die nachträglich gefährlich sein können. Man muss darauf achten, welche Dinge man über sich veröffentlicht. Ob eine Person ihren richtigen Namen verwenden soll, oder eher ein Pseudonym hängt davon ab: Will man Networking betreiben, sich selbst im Internet vermarkten und dadurch seine eigene Karriere vorantreiben, dann ist es sicherlich sinnvoll mit dem echten Namen aufzutreten. Sucht man allerdings Spaß, dann darf sollte man definitiv ein Pseudonym auswählen.“*

Der Experte unterscheidet ganz klar, ob er seinen richtigen Namen wählt oder nicht. Für ihn als erfolgreichen Blogautor ist es auf wichtig seinen eigenen Namen zu verwenden. Bezogen auf Social Communities ist die offene Frage: Aus welchem Grund verwende ich die Plattform? Will ich mich auf einer Business Community präsentieren um Jobangebote zu erhalten? Dann ist es sinnvoll den richtigen Namen anzugeben. Wozu dienen jedoch Plattformen wie StudiVZ, Facebook oder MySpace? Ist es wirklich notwendig richtige personenbezogene Daten einzugeben? Laut dem CMO von StudiVZ ja (s. Kapitel 4.2.5) – der Autor ist der Meinung, dass Benutzer selbst die Entscheidung treffen sollen dürfen.

Fragestellung 4:
Wie verändern sich Web2.0, Social Communities und der Datenschutz in den nächsten 10 Jahren?

> *„In Zukunft, egal ob in drei oder fünf Jahren, wird sich das Internet anders präsentieren. Es wird vielleicht nicht nur noch einzelne Seiten darstellen, sondern Dienste werden miteinander verschmelzen. Benutzer werden in der Lage sein wahllose Elemente miteinander zu verknüpfen. Wenn es weiterhin so läuft, wie bisher und Benutzer nur die guten Seiten des Web2.0 kennenlernen, dann werden sie weiterhin Dinge über sich Preis geben. Das Bewusstsein dafür wird sich entwickeln und das Thema Datenschutz verändern. Ich hoffe jedoch, dass es in Zukunft weniger Fallen, wie dies zum Beispiel vor kurzem bei dem Programm Adobe Photoshop Express[20] der Fall war, für die Benutzer geben wird. Solche Regelungen schaden dem Erfolg vom Web2.0. Speziell hoffe ich, dass die deutschen Communities (wirtschaftlich) erfolgreich bleiben und viele Personen miteinander verbinden. Am besten alle Personen. Social Networ-*

[20] Die Firma Adobe legte in den AGB fest, dass die Firma alle urheberlichen Rechte, die mittels Photoshop Express bearbeitet werden, erhält.

king macht nur dann Spaß, wenn man nach Personen sucht und diese auch findet. Zu ehemaligen Studienkollegen, die nur noch per E-Mail erreichbar sind habe ich nur noch wenig Kontakt. Der Kontakt innerhalb sozialer Netze erfolgt rasch und zwanglos. So gesehen hoffe ich, dass Social Networking ein Tool für alle wird.
Sicher ist, dass die sozialen Medien die gesamte Medienlandschaft extrem verändern werden. Bisher kennen die meisten nur Dienste wie YouTube oder Flickr. Aber ihnen ist nicht klar, dass Benutzer die Inhalte erstellen, dass es viele soziale Anwendungen gibt und das die Benutzer selbst das Medium *geworden sind."*

Social Communities werden zum Kommunikationsmittel der Zukunft. Bereits heute zeigen durchgeführte Studien diesen Trend (vgl. CSCM, 2008). Die klassische E-Mail-Kommunikation wird dennoch nicht ganz verschwinden. Zu groß ist die Zahl derjenigen, die nicht in sozialen Netzen registriert sind und dies auch zukünftig nicht sein werden. Dennoch: Hat man all seine Bekannten in einem Netzwerk gespeichert, ist die Kontaktaufnahme sehr einfach und rasch möglich. Ein Beispiel einer privaten Nachricht innerhalb eines sozialen Netzwerks aus dem Freundeskreis des Autors zeigt jedoch, wie die Erreichbarkeit von Freunden in sozialen Netzwerken ad absurdum geführt werden kann: „*Hallo S, ich hab dir gerade eine E-Mail geschrieben! Bis später.*" Müssen wir immer über die sozialen Netzwerke kommunizieren? Sind die vielen Informationen, die früher über Mailboxen verschickt wurden, in den Communities gut aufgehoben?

Fragestellung 5:
Die durchgeführte Umfrage zeigt, dass auch unter Personen, die sich mit dem Datenschutz beschäftigen, kein geändertes Verhalten im Umgang mit den persönlichen Daten erkennbar ist. Gibt es überhaupt eine Möglichkeit auf die Gefahren vom Social Web (und im speziellen Social Communities) hinzuweisen und wenn ja, wie?

„Es entsteht gerade ein völlig neues Bewusstsein dafür, welche Informationen man über sich Preis geben sollte und welche nicht. Die Benutzer müssen dies erst lernen und dahingehend „erzogen werden". Ich glaube, dass der Staat oder die Gesellschaft selbst die Verantwortung hat der nachwachsenden Generation ein Verständnis für Datenschutz beizubringen. Rein theoretisch müsste man daher bereits in der Schule ein Fach einführen, dass sich damit auseinandersetzt. Dennoch: Das Veröffentlichen von Daten ist nicht immer schlecht. Grundsätzlich muss festgestellt werden: Ob es gefährlich ist, jedem meine Hobbies zugänglich zu machen hängt nur davon ab, ob die Hobbies peinlich sind oder mir jemand etwas ankreiden kann. Der Benutzer ist verantwortlich für seinen Schutz. Ich bin geneigt zu sagen: Manchmal muss man negative Erfahrungen machen um aus Fehlern zu lernen. Diese Fehler können jedoch fatal enden, wenn sie die Karriere einer Person betreffen. Was passiert, wenn zum Beispiel Trinkbilder eine Person kompromittieren? Je mehr Personen solche Bilder veröffentlichen, desto mehr müssen wir umdenken. Wer bestimmt, ob die Preisgabe von Daten etwas Schlechtes ist? Sind Menschen, die ihre letzten Trinkbilder veröffentlichen, tatsächlich schlechter? Personalchefs argumentieren, dass sich Alkohol negativ auf die Karriere auswirken kann. Ist es jedoch nicht so, dass auch Personalchefs trinken? Ich bin daher der Meinung, dass eine Emanzipation der Elite und der Entscheider notwendig ist um die veröffentlichen Daten objektiver beurteilen zu können."

Der Experte spricht sich für das Lehren und Erziehen der Benutzer aus, fügt jedoch im Nachsatz amüsiert hinzu, dass er sich dennoch kein Fach „Datenschutz in Social Communities" an deutschen Schulen vorstellen könne. Die Frage, wie Personen erzogen werden können, bleibt daher offen. Im Gegensatz zu Weigert, der zwar „negative Erfahrungen" anspricht, diese aber nicht unbedingt für zwingend notwendig hält, ist der Autor der Meinung, dass Benutzer ihr Verhalten in Bezug auf Datenschutz in sozialen Netzen ohne der Häufung von negativen Erfahrungen mittelfristig nicht verändern werden. Definitiv interessant ist die

Problematik der Wertschätzung von Inhalten. Sich nur auf die veröffentlichten Inhalte einer Person zu beschränken, um diese zu bewerten, kann definitiv nicht der richtige Weg sein.

4.3.2. Interview mit Hendrik Speck (Social Network Experte)

Professor Hendrik Speck unterrichtet an der Fachhochschule Kaiserslautern und verfasste zahlreiche Publikationen und Interviews zum Thema Social Communities. Durch Medienberichte wurde der Autor auf Herrn Speck aufmerksam und bat ihn aus Sicht des Communities Experten folgende Fragestellungen zu beantworten:

Fragestellung 1:
Warum geben Benutzer Daten in Social Communities Preis?

> *„Während noch vor 10 Jahren die Daten und Kontakte gemeinsamer Schul- oder Berufszeiten unter dem gnädigen Mantel des Vergessens verschwanden, erlauben die omnipräsenten Medien mit ihren effizienten Information Retrieval Systemen, diese Verbindungen auch nach langer Zeit aufzuspüren, zu kontaktieren und aufrechtzuerhalten. Gleichzeitig lässt sich eine „latente Flirtisierung" beobachten - die Kontaktaufnahme zu potentiellen Partnern wird erleichtert und die Anzahl der Kontakte zum Flüchtigen und Bekannten steigt. Durch technische Verfahren wie Wortschatzanalyse, Klassifikation und Clustering von Inhalten lässt sich empirisch nachweisen, dass Social Communities vor allem zur Unterhaltung und Kontaktaufnahme genutzt werden. Dabei spielt der Faktor „Schadenfreude" eine nicht unwesentliche Rolle: Peinliche Fotos von anderen sieht man sich gerne an."*

Durch neue technische Möglichkeiten ist der kontinuierliche Kontakt zu Personen möglich geworden. Die Nutzungsszenarien sind dabei sehr ähnlich und wenig überraschend. Die Unterhaltung und Kontaktaufnahme ist die logische Weiterführung des passiven Konsums klassischer Medien wie dem Fernsehen.

Fragestellung 2:
Wie wird sich die Nutzung von sozialen Netzen entwickeln?

> *„Momentan lässt sich eine dramatische Verschiebung der mediendemografischen Nutzung kompletter Bevölkerungsgruppen beobachten: Die klassische Bastion des westlichen Wissens, das Printmedium, sieht seiner Auflösung entgegen, die Nutzung von Fernsehen und Radio nimmt ebenfalls ab beziehungsweise stagniert. Immer größere Anteile unseres Lebens finden in vernetzten Medien statt, dies schließt auch studiVZ und anderen Social Communities mit ein. Dabei ist davon auszugehen, dass die Verweildauer solcher sozialen Netzwerke, die bei einigen Benutzern bereits mehrere Stunden am Tag betragen kann, in naher Zukunft zumindest stabil bleiben wird. Obwohl laut der Analysefirma Gartner die Nutzung von sozialen Netzen bereits die Spitze des sogenannten „Hypecycle" erreicht hat, werden Social Communities zum täglichen Leben gehören und sich in der Medienlandschaft etablieren."*

Wie bereits Martin Weigert im vorherigen Interview prognostizierte, ist sich auch Speck sicher, dass Social Media Applikationen die Medienlandschaft nachhaltig verändern werden und klassische Medien verdrängt werden.

Fragestellung 3:
Wie werden sich Communities in Zukunft verändern? Was halten Sie von OpenSocial und DataPortability?

„Soziale Netzwerke befinden sich momentan in einem sehr frühen Reifestadium, welches an die Anfänge von Instant Messaging- und E-Mail-Diensten erinnert. Es handelt sich dabei um proprietäre Anwendungen, die keine Möglichkeit zur Extraktion von Daten durch den Benutzer bieten und in sich geschlossene Systeme darstellen. In naher Zukunft wird es sich bei sozialen Netzen jedoch um verteilte Systeme handeln, bei der die Kontrolle über die Daten zu deren Benutzern zurückkehrt und Systeme miteinander verschmelzen. Die von Google angeführte OpenSocial Initiative beschränkt sich leider auf die Sicht des Entwicklers und den Austausch von Daten. Sie bietet keine wesentlichen Verbesserungen für die Wahrnehmung der informationellen Selbstbestimmung durch den Benutzer, entsprechende Ansätze und Technologien sind von OpenSocial eher verschenkt worden. Die DataPortability Initiative geht hierbei einen Schritt weiter und könnte daher zukünftig eine Basis für die Vernetzung von sozialen Netzwerken darstellen."

Technische Spezifikationen zukünftiger Systeme werden bald verfügbar sein. In der Zwischenzeit sind sowohl OpenSocial als auch DataPortability lediglich geistige Konstrukte. Wie die Applikationen der Zukunft aussehen, die miteinander verschmelzen und proprietäre Hürden hinter sich lassen, ist aktuell noch nicht auszumalen. Hier werden noch viele Besprechungen und Entwürfe der beiwohnenden Parteien notwendig sein, bevor tatsächlich von einem Erfolg zu sprechen ist. Klar ist, dass beide Initiativen die Nutzung der Communities nachhaltig verändern werden.

Fragestellung 4:
Wird in Zukunft die rege Teilnahme der Benutzer an Social Web Diensten zu neuen Datenschutzmaßnahmen führen, oder ist die Privatsphäre der einzelnen Personen dadurch gefährdet?

„Diese Frage ist nicht einfach zu beantworten. Bei den Sozialen Netzwerken handelt es sich um neuartige Technologien, deren Auswirkungen und Graubereiche zum jetzigen Zeitpunkt weder gesellschaftlich noch juristisch komplett erfasst worden sind. Wir wissen, dass Menschen am ehesten aus Katastrophen und Fehlern lernen, es ist daher eine Frage der Zeit, bis entsprechende Aktionspotentiale auch innerhalb dieser Medien überschritten werden. Dabei gibt es bereits jetzt Missbrauchsszenarien und Risiken: Der ehemalige Hacker und heutige Blogger Kevin Poulsen beispielsweise identifizierte auf MySpace mehrere 10.000 Sexualstraftäter, die einen nicht unerhebliche Bedrohung für die jugendlichen Benutzern sozialer Netze darstellen. Momentan gibt es jedoch wenige Bestrebungen seitens der Provider, entsprechende Datenschutzmaßnahmen zu entwickeln. Durch die Entwicklung von dezentralen Netzen, die auf Verschlüsselungskomponenten wie Public/Private Key Verfahren und Mikroformaten basieren und dem Benutzer die Kontrolle der Daten erlauben, entsteht jedoch ein technologischer Druck auf die Anbieter, der zu einer Verbesserung der Privatsphäre der Nutzer führen könnte."

Professor Speck spricht, wie bereits Weigert zuvor, Katastrophen an, die die Nutzung nachhaltig verändern werden. Die Übereinstimmung der beiden Experten verdeutlicht die vertretene Meinung. Laufen Benutzer tatsächlich Gefahr, in den kommenden Monaten und Jahren durch zu wenig Schutz ihrer Daten in ein Fiasko zu laufen, oder ist es doch noch möglich die negativen Auswirkungen abzufangen? Diese Frage bleibt weiterhin zentrales Thema der Arbeit. Eine Antwort auf diese Antwort dürfte jedoch nur die Zukunft bringen.

Fragestellung 5:
Was halten Sie von der Diskussion über personalisierte Werbung in sozialen Netzen und den Geschäftsmodellen der Communities?

„Das Businessmodell von Social Communities ist sehr oft rein werbe- bzw. bannerbasiert. Hier stellt sich für mich ernsthaft die Frage nach der Langfristigkeit des Modells.

Verbunden mit steigenden Marktanteilen von alternativer Browsersysteme lassen sich enorme Steigerungsraten bei Adblocker-Programmen feststellen, die Werbebanner komplett unterdrücken. Gleichzeitig wird die Click-through-Rate entsprechender Werbebanner zunehmend geringer und oftmals lohnt sich die Werbung für die werbenden Firmen nicht mehr. Verbunden ist dies mit einer deutlichen Darstellung des Nutzerunwillens gegen jegliche Formen der Bespitzelung, dies schließt auch die sogenannte personalisierte beziehungsweise verhaltensbasierte Werbung mit ein. Auch Werbetreibende und Regulierungsbehörden haben deshalb ein großes Interesse an einer Änderung der Geschäftsmodelle von Social-Web-Diensten. Selbst Google hat vor wenigen Wochen von der schwierigen „Monetarisierung des sozialen Inventars" gesprochen und sieht die Verwertungsmöglichkeiten sämtlicher sozialer Netze äußerst unzufrieden stellend. Es ist daher anzunehmen, dass es in den nächsten Jahren zu einer Marktkonsolidierung kommen wird."

Der Befragte findet klare Worte: Das Geschäftsmodell ausschließlich auf Werbung zu fokussieren ist zwecklos. Die mediale Diskussion über die personalisierte Werbung klingt, nachdem man die Aussage von Professor Speck gelesen hat, übertrieben und veraltet. Sollten sich Adblocker tatsächlich rasch durchsetzen und die Anzeige von Werbung unterdrücken, wären viele Communities rasch übernahmefähig für größere Netze. Die Konsolidierung würde rasch fortschreiten. Die Vergangenheit zeigte jedoch bereits oft, dass sowohl Anbieter als auch Konsumenten rasch technische Antworten auf Hürden der jeweils anderen Parteien finden. Als Beispiel seien hier die Kopierschutzmaßnahmen erwähnt, die oftmals wenige Tage nach offiziellem Start überlistet werden können. Sollte sich also die Art, wie Werbebanner geschalten werden, grundlegend ändern, wären Adblocker zumindest kurzfristig besiegt. Klar ist jedoch, dass Werbung langfristig kein Geschäftsmodell sein kann, das Erfolg verspricht, außer die Werbung beruht auf dem Konzept des viralen Marketings. Datenschutzrechtlich sind diese Vorhaben mindestens gleich bedenklich, wie *klassische* personalisierte Werbung.

Fragestellung 6:
Sehen Sie einen Unterschied beim Datenschutz zwischen deutschen und amerikanischen Communities? Was halten Sie persönlich von kaioo?

„Die potentielle Gefahr des Missbrauchs ist bei amerikanischen im Gegensatz zu deutschen Anbietern deutlich höher, da diese nicht den strengen Datenschutzgesetzen Deutschlands unterliegen. Ich bedauere, dass in der Vergangenheit außer Kaioo keine der deutschen Plattformen Datenschutz als USP hervorgehoben hat. StudiVZ beispielsweise hat sich diesbezüglich sogar in entsprechenden Presseinterviews als klassischer Gegenkandidat geoutet, die Bereitwilligkeit der Plattform zur kommerziellen Ausbeutung der Nutzerprofile und der Weitergabe der Nutzerdaten unterstreicht leider das Gefahrenpotential. Kaioo ist zumindest als Diskussionsbeitrag alle mal eine Überlegung wert, da die Entwickler zumindest ansatzweise in die richtige Richtung gehen. Kaioo löst jedoch bestimmte Fragen, wie die Zurückgabe der Selbstbestimmung über Daten an die Nutzer, eine explizite Datenfreigabe durch den Nutzer und die Mitnahme von Daten, leider ebenfalls nicht."

Die geltenden Datenschutzrichtlinien in Europa sind wie bereits im theoretischen Teil (s. Kapitel 3.1.5) beschrieben deutlich strenger. Auch Professor Speck weist auf diesen Umstand hin. kaioo, das als sehr kleiner Kontrahent gegen die renommierteren Communities in dieser Arbeit verglichen wurde, ist für den Experten einen Diskussionsbeitrag wert. Der Vergleich zeigte bereits, dass die Applikation zwar solide entwickelt, bis auf das USP des Vereins nicht wirklich hervorstechen kann. Die AGB von kaioo sind im Vergleich zu studiVZ nicht wesentlich anders, und wichtige Funktionen wie die explizite Datenfreigabe fehlen auch in dieser Community. Die Betreiber werden langfristig Probleme bei der Konkurrenzfähigkeit bekommen, sollten die angebotenen Funktionen nicht deutlich erweitert werden.

Fragestellung 7:
Wie viele Social Communities benutzen sie selbst und glauben Sie, dass ihre Daten sicher sind?

> *„Ich bin bei jeder Menge Plattformen aus Forschungsinteresse angemeldet. Auf den Plattformen werden Sie jedoch keine Informationen finden, die nicht auch auf der entsprechenden Darstellung des Lehrkörpers meiner Fachhochschule enthalten sind. Für mich persönlich ist also die Frage, ob die Daten auf einer Plattform sicher sind, nicht primär relevant. Die generelle Frage sollte jedoch lauten: Wie viele und welche Dinge gebe ich über mich Preis? Welche Informationen kompromittieren mich? Dabei empfiehlt es sich, sich sehr, sehr genau zu überlegen, welche Informationen tatsächlich sozialen Netzwerken preisgegeben werden sollen. Die mehrfach dokumentierte Datenklau der Plattform StudiVZ beispielsweise schafft sicher kein Vertrauen in die Sicherheit meiner Daten gerade bei dieser Plattform."*

Professor Speck, antwortet auf die Frage, die bereits in der durchgeführten Umfrage an alle Benutzer gestellt werden, ausweichend, aber äußerst schlüssig und treffend. Laut ihm ist es nicht relevant, ob und welche Vorkehrungen Betreiber zum Datenschutz und der Informationssicherheit trifft, einzig relevant ist welche Daten ich über meiner Person veröffentliche. Aus diesem Grund stellt auch der zweite Experte den Benutzer in den Mittelpunkt des Datenschutzes.

4.3.3. Interview mit Gregor Ribarov (Rechtsexperte)

Herr Mag. Ribarov ist wissenschaftlicher Mitarbeiter am Institut für Österreichisches und Europäisches Öffentliches Recht an der Wirtschaftsuniversität Wien.

Nachdem bereits Experten auf dem Gebiet des Web und sozialer Netze zu Wort kamen, möchte der Autor ebenfalls die rechtliche Situation beleuchten und erfahren was ein Experte, der tagtäglich Rechtsthemen und daher auch mit Datenschutz konfrontiert ist, über Communities denken (vgl. RIBAROV, 2008).

Fragestellung 1:
Gelebter Datenschutz ist eine Kombination aus mehreren Parteien. Sowohl Betreiber, Gesetzgeber als auch Benutzer tragen dazu bei. Welche dieser Parteien ist für Sie am maßgeblichsten für die Wahrung des Datenschutzes verantwortlich?

> *„Das ist aus meiner Sicht grundsätzlich der "Betreiber". Er erhebt die Daten bzw. sammelt sie, um sie im Anschluss zu verarbeiten und gibt damit überhaupt erst den Anlass dafür, dass sich datenschutzrechtliche Fragen stellen. Der Gesetzgeber hat daher im DSG 2000 entsprechende Regelungen vorgesehen, die sowohl für Betreiber aus dem öffentlichen Bereich (zB die Bezirksverwaltungsbehörde, die das Melderegister führt) als auch für solche aus dem privaten Bereich (also etwa eine GmbH die eine "Social Community Plattform" im Internet betreibt) gleichermaßen gelten. […] Den Betreiber treffen darüber hinaus zahlreiche weiter Pflichten zur Wahrung des Informations-, Auskunfts-, Richtigstellungs-, Löschungs- und Widerspruchsrechts des Benutzers, die einer Verletzung des Rechts auf Datenschutz vorbeugen sollen."*

Im Gegensatz zu den beiden Web-Experten, die vor allem den Benutzer in den Mittelpunkt der Wahrung des Datenschutzes stellen, nimmt Ribarov hier eine konträre Position ein und spricht sich für die Betreiber der Plattformen aus, die gesetzlich verpflichtet sind, sich um den Datenschutz zu kümmern.

Fragestellung 2:
Was denken Sie können Behörden und die Politik dazu beitragen, um die Gefahr, die von sozialen Diensten im Internet (besonders durch Communities) ausgeht, zu minimieren?

- *„Regelmäßige Evaluierung der Datenschutzbestimmungen auf Anwendbarkeit und Effektivität*
- *Maßnahmen zur Schulung der „Awareness" für datenschutzrechtliche Probleme bei Benutzern und auch Betreibern von sozialen Diensten im Internet"*

Für Ribarov ist die laufende Evaluierung der Datenschutzbestimmungen maßgebend für eine Minimierung der Risiken. Darüberhinaus ist es ebenfalls wichtig die Benutzer von sozialen Diensten zu schulen und deren Bewusstsein für Datenschutz zu sensibilisieren. Die Auswertung der durchgeführten Umfrage zeigt hierbei, dass es zukünftig noch verstärkter zu einer Bewusstseinsbildung kommen muss, da das bisherige Wissen, das Personen über Datenschutz haben, zwar durchaus vorhanden ist, dennoch kein Umdenken bei den Benutzern hervorruft.

Fragestellung 3:
Stellt das Internet eine Grauzone dar, in der Daten und Informationen per Definition nicht sicher sein können, da die Anwendbarkeit von geltendem Recht für Laien schwer fällt?

„Nein, grundsätzlich gibt es für den Datenschutz ganz klare Regeln:

- *Für eine Datenverarbeitung deren Auftraggeber seinen Sitz innerhalb der EU hat, gilt das Herkunftslandprinzip. Das bedeutet es ist das Recht des Sitzstaates anzuwenden. Für den Fall dass es um ein Social Network handelt dessen Betreiber in Österreich sitzt, ist also sowohl für die Verarbeitung von personenbezogenen Daten österreichischer Mitglieder als auch französischer Mitglieder das österreichische DSG anzuwenden.*

- *Für eine Datenverarbeitung deren Auftraggeber seinen Sitz außerhalb der EU hat, gilt das Recht jenes Staates in dem die Datenverarbeitung stattfindet. Ein Social Network dessen Betreiber in den USA niedergelassen ist, hat daher für die Verarbeitung von personenbezogenen Daten seiner österreichischen Mitglieder auch österreichisches Datenschutzrecht, also die Vorschriften des DSG einzuhalten."*

Für den Rechtsexperten ist der Datenschutz klar geregelt. Während innerhalb der EU das Herkunftslandprinzip gilt, stellt sich das Bild für Betreiber außerhalb der EU anders dar. Diese müssen sich an die Rechtssprechungen desjenigen Landes halten, in denen die Datenverarbeitung stattfindet. Ein Umstand, der für einige Betreiber für enormen Aufwand führen könnte, da in Communities wie MySpace oder Facebook Benutzer aus aller Welt registriert sind. Die Auswertung der AGB dieser Communities verdeutlicht jedoch, dass diese das amerikanische Recht als ausschließlich geltendes Recht definieren. Diese Regelung widerspricht theoretisch dem österreichischen Datenschutz, bekräftigt der Experte. Dennoch ist zwischen der Theorie und der tatsächlichen Umsetzung des geltenden Rechts ein Unterschied.

Fragestellung 4:
"Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten…" (Datenschutzgesetz, Art. 1 § 1)

Sehen Sie dieses Gesetz in Social Communities, in denen Daten standardmäßig für jedermann zugänglich sind, für gefährdet bzw. missachtet?

> *„Ja. In Social Communities werden häufig personenbezogenen Dossiers erstellt bzw. Kommunikationsdaten erhoben, ohne dass eine entsprechende rechtskräftige Zustimmung des Betroffenen vorliegt und damit schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt werden. Da es meist nicht möglich ist tatsächlich selbst zu entscheiden, wer das in der Social Community erstellte Profil sehen und damit verbunden Informationen abrufen kann, besteht außerdem die Gefahr des Missbrauchs durch andere User. Accounts können überdies gehackt und gefälschte Profile erstellt werden. Es gibt außerdem Schwierigkeiten erstellte Dossiers, also einen Account zu löschen, was dem Recht auf Löschung von einmal erhobenen und verarbeiteten Daten widerspricht.“*

Der Vergleich der ausgewählten Plattformen (s. Kapitel 4.1) zeigt, dass sich alle Anbieter eine Zustimmung des Benutzers zur Erhebung von (personenbezogenen) Daten durch die AGB und Nutzungsbestimmungen sichern. Bei den amerikanischen Betreibern gelten diese Bestimmungen ebenfalls für nicht registrierte Benutzer – es ist davon auszugehen, dass ein Großteil dieser Gäste nicht über die Bestimmungen Bescheid wissen. Alle getesteten Anbieter haben Möglichkeiten zur Einstellung der Privatsphäre ihrer Benutzer vorgesehen. Dennoch herrscht ein großer Unterschied bei dem tatsächlichen Funktionsaufwand. Die Erfahrung des Autors zeigt, dass es vor allem in kleineren Communities, keine Möglichkeit zur Selbstbestimmung gibt und daher Daten für jeden Benutzer, Gast und möglichen Angreifer verfügbar sind.

Da Herr Ribarov angab, dass er in keiner Social Community Mitglied sei, jedoch unter seinem Namen ein Weblog betreibt, fragte der Autor nach dessen Beweggründen:

> *„Das größte Problem in Social Networks im Internet ist meines Erachtens, dass sich die Benützer selten darüber im Klaren sind, dass das was sie im vermeintlich "privaten" oder "halbprivaten" Umfeld tun, sich nicht weit entfernt von einer gewissen Öffentlichkeit abspielt. Obwohl ich mir den damit verbundenen Gefahren bewusst bin und die meisten Risiken durch überlegtes Vorgehen stark minimieren könnte, bietet bis dato kein Social Network für mich persönlich Vorteile, die die potentielle Gefahr einer Manipulation meiner Daten aufwiegen und mich zu einer Mitgliedschaft animieren würden. […] Den Blog, den ich mit Kollegen betreibe, habe ich bzw. haben wir selbst in der Hand, da ich/wir kontrolliere/n wer dort wann und wie postet, welche Kommentare zugelassen werden etc. Auch kann ich ihn jederzeit offline nehmen, bzw. alte Posts unwiderruflich löschen. Ich stelle mich also selbst dar und bin abgesehen von der Verwaltung der Url von keinem Dienstanbieter abhängig.“*

Alle angebotenen Funktionen und die Möglichkeit mit Personen über längere Zeiträume hinweg verbunden zu sein sind für Ribarov keine Vorteile, die potentielle Gefahren, die durch Social Communities ausgehen, aufwiegen würden. In Bezug auf die durchgeführte Umfrage, in der angemeldete Freunde, die angebotenen Funktionen und der Informationsgewinn als Top Gründe für eine Registrierung genannt wurden, müssen daher zusätzlich noch das Vertrauen in den Betreiber und dessen Umfeld vorhanden sein um auch skeptische Personen zu einer Registrierung zu bewegen, wie Ribarov weiter erklärt: „*Wenn so ein Service aber von einem bestimmten Betreiber angeboten würde, dem gegenüber ich ein entsprechendes Vertrauen habe, dann wäre dies eventuell anders*“.

Die Kontrolle der eigenen Daten, sowie die Möglichkeit diese jederzeit vollständig vom Netz nehmen zu können schafft eine Sicherheit für Betreiber von Blogs, die tendenziell natürlich richtig ist, vor allem jedoch durch Suchmaschinen oder Archivierungssoftware zu Nichte gemacht wird. Sobald Informationen im Netz publiziert wurden, ist eine gänzliche Löschung meist ausgeschlossen. Dennoch: Das Modell des Betriebs eines Blogs, bei dem der Autor

selbst Kontrolle über alle publizierten Daten innehält, könnte in Zukunft die Social Community Welt nachhaltig verändern. TechCrunch berichtet Anfang März 2008, dass die frei erhältliche Blogging-Software WordPress adaptiert wurde, um zukünftig auch als Social Networking Plattform (mit dem Namen BuddyPress) eingesetzt werden könne. (vgl. Schonfeld, 2008)

5. Fazit

5.1. Fazit zum Vergleich der Social Community Anbieter

Fünf, teils sehr unterschiedliche, Anbieter wurden auf den Datenschutz und die Informationssicherheit überprüft. Die Ergebnisse zeigten, dass viele Bemühungen der Betreiber sehr ähnlich sind. Zur Abwehr von automatisierten Angriffen, die bei allen Betreibern in den AGBs verboten sind, wurden, zumindest bei der Registrierung, CAPTCHAs installiert. Jede Community besitzt Privatsphäre-Einstellungen, die den Datenfluss persönlicher Profildaten einschränken soll. Die angebotenen Funktionen unterschieden sich in der Bedienung, der Standardeinstellungen und beinhalteten Möglichkeiten Daten zu schützen. XING bietet als einzige Plattform eine Einstellvariante auf Kontaktebene.

Durch welche Merkmale unterscheiden sich einzelne Communities in Bezug auf den gelebten Datenschutz und die Sicherheit innerhalb der Plattform?

Vor allem die Nutzungsbedingungen der verglichenen Plattformen unterschieden sich stark. Durchschnittsbenutzer wissen jedoch von den Klauseln dieser Nutzungsbedingungen nichts. Vor allem die Regelungen der zwei amerikanischen Anbieter (MySpace, Facebook) lassen deutschsprachige Datenschützer aufschreien. Sie beinhalten Regeln, die laut europäischem Datenschutzrecht keineswegs akzeptabel sind. Theorie und Rechtsdurchsetzung sind jedoch zwei getrennte Welten. In der Praxis wird es für deutschsprachige Benutzer unmöglich sein, gegen die AGB von MySpace oder Facebook anzukämpfen. Eine genaue Durchsicht der Regelungen hat einige besonders fragwürdige Regelungen zum Vorschein gebracht:

- Benutzer haben keine Möglichkeit der Löschung ihres Profils (Facebook)
- Betreiber dürfen AGB und Datenschutzbestimmungen jederzeit ändern, wobei die weitere Nutzung der Webseiten automatisch als Akzeptanz der Benutzer gewertet wird (Facebook, MySpace, eventuell kaioo).
- Auch nach Ableben eines Benutzers wird sein Profil unter entsprechendem Hinweis weitergeführt (Facebook)
- Betreiber können in Zeitungen, Blogs und sonstigen Medien Informationen über Benutzer sammeln, um dem Benutzer personalisierte Angebote bieten zu können (Facebook)

Die Recherche des Autors zeigte weiter, dass alle Netzwerke bis auf kaioo, das zum Zeitpunkt der Untersuchung noch relativ jung war, bereits Probleme in Bezug auf Datenschutz oder Informationssicherheit hatten.

Geschäftsmodell: Datenspeicherung
Sinnvolle Geschäftsmodelle für Social Communities bestehen aktuell noch nicht. Die Wirtschaftliche Betrachtung der Communities fällt daher ernüchternd aus. Alle großen Anbieter schreiben rote Zahlen. Wie Professor Speck erklärt, ist das Werbebanner-basierte Geschäftsmodell langfristig nicht rentabel. (s. Kapitel 4.3.2). Mittelfristig bleibt Communities nur die Speicherung der Nutzerdaten und die Hoffnung darauf von einem Investor aufgekauft zu werden. Betreiber werden daher keine Schutzmechanismen einsetzen, die dem Wert des Unternehmens schaden. Betreiber verfolgen die Maximierung der Datenbestände, um die sozialen Netze interessant für Geldgeber zu machen. Rein aus dieser Betrachtung ergibt sich der Schluss, dass sich Benutzer nicht auf die Betreiber zur Sicherung ihrer Daten verlassen dürfen.

5.2. Fazit zur durchgeführten Umfrage

Govani & Pashley (2005) hofften nach der Durchführung ihrer Umfrage zum Thema *Datenschutz auf Facebook* eine Reduktion der Benutzerinhalte bei Profilen von Umfrageteilnehmern um 25 bis 50 Prozent zu finden. Die Überprüfung dieser These ergab allerdings, dass Benutzer ihre Inhalte nur um einen deutlich niedrigen Prozentsatz reduziert hatten. Das Bewusstsein für Datenschutz konnte nicht nachhaltig gesteigert werden.

Sind Benutzer über die Gefahren der Bekanntgabe ihrer privaten Daten aufgeklärt?

Ein ähnliches Ergebnis zeigte auch die selbst durchgeführte Befragung. Das Ergebnis war, dass sich bereits viele Teilnehmer mit Datenschutz auseinander gesetzt haben. Umso interessanter sind die Ergebnisse, die ein „Datenschutz-faules" Bild der Teilnehmer skizzieren. Es waren **keine signifikanten Zusammenhänge** ersichtlich, die zeigen würden, dass

- Benutzer weniger Daten veröffentlichen, wenn sie sich mit Datenschutz auskennen
- Benutzer weniger Daten veröffentlichen, wenn sie bereits in der Vergangenheit durch Daten kompromittiert wurden

Die Auswertung zeigt weiter, dass 75% der befragten Teilnehmer angeben, dass sie Bedenken beim Veröffentlichen ihrer Daten haben. Fast jeder 2. vertraut nicht darauf, dass Betreiber von sozialen Netzwerken über die genaue Verwendung der Daten informieren. 50% der Teilnehmer geben an, dass Daten in Social Communities nicht sicher sind. Dennoch: Eine Signifikanz zwischen den Werten und einer Reduktion der eigenen Partizipation der Teilnehmer ist nicht feststellbar.

Dieses Phänomen bestätigt der schleswig-holsteinische Datenschutzbeauftragte Thilo Weichert in einem Interview mit Herrn Merschmann (2006). Er bestätigte, dass die Sensibilität der Benutzer für Datenschutz prinzipiell zugenommen hat, jedoch eine „*vollkommene Unbekümmertheit im Umgang mit der eigenen Privatsphäre*" herrscht. Er nennt dieses Phänomen eine „*individuelle Kapitulation vor dem Recht auf Privatheit.*"

Ein Gespräch mit dem CMO von studiVZ, Herrn Malte Cherdron, in dem die Ergebnisse bereits vorab besprochen wurden, ergab, dass dieser die Bedenken der Nutzer grundsätzlich für notwendig hält, damit soziale Netzwerke funktionieren können. Erst wenn diese Bedenken hätten, bzw. sich Gedanken über die Veröffentlichung ihrer Daten machen, würde Datenschutz funktionieren.

Die Fragestellung nach Gründen für die Abmeldung bei einer Social Community ergab, dass 90 Prozent der befragten Teilnehmer ihr Profil löschen würden, wenn Daten durch den Betreiber an Dritte weitergeleitet werden würden. Dieses Ergebnis ist verblüffend, da 10 Prozent weiterhin auf der Plattform registriert bleiben würden. Nach einer inakzeptablen AGB Änderung würden lediglich 70% das Profil löschen. Offen bleibt, wie viele Prozent der Teilnehmer ihre Profile kündigen würden, nachdem sie draufkommen, dass bereits jetzt viele Anbieter Daten an Dritte übermitteln und (amerikanische) AGBs bereits jetzt eine Menge an inakzeptablen Klauseln beinhalten.

5.3. Fazit zu den Experteninterviews

Die Experteninterviews zeigten die Notwendigkeit der Betrachtung des Themas Datenschutz aus verschiedenen Blickwinkeln. Die Interviewpartner lieferten wichtige Antworten und konnten Einblicke in die Unterschiede der Bedeutung des Datenschutzes geben.

Alle Experten verdeutlichten die Wichtigkeit der Sensibilisierung der Benutzer. Folgende Aussagen sind für zukünftige Betrachtungen des Themas von großer Bedeutung:

> *„Für mich persönlich ist also die Frage, ob die Daten auf einer Plattform sicher sind, nicht primär relevant. Die generelle Frage sollte jedoch lauten: Wie viele und welche Dinge gebe ich über mich Preis? Welche Informationen kompromittieren mich?“* (Speck)

> *„Wer bestimmt, ob die Preisgabe von Daten etwas Schlechtes ist? Sind Menschen, die ihre letzten Trinkbilder veröffentlichen, tatsächlich schlechter? Personalchefs argumentieren, dass sich Alkohol negativ auf die Karriere auswirken kann. Ist es jedoch nicht so, dass auch Personalchefs trinken? Ich bin daher der Meinung, dass eine Emanzipation der Elite und der Entscheider notwendig ist um die veröffentlichen Daten objektiver beurteilen zu können.“* (Weigert)

> *„Den Blog, den ich mit Kollegen betreibe, habe ich bzw. haben wir selbst in der Hand, da ich/wir kontrolliere/n wer dort wann und wie postet, welche Kommentare zugelassen werden etc. Auch kann ich ihn jederzeit offline nehmen, bzw. alte Posts unwiderruflich löschen.“* (Ribarov)

Professor Speck verweist darauf, dass die Sicherheit von sozialen Netzwerken nicht relevant sei, wenn man lediglich Informationen über sich veröffentliche, die auch auf andere Weise auffindbar seien. Veröffentlichen Benutzer keine Informationen, die sie kompromittieren können, gäbe es daher kein Problem mit dem Datenschutz. Weigert lenkt diesen Gedanken in eine etwas andere Richtung und fragt sich, warum die Veröffentlichung von Trinkbildern Personen tatsächlich kompromittiert, da schließlich eine Vielzahl an Personen, auch leitende Funktionäre, ähnliche Fotos von sich hätten. Eine Emanzipation in Bezug auf die veröffentlichten Daten ist also notwendig, um (negative) Daten objektiver betrachten zu können.

Herr Mag. Ribarov wählt einen anderen Ansatzpunkt für die Thematik: Behalte ich als Benutzer das Recht und die Möglichkeit, Daten über mich jederzeit selbst offline nehmen zu können, ist die Veröffentlichung von Daten weitaus ungefährlicher. Der dezentrale Betrieb von Datenbeständen ermöglicht es daher in Zukunft dem Benutzer, die Kontrolle über seine Daten zu erlangen.

Welche der involvierten Parteien bei der Veröffentlichung von Daten ist am maßgeblichsten für die Wahrung des Datenschutzes verantwortlich?

Die Experten sind sich über diese Fragestellung uneinig. Der Autor ist daher der Meinung, dass sowohl Gesetzgebung, Betreiber als auch Benutzer von Plattformen maßgeblichen Anteil an der Wahrung des Datenschutzes haben. Tendenziell ist jedoch feststellbar, dass der Benutzer durch die aktive Veröffentlichung seiner Daten am maßgeblichsten verantwortlich ist. Nutzer sind jedoch oftmals nicht bereit die Verantwortung für ihre Handlungen zu übernehmen.

Trägt das rasante Anwachsen der Social Communities in den letzten Jahren zur Entwicklung von neuen Datenschutzmaßnahmen bei oder gefährdet es den Datenschutz von Privatpersonen?

Hierzu kann keine Antwort getroffen werden. Die Entwicklung von Social Communities befindet sich aktuell noch in den Kinderschuhen. Entscheidende Änderungen an der Architektur von sozialen Netzwerken wie OpenSocial und DataPortability werden Netze nachhaltig verändern und für den Austausch von Daten öffnen. Aus heutiger Sicht kann nicht gesagt werden, inwieweit zukünftig Betreiber Mechanismen bereitstellen werden, die die Kontrolle der Daten an den Benutzer zurückgibt. Aktuell stellen die Communities Insellösungen dar, die klassische „Datensenken“ bereitstellen. Informationen werden proprietär gespeichert. Der

Datenschutz von Benutzern hängt daher von den Datenschutz- und Informationssicherheitsmechanismen der Betreiber ab. Die angebotenen Privatsphäre-Einstellungen helfen um den Informationsfluss unter den Benutzern oberfläch zu steuern, können jedoch nicht mit den tatsächlich benötigten Funktionsumfang mithalten. Hier ist anzumerken, dass die aktuellen Einstellungen für Durchschnittsbenutzer zu komplex sind und neue Datenschutzmaßnahmen nur dann erfolgreich sein können, wenn diese für den Benutzer leicht verständlich sind. Die Simplizität und die intuitive Bedienung der Mechanismen sind für deren Erfolg maßgebend.

5.4. Richtlinien für Benutzer sozialer Dienste

Benutzer wollen Social Communities nutzen und aktiv partizipieren. Die vielen Studien, die in der vorliegenden Arbeit präsentiert wurden zeigen deutlich, dass Networking und Selbstdarstellung im Internet boomen. Benutzer, aufgrund der offen gelegten Datenschutzprobleme, von der Verwendung der Dienste abzuhalten erscheint daher unmöglich und würde das Problem nicht lösen. Darüberhinaus gibt es natürlich auch Gründe, die für eine Nutzung der Dienste sprechen. Sinnvoll eingesetzt, können die virtuellen Netzwerke eine Ergänzung für das Kontaktmanagement darstellen. Daher versucht der Autor Vorschläge zu einer sichereren Nutzung von sozialen Netzen aufzustellen. Ein Risiko der Teilnahme soll damit minimiert werden und Benutzer nachhaltig für das Thema Datenschutz sensibilisiert werden. Als Grundlage der Empfehlungen wurde das Enisa Position Paper No.1 zum Thema „*Security Issues and Recommendations for Online Social Networks*“, das Ende des Jahres 2007 durch die Europäische Union veröffentlicht wurde, herangezogen. (vgl. Hogben, 2007) Die präsentierten Regeln sind

Richtlinien vor der Registrierung in Social Communities
Bevor sich Benutzer in Social Communities oder sonstigen Web2.0-Diensten registrieren, sollten folgende Schritte überlegt und Erwägung gezogen werden:

Besteht die Möglichkeit für eine Vorab-Ansicht der Plattform?
Bereits angemeldete Freunde stellen einen Hauptgrund für Benutzer für eine Registrierung dar. Bevor man sich selbst mit seinen eigenen Daten (und Namen) auf einer Plattform registriert, kann ein Freund gebeten werden, die Community herzuzeigen. Benutzer sollten aktiv über die Vorteile einer Mitgliedschaft bei einer bestimmten Community mit ihren Freunden sprechen und ebenfalls Suchmaschinen zu dem Image des Betreibers befragen.

Sollte keine Möglichkeit bestehen, dass die Plattform getestet werden kann, ist die Registrierung mit falschen Angaben eine Möglichkeit um einen Blick auf die Community werfen zu können. So kann bereits vorab getestet werden, ob die Plattform den Wünschen entspricht und ob man sich problemlos abmelden kann.

AGB und Datenschutzbestimmungen sollten ernst genommen werden.
Die langen, oftmals sehr rechtlich klingenden Texte laden nicht zum Lesen ein. Dennoch sollten sie zumindest überflogen werden, wie der durchgeführte Vergleich der Communities und der Regelungen zeigte. Vor allem folgende Klauseln sollten betrachtet werden, bevor man sich registriert:

- Welche meiner Daten werden (permanent) gespeichert?
- Was darf der Betreiber mit den von mir veröffentlichten Daten (wie lange) unternehmen?
- In welchem Land werden die Daten gespeichert?
- Welches nationale Recht ist im Streitfall anwendbar?
- Ist eine Löschung des Profils möglich?
- Muss der Betreiber Änderungen an den AGB vorab bekanntgeben?

Richtlinien bei der Registrierung in Social Communities
Bei der Registrierung selbst sollten nur die notwendigen Profilfelder ausgefüllt werden, vor allem wenn noch kein Test vorab durchgeführt wurde, ob die Plattform den Wünschen entspricht. Erst bei Bedarf sollten weitere Profilfelder ergänzt werden.

Um Methoden wie dem „*Integrated Behavioral Targeting*" vorzubeugen, bei dem Benutzerprofile über die Grenzen von Plattformen hinweg gebildet werden (vgl. Grauel, 2006), macht es Sinn, unterschiedliche E-Mail-Adressen, sowie ebenfalls unterschiedliche Fotos (vgl. Gross & Acquisti, 2005) bei den Registrierungen zu verwenden. Eine Nachverfolgung der Benutzeraktivitäten über die Plattformgrenzen hinweg ist dadurch nur noch erschwert möglich. Sollte dem Benutzer nur eine E-Mail-Adresse zur Verfügung stehen, kann die Verwendung eines Anbieters für temporär erstellte E-Mail-Adressen empfohlen werden. Bekannte Dienste wie 10minutemail.com oder mailinator.com werden jedoch bereits von Communities wie Facebook geblockt.

Vor allem wenn bei der Registrierung in einer Social Community eine Adresse benutzt wird, die schon bei anderen Diensten verwendet wird, sollte darauf geachtet werden, dass nicht das gleiche Passwort verwendet wird. Dieses sollte sich auch auf jeden Fall zu dem für die E-Mail-Adresse selbst unterscheiden. Passwörter sollten im Idealfall mindestens 6 Zeichen lang sein und Sonderzeichen beinhalten. Sollte sich ein Hacker Zugriff auf Daten eines Benutzers verschaffen, der idente Passwörter und E-Mail-Adressen auch auf anderen Seiten benutzt, wäre dieser in der Lage auch an die Daten der anderen Plattformen zu kommen. Die Mindestlänge von Passwörtern ist ratsam, da ein so genannter *Brute-Force-Angriff* (alle möglichen Kombinationen werden automatisiert ausprobiert) bei einem komplexen Passwort weitaus länger dauern würde. Während ein Angriff auf ein Passwort, dass nur 1 Zeichen lang ist maximal 36 Möglichkeiten[21] überprüfen müsste, benötigt der Angriff auf ein Passwort mit der Länge von 6 Zeichen unter Berücksichtigung von 10 möglichen Sonderzeichen bereits 9.474.296.896 Versuche.

Richtlinien während der Mitgliedschaft in Social Communities
Ist man bereits in einem Netzwerk registriert, können ebenfalls Schritte befolgt werden, um den Selbstschutz zu erhöhen:

Um Phishing-Angriffen vorzubeugen, sollte die Adresse der Social Community immer nur mit der Hand eingegeben werden. Unterstützt die Plattform den Zugriff über HTTPS, sollte dieser auf jeden Fall genutzt werden. Die (Login-)Daten werden bei dieser Form der Übertragung ausschließlich verschlüsselt übermittelt und können nicht mehr im Klartext mitgeschnitten werden. Moderne Browser zeigen die Gültigkeit eines SSL-Zertifikats in der Adressleiste an, dass die Authentizität des Kommunikationspartners garantiert (vgl. Poguntke & Balzert, 2006, S. 55). Durch die immer größer werdende Verbreitung von WLAN-Netzen ist der Einsatz einer Verschlüsselung zwingend notwendig, da sonst bereits mit leichten Mitteln die Passwörter von Benutzern ausgelesen werden können. Vor allem in Firmen oder Universitäten, in denen oftmals drahtlos Internet gesurft wird, sollten Daten immer nur über HTTPS übertragen werden.

Angebotene Privatsphäre-Einstellungen sollten verwendet und auf die eigenen Bedürfnisse angepasst werden. Die Standardeinstellungen der Betreiber erlauben in der Regel oftmals zu viele öffentliche Daten. Persönliche Informationen sollten immer dahingehend eingeschränkt werden, dass nur „Freunde" Zugriff darauf haben. Profilfelder wie Vorlieben, politische Gesinnung oder die Konto-Daten von anderen Diensten (Instant Messaging, weiteren Web2.0-Diensten) sollten gar nicht ausgefüllt werden. Bei Bedarf können diese Informationen über private Nachrichten mitgeteilt werden. Das Ausfüllen der Profilfelder mit vorgefertigten Antwortmöglichkeiten erlaubt es Betreibern statistische Informationen über ihre Benutzer zu er-

[21] 26 verschiedene Buchstaben und 10 verschiedene Zahlen

langen, die in keinster Weise für den Betrieb der Dienste notwendig sind. Angreifer und Werbetreibende sind die einzigen Parteien, die sich über die gespeicherten Informationen freuen können.

Fotos, die den Benutzer selbst oder dessen Freunde in peinlichen Situationen zeigen, haben in Social Communities nichts verloren. Zu hoch ist die Gefahr, dass die Fotos in falsche Hände geraten können oder Jahre später für große Probleme sorgen können. Es sollten daher weder Personen auf Bildern verlinkt werden, noch sollte man sich selbst, ohne Zustimmung, auf Fotos verlinken lassen. Viele Communities bieten hierzu Funktionen, um diese Möglichkeit zu unterdrücken.

Verfasst man private Nachrichten oder schreibt kurze Einträge auf den virtuellen Pinnwänden von Freunden sollte darauf geachtet werden, dass in den Nachrichten nicht der eigene Name vorkommt. Nachrichten, die zumeist bei einer Kündigung der Mitgliedschaft nicht gelöscht werden, werden durch den Betreiber zwar anonymisiert. Sobald der eigene Name jedoch im Nachrichtentext vorkommt, sind diese immer noch eindeutig zuordenbar.

Richtlinien bei der Löschung von Profilen in Social Communities
Wenn man die Community nicht mehr aktiv benutzt, sollte das Profil unbedingt gelöscht werden, sofern dies möglich ist. Besteht in Zukunft dennoch wieder ein Interesse an einer Rückkehr zu der Plattform, können die Daten erneut eingetragen werden. Bevor das Konto vollständig gelöscht wird, sollten händisch Nachrichten und Gruppenzugehörigkeiten gelöscht werden. Nachrichten in Foren, falls diese auffindbar sind und durch den Benutzer gelöscht/verändert werden können, sollten ebenfalls nicht vergessen werden.

Sollte kein Löschen des Profils möglich sein, empfiehlt sich darauf zu achten, dass alle Daten und Fotos, bevor man das Konto „deaktiviert“ oder einfach nicht mehr verwendet, gelöscht und sofern notwendig, durch Fehlinformationen überschrieben werden.

Generell gilt:
In vielen Internetquellen findet man den nicht ganz ernst gemeinten Hinweis auf das Programm „brain.exe“ (vgl. Marx, 2008). Im Umgang mit den Gefahren ist der Einsatz des „*eigenen Gehirns*“ (vgl. Hausverstand) ratsam. Gemeint ist: Der Benutzer muss selbst überlegen, ob Informationen und Aktionen „richtig“ sind. Das Unterscheiden zwischen richtigen und falschen Informationen ist jedoch vor allem für Neulinge schwer. Als Faustregel bei der Benutzung von Social Communities gilt: *Dinge, die man im wahren Leben nicht macht, sollte man im virtuellen Leben ebenfalls nicht machen.*

6. Diskussion

Drei Thesen, die von Jones & Soltren (2005) aufgestellt wurden, führten den Autor zur Behandlung des Themas:

- *Benutzer geben im Internet zu viel über sich Preis,*
- *Betreiber unternehmen zu wenige Schritte um die Daten ihrer Benutzer zu schützen,*
- *Interessierte Personen suchen gezielt in Communities nach Informationen über Benutzer in Social Communities*

Alle drei Thesen konnten durch die durchgeführten Arbeiten des Autors bestätigt werden. Die Arbeit liefert daher grundlegende Informationen über die Nutzung von Social Communities im deutschsprachigen Raum. Die Erkenntnisse sind wichtig, weil seit den letzten Monaten verstärkt über Themen wie Datenschutz und Social Communities berichtet wird. Probleme treten definitiv auf und sind zukünftig auch nicht zu verhindern. Die Berichterstattung ist leider oftmals sehr einseitig. Vor allem der Vergleich der Anbieter zeigte, dass die AGB von studiVZ im internationalen Vergleich eher harmlos sind. Was tatsächlich mit den Daten der Benutzer innerhalb der Communities sei hier ausgenommen.

Das Fazit wiederholt, was Experten bereits in den Unterkapiteln erwähnten: Erst wenn es zu Katastrophen oder Situationen kommt, in denen Benutzer die Gefahr ihrer veröffentlichten Daten erkennen, werden sie ihre Nutzungsgewohnheiten ändern. Die Diskussion zeigt daher, dass bereits jetzt viele Personen mit den Problemen ihrer veröffentlichten Daten zu kämpfen haben. Die vorherrschende Meinung, dass die eigenen Daten keine Relevanz für außenstehende Personen hätten kann dadurch schlagkräftig widerlegt werden.

Karrierekiller Internet
Daten, die heute im Internet publiziert werden, können durch die Trägheit der Benutzer bei der Abmeldung von Diensten, bzw. der oftmaligen Speicherung von Informationen in Suchmaschinen und Webarchiven über Jahre im Internet gespeichert werden. Auch wenn Benutzer heute noch nicht über die Folgen des Publizierens nachdenken, Jobscouts tun dies sehr wohl. Eine Befragung der Wirtschaftswoche und des Verbands Deutscher Unternehmensberater zeigt, dass bereits 28 Prozent das Internet und Social Communities zur Sammlung von Informationen über Bewerber nutzen. 26 Prozent der befragten Personalexperten gaben an, dass Kandidaten aufgrund der gefundenen Daten nicht weiter berücksichtigt wurden. (vgl. Beeger, 2007)

Die scheinbare Privatsphäre in sozialen Netzwerken trügt ebenfalls. Am 6. März 2008 wurden neun Angestellte eines deutschen Hotels entlassen. Grund: Auf studiVZ wurden in einer Gruppe Drohungen gegen ein Hotel und dessen Besitzer veröffentlicht. Dieser hat die Mitglieder angezeigt, weil sie Anschläge auf das Haus planten. (vgl. Holzschuh & Erler, 2008)

Gefahren der Teilnahme
In einigen wenigen Fällen stellt die Teilnahme in Communities noch weit höhere Risiken dar, als einen Arbeitsplatz nicht zu bekommen, bzw. zu verlieren. Vor kurzem wurden Nachrichten von Anhängern der Terror-Organisation Hisbollah auf Facebook entdeckt, die anderen Benutzer die Nachricht „*Ich bin Hisbollah und ich werde dich und deine ganze Familie töten – das verspreche ich.*“ schickten. Doch die Social Communities werden ebenfalls zur Rekrutierung von neuen Mitgliedern genutzt. (vgl. derStandard, 2008d). Einer ganz anderen Bedrohung der Teilnahme fiel eine saudi-arabische Frau zum Opfer. Sie wurde von ihrem Vater getötet, weil dieser sie beim Chatten mit einem Mann auf Facebook erwischte. Social Communities sind aus vielen Gründen in islamischen Ländern verboten - dennoch registrieren sich Personen, um Kontakte außerhalb der Familien zu finden. (vgl. McElroy, 2008)

Selbstschutz und Bewusstsein

Die theoretischen Grundlagen haben viele Definitionen von Datenschutz gezeigt. Einen Grundsatz, den Fischer-Hübner (2001, S. 11) als wichtig erachtet, scheint in Social Communities definitiv nicht möglich:

> *"[…] information systems should guarantee, if possible, that users can act anonymously. The best design strategy to enforce this requirement is the avoidance or (at least) minimization of personal data. […]" (Fischer-Hübner, 2001, S. 11)*

Selbst wenn Communities nicht mit dem richtigen Namen genützt werden, so sind auch Pseudonyme oder Phantasienamen niemals gänzlich anonym. Die Nachverfolgung der Nutzer ist über E-Mail-Adresse, Name, Foto, oder technischen Mitteln (IP-Adresse, Cookie, …) immer möglich. Datenschutz in sozialen Netzwerken ist daher ein unerreichbares Paradigma. Die Reduktion der Daten, die durch Fischer-Hübner angesprochen wird, erfolgt am besten durch den Benutzer selbst. Daten, die nicht im Internet publiziert werden, werden immer die sichersten Daten bleiben. Der Autor ist daher im Gegensatz zu Experten, die Betreiber und die Gesetzgebung am maßgeblichsten für den Erfolg von Datenschutz erachten, der Meinung, dass ohne das Bewusstsein für Datenschutz durch die Benutzer selbst kein Schutz existieren kann.

Alle vorliegenden Quellen und die selbst durchgeführte Umfrage verdeutlichen: Benutzer wissen Bescheid. Sie können erahnen, dass sie selbst für den Schutz ihrer Daten verantwortlich sein könnten. Dennoch spielt die eigene Privatsphäre eine untergeordnete Rolle, weil die Gefahren des Internets noch nicht verstanden werden. Der Autor hat daher mit der vorliegenden Arbeit versucht diese zu verdeutlichen. Die Arbeit endet daher noch einmal mit einem Zitat von Sir Tim Berners-Lee, das Benutzer sozialer Systeme zum Nachdenken anregen soll:

> *„Beachte, dass Alles was man im Netz schreibt von jener Person gelesen werden wird, bei der du dich um einen Job bewirbst. Beachte außerdem, dass dies Alles nicht nur von deinen Eltern, sondern auch von deinen Großeltern und Großenkeln gelesen werden wird."* (derStandard, 2008b)

Privatsphäre ist ein Luxus, der auch noch nach der Benutzung von Social Communities, existieren sollte.

7. Ausblick

In den Anfängen des neuen Jahrhunderts, die von Bill Gates als die digitale Dekade (vgl. Dirscherl, 2001) bezeichnet wurden, stehen Internetbenutzer vor einer neuen Ära. Wir sind heute die erste Generation, die soziale Netze im Web nutzen. Erstmals ist es für die Masse der Benutzer möglich im Internet zu partizipieren und Freunde online am Leben teilhaben zu lassen. Wir publizieren unser Leben gerne in sozialen Netzwerken, weil wir vom Netzwerk auch Informationen zurückbekommen. Wer hat sich vor kurzem aktualisiert? Wer kennt nun wen? Was macht Benutzer X gerade? Während man sich für die Beantwortung dieser Fragen vor 20 Jahren noch persönlich mit den einzelnen Personen treffen musste, revolutionierte vor 10 Jahren das Handy diesen Prozess. Freunde waren rund um die Uhr erreichbar; ein simpler Anruf genügte und man war am neuesten Stand. Heutzutage hat sich das Blatt jedoch gänzlich verändert. Information ist plötzlich keine Holschuld mehr. Sie wird uns in Social Communities am Servierteller präsentiert. Wir erfahren automatisch über alle Neuigkeiten von unseren Bekannten, wenn diese im gleichen Netzwerk registriert sind. Ob es uns interessiert oder nicht. *Information ist eine Serviceleistung geworden*.

Die erste Generation bei etwas zu sein, ist jedoch auch immer mit gewissen Problemen behaftet. Der „*gesunde Umgang*“ mit dem neuen Medium fehlt. Niemand konnte am Anfang des Web2.0 Booms sagen, wohin sich das soziale Web entwickelt. Welche Themen unbeachtet blieben. Aus heutiger Sicht kann man jedoch sagen, dass Datenschutz definitiv ein Thema ist, worüber zu wenig gesprochen und *gelernt* wurde. Eine Aufklärung über die Folgen von zu wenig Selbstschutz, Informationssicherheit und Datenschutz fehlt.

Das Publizieren von Daten geht dabei weiter. Je mehr Daten im Internet und vor allem in sozialen Netzen gefunden werden kann, desto größer wird der Markt mit den Daten. Zeitschriften, die ihre Informationen über plötzlich relevante Menschen in Social Communities finden, Arbeitgeber, die sich über ihre (zukünftigen) Mitarbeiter erkundigen und auf Grund ihrer Äußerungen im Internet diese kündigen oder erst gar nicht anstellen. Wer das reichhaltige Pool an Informationen nicht nutzt, der ist selbst schuld. Der Trend des Publizierens wird deswegen so lange steigen, bis sich Missbrauchsfälle häufen. Benutzer werden Falschinformationen publizieren. Eigenschaften, Geschichten, Erlebnisse werden aufgebessert, um sich selbst in ein besseres Licht für den zukünftigen Arbeitgeber zu rücken. Vereinzelt werden Personen erkennen, dass weniger zu publizieren oftmals mehr ist. Ein Zeitalter der Ungewissheit bricht an: Kann man den verfügbaren Informationen vertrauen? Die Netzwerke werden ob der Ungewissheit kleiner. Der Boom ist vorbei. Trotzdem bleiben die Daten im Internet gespeichert. Erst einige Generationen später werden diese uninteressant. Lange werden die Informationen über die erste Generation als Mahnmal dienen und dem Datenschutzunterricht kommender Generationen als Negativbeispiel dienen.

Die zweite und dritte Generation von Social Community Benutzern wird ein gänzlich anderes Nutzungsverhalten gelernt bekommen. Die „*neue*“ Technologie ist nunmehr fixer Bestandteil des Lebens geworden. Jeder ist über die Gefahren aufgeklärt, heikle und intime Daten werden nicht mehr öffentlich in Communities kommuniziert. Die jungen Wilden haben von ihren Eltern gelernt, dass zu viel Informationsdichte im Internet große Gefahren birgt.

Die Selbstregulierung der veröffentlichten Daten in Social Communities wird definitiv stattfinden. Die aktuell gefährdete Privatsphäre von Millionen von Menschen ist es jedoch wert, dass bereits jetzt, vor dem Eintritt von Katastrophen, mit aller Mühe Aufklärungsarbeit über die negativen Seiten der Veröffentlichung von Daten betrieben werden sollte. Von jedem von uns.

Abbildungsverzeichnis

Tabellenverzeichnis

Diagrammverzeichnis

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CSS	Cascading Style Sheet
FAQ	Frequently Asked Questions
HTML	Hypertext Markup Language
HTTPS	Hypertext Transfer Protocol over SSL (-> siehe SSL)
LAN	Local Area Network
SC	Social Community
SQL	Structured Query Language
SSL	Secure Socket Layer
WLAN	Wireless LAN (-> siehe LAN)
XSS	Cross Side Scripting

Literaturverzeichnis

ALBY, T. 2006. *Web 2.0 Konzepte, Anwendungen, Technologien*. München: Carl Hanser Verlag

AGARWALA, V. 2006. (Ohne Titel) [online]. Verfügbar bei: http://www.albumoftheday.com/facebook/final2.swf [Zugang am 20.02.2008]

ALEXANDER, M. 2006. *Netzwerke und Netzwerksicherheit – Das Lehrbuch*. Heidelberg: Verlagsgruppe Süddeutscher Verlag Hüthig Telekommunikation GmbH

ANDERSON, T. 2008. protect your self from phishing! [online]. Verfügbar bei: http://blog.myspace.com/index.cfm?fuseaction=blog.view&friendID=6221&blogID=355522809 [Zugang am 10.04.2008]

ANON, 2006. A day without Facebook [online]. Verfügbar bei: http://daywithoutfacebook.blogspot.com/ [Zugang am 25.02.2008]

ANON, 2008. Die studiVZ Chroniken [online]. Verfügbar bei: http://www.daburna.de/blog/2006/12/01/die-studivz-chroniken/ [Zugang am 24.02.2008]

BAGER, J. 2008. Dabei sein ist alles. *c't*, 5/2008, S. 92

BALAZS, J. 2008. Vom StasiVZ in die Bertelsmann-Datenbank? [online]. Verfügbar bei: http://www.asta.uni-wuppertal.de/index.php?option=com_content&task=view&id=215&Itemid=125 [Zugang am 08.03.2008]

BBC. 2007. MySpace bars 29,000 sex offenders [online]. Verfügbar bei: http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6914870.stm [Zugang am 15.04.2008]

BEEGER, B. 2008. Karrierekiller im Internet [online]. Verfügbar bei: http://www.stern.de/computer-technik/internet/596742.html [Zugang am 20.02.2008]

BERESZEWSKI, M. 2007. Offshore-Stolperfalle Datenschutz [online]. Verfügbar bei: http://www.informationweek.de/services/showArticle.jhtml?articleID=197002165&printable=true [Zugang am 15.04.2008]

BONOW, T. 2006. studiVZ.net wächst schneller als bekanntes Online-Netzwerk openBC [online]. Verfügbar bei: http://www.studivz.net/l/press/9 [Zugang am 27.03.2008]

BÖCKER, J. 2008. Erfolgsfaktoren von Communities im Web2.0 [online]. Verfügbar bei:

http://www.fh-brs.de/data/fhbrs_/fh_brs/die_fachhochschule/aktuell/news/2008/FH_BRS_Abschlussbericht_Forschungsprojekt_Web_2.0.pdf [Zugang am 20.03.2008]

BRIEKE, I. 2008. CommunityEffects 2008. Studie zu Werbung und viralen Marketing in Social Communities [online]. Verfügbar bei: http://pickup.tomorrow-ag.de/_adtech/sales/downloads/pdf/2008/ErgebnisbandCommunityEffects2008.pdf [Zugang am 09.04.2008]

BRISCOE, B. und ODLYZKO, A. und TILLY, B. 2006. Metcalfe's Law is Wrong [online]. Verfügbar bei: http://spectrum.ieee.org/print/4109 [Zugang am 20.02.2008]

BUMANN, M. 2006. StudiVZ in original Facebook Farben [online]. Verfügbar bei: http://bumi.wordpress.com/2006/10/03/studivz-in-original-facebook-farben/ [Zugang am 16.04.2008]

BUTTLER, M. 2007. Vom Terrorverdächtigen zum Kunstobjekt [online]. Verfügbar bei: http://www.tagesschau.de/ausland/meldung494000.html [Zugang am 24.02.2008]

CARNEGIE MELLON UNIVERSITY, 2008. What is reCAPTCHA? [online]. Verfügbar bei: http://recaptcha.net/learnmore.html [Zugang am 15.04.2008]

CHERDRON, M. (Auf Wunsch keine E-Mail-Adresse veröffentlicht), 05.05.2008. *RE: Umfrage zum Datenschutz.* e-Mail to J. NAGL. (se07m015@technikum-wien.at)

CSCM, 2008. Zwischenbericht: Erste Ergebnisse der Umfrage zur privaten Nutzung von Social Networking Services (SNS) in Deutschland [online]. Verfügbar bei: http://www.cnss.de/files/sns-umfrage_final1.pdf [Zugang am 20.02.2008]

DERSTANDARD. 2008a. Social Communitys erschaffen den „gläsernen Menschen" [online]. Verfügbar bei: http://derstandard.at/druck/?id= 3280163 [Zugang am 28.03.2008]

DERSTANDARD. 2008b. Der Politiker, die Prostituierte und das Internet [online]. Verfügbar bei: http://derstandard.at/druck/?id=3270762 [Zugang am 19.03.2008]

DERSTANDARD. 2008c. Facebook macht komplette Profil-Löschung unmöglich [online]. Verfügbar bei: http://derstandard.at/druck/?id=3220015 [Zugang am 20.02.2008]

DERSTANDARD. 2008d. Terroristen missbrauchen Facebook für Morddrohungen [online]. Verfügbar bei: http://derstandard.at/druck/?id=3292712 [Zugang am 08.04.2008]

DREWS H & KASSEL H & LESSENICH, H. 1993. *Lexikon Datenschutz und Informationssicherheit*. 4. Auflage. Berlin und München: Siemens Aktiengesellschaft.

DIRSCHERL, Hans-Christian. 2001. Bill Gates verkündet “Digitale Dekade” [online]. Verfügbar bei: http://www.pcwelt.de/start/gaming_fun/archiv/20068/bill_gates_verkuendet_digitale_dekade/index.html [Zugang am 13.04.2008]

ECONOMIST, 2008. Everywhere and nowhere [online]. Verfügbar bei: http://www.economist.com/business/PrinterFriendly.cfm?story_id=10880936 [Zugang am 22.03.2008]

FACEBOOK, 2007. Facebook Ads Launches with 12 Landmark Partners [online]. Verfügbar bei: http://www.facebook.com/press/releases.php?p=9171 [Zugang am 20.02.2008]

FISCHER-HÜBNER, S. 2001. *IT-Security and Privacy*. Berlin Heidelberg: Springer-Verlag.

FITZPATRICK, B. 2007. Thoughts on the Social Graph [online]. Verfügbar bei: http://bradfitz.com/social-graph-problem/ [Zugang am 22.02.2008]

FREIERT, M. 2008. February Top Social Networks – Make way for the new guys [online]. Verfügbar bei: http://blog.compete.com/2008/03/07/top-social-networks-traffic-feb-2008/ [Zugang am 22.03.2008]

FRITSCH, H. 2006. StudiVZ – Inoffizielle Statistiken vom Dezember 2006 [online]. Verfügbar bei: http://studivz.irgendwo.org/ [Zugang am 28.03.2006]

GÖLDI, A. 2007. Benutzer ist nicht gleich Benutzer. Warum Facebook nicht das nächste Google ist [online]. Verfügbar bei: http://medienkonvergenz.com/2007/10/14/benutzer-ist-nicht-gleich-benutzer-warum-facebook-nicht-das-naechste-google-ist/ [Zugang am 05.04.2008]

GÖLDI, A. 2008. Social Networks: Der Long Tail wedelt [online]. Verfügbar bei: http://medienkonvergenz.com/2008/03/08/social-networks-der-long-tail-wedelt/ [Zugang am 22.03.2008]

GOVANI, T & PASHLEY, H. 2005. Student Awareness of the Privacy Implications When Using Facebook [online]. Verfügbar bei: http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf [Zugang am 20.02.2008]

GRANGER, S. 2001. Social Engineering Fundamentals, Part I: Hacker Tactics [online]. Verfügbar bei: http://www.securityfocus.com/print/infocus/1527 [Zugang am 15.04.2008]

GRAUEL, R. 2006. Werbung 2.0 [online]. Hamburg, *Brand Eins,* Verfügbar bei: http://www.brandeins.de/home/inhalt_print.asp?id=2114&MagID=79&MenuId=130&SID=su8152417241449327 [Zugang am 10.04.2008]

GREIF, B. 2008. Hotmail-Captcha per Bot in sechs Sekunden ausgehebelt [online]. Verfügbar bei: http://www.zdnet.de/security/print_this.htm?pid=39189603-39001541c [Zugang am 14.04.2008]

GROSS, R. & ACQUISTI, A. 2005. Information Revelation and Privacy in Online Social Networks (The Facebook Case) [online]. Pittsburgh. Verfügbar bei: http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf [Zugang am on 12.03.2008]

GROSSMANN, J. 2006. Cross-site Scripting Worms and Viruses [online]. Verfügbar bei: http://www.whitehatsec.com/downloads/WHXSSThreats.pdf [Zugang am 07.04.2008]

HADDAD, N. 2008. 123people will hoch hinaus [online]. Verfügbar bei: http://futurezone.orf.at/business/stories/269098/ [Zugang am 09.04.2008]

HAEUSLER, J. 2006. StudiVZ: Interview mit Martin Weber, Holtzbrinck Ventures [online]. Verfügbar bei: http://www.spreeblick.com/2006/11/27/studivz-interview-mit-martin-weber-holtzbrinck-ventures/ [Zugang am 24.02.2008]

HARRISINTERACTIVE, 2008. Majority Uncomfortable with Websites Customizing Content Based Visitors Personal Profiles [online]. Verfügbar bei: http://www.harrisinteractive.com/harris_poll/index.asp?PID=894 [Zugang am 12.04.2008]

HEIDRICH, J. 2008. XING-Nutzer protestieren gegen ungewollte Profil-Werbung [Update] [online]. Verfügbar bei: http://www.heise.de/newsticker/meldung/print/101263 [Zugang am 20.02.2008]

HEISE, 2008. Britische Regierung will Sexualstraftäter von Sozialnetzwerken aussperren [online]. Verfügbar bei: http://www.heise.de/newsticker/meldung/print/106029 [Zugang am 04.04.2008]

HENDRICKSON, M. 2008. Facebook Chat Launches, For Some [online]. Verfügbar bei: http://www.techcrunch.com/2008/04/06/facebook-chat-enters-pre-release-beta/ [Zugang am 16.04.2008]

HIPPNER, H. und MERZENICH, M. und WILDE, K. 2002. *Handbuch Web Mining im Marketing.* Braunschweig/Wiesbaden: Vieweg Verlag.

HODGKINSON, T. 2008. With friends like these … [online]. Verfügbar bei: http://www.guardian.co.uk/technology/2008/jan/14/facebook/print [Zugang am 20.02.2008]

HOGBEN, G. 2007. Security Issues and Recommendations for Online Social Networks [online]. Verfügbar bei: http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf [Zugang am

20.02.2008]

HOLZSCHUH, A. und ERLER, S. 2008. Kündigung nach Anschlagsdrohung [online]. Verfügbar bei: http://www.rbb-online.de/_/brandenburgaktuell/beitrag_druck_jsp/key=rbb_beitrag_mini_7269372.html [Zugang am on 15.04.2008]

HUSEBY, S. 2004. *Sicherheitsrisiko Web-Anwendung*. Heidelberg: dpunkt.verlag

HÜLSBÖMER, S. 2008. Nutzer sozialer Netze spielen mit dem Feuer [online]. Verfügbar bei: http://www.computerwoche.de/1857176 [Zugang am 22.03.2008]

HÜSING, A. 2008. studiVZ tritt OpenSocial bei [online]. Verfügbar bei: http://www.deutsche-startups.de/2008/05/13/studivz-tritt-opensocial-bei/ [Zugang am 13.05.2008]

IHLENFELD, J. 2008. Xing hat über 5 Millionen Mitglieder [online]. Verfügbar bei: http://www.golem.de/0802/57793.html [Zugang am 16.04.2008]

JACQUEMAIN, K. 2008. Gutes tun im Web 2.0 [online]. Verfügbar bei: http://www.abendblatt.de/daten/2008/02/01/842970.html?prx=1 [Zugang am 24.03.2008]

JANOWICZ, K. 2007. *Sicherheit im Internet*. 3. Auflage. Köln: O'Reilly Verlag.

JONES, H & SOLTREN, J. 2005. Facebook: Threats to Privacy [online]. Verfügbar bei: http://www-swiss.ai.mit.edu/6095/student-papers/fall05-papers/facebook.pdf [Zugang am 12.02.2008]

KAIOO, 2008. Über Kaioo [online]. Verfügbar bei: http://www.kaioo.com/kaioo.html?locale=de [Zugang am 22.03.2008]

KAUL, M. 2008. Jäger und Sammler [online]. Verfügbar bei: http://www.taz.de/1/leben/internet/artikel/1/jaeger-und-sammler/?type=98 [Zugang am 26.03.2008]

KLAU, P. 2002. *Hacker, Cracker, Datenräuber* Braunschweig/Wiesbaden: Vieweg Verlag.

KÖTTER, Y. 2007. Podcast: StudiVZ gibt nach – AGB teilweise widerrufen [online]. Verfügbar bei: http://www.netzwelt.de/print/news/76775-podcast-studivz-gibt-nach-.pdf [Zugang am 09.05.2008]

KRÜGER, A. 2008. Zombie-Rechner lösen Bilderrätsel [online]. Verfügbar bei: http://www.heute.de/ZDFheute/inhalt/21/0,3672,7225397,00.html [Zugang am 15.04.2008]

LENSSEN, P. 2005. Samy, Their Hero [online]. Verfügbar bei: http://blogoscoped.com/archive/2005-10-14-n81.html [Zugang am 24.03.2008]

LEVENE, M. und POULOVASSILIS, A. 2004. *Web Dynamics.* Berlin Heidelberg: Springer.

LISCHKA, K. 2007a. Werber spähen Surfverhalten aus [online]. Verfügbar bei: http://www.spiegel.de/netzwelt/web/0,1518,druck-515932,00.html [Zugang am 20.02.2008]

LISCHKA, K. 2007b. Studentennetz StudiVZ verzichtet auf Schnüffel-Passus [online]. Verfügbar bei: http://www.spiegel.de/netzwelt/web/0,1518,druck-523564,00.html [Zugang am 20.02.2008]

MARX, P. 2008. Brain.exe – Die Rundumlösung für viele Probleme [online]. Verfügbar bei: http://brain.yubb.de/ [Zugang am 10.04.2008]

MCELROY, D. 2008. Saudi woman killed for chatting on Facebook [online]. Verfügbar bei: http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2008/03/31/wsaudi131.xml [16.04.2008]

MEDIENKULTURZENTRUM, 2008a. Social Networks unter der Lupe [online]. Verfügbar bei: http://www.medienkulturzentrum.de/fileadmin/user_upload/verein/dokumente/safer_internet/MySpace.pdf [Zugang am 16.03.2008]

MEDIENKULTURZENTRUM, 2008b. Ergebnisse [online]. Verfügbar bei: http://www.medienkulturzentrum.de/index.php?id=242&L=0&type=1 [Zugang am 16.03.2008]

MERSCHMANN, H. 2006. Privatsphäre ist einfach Mega-out [online]. Verfügbar bei: http://www.spiegel.de/netzwelt/web/0,1518,druck-443539,00.html [Zugang am 11.03.2008]

METCALFE, B. 2006. Guest Blogger Bob Metcalfe: Metcalfe's Law Recurses Down the Long Tail of Social Networks [online]. Verfügbar bei: http://vcmike.wordpress.com/2006/08/18/metcalfe-social-networks/ [Zugang am 20.02.2008]

MEUSERS, R. 2006. Peinliche Pannen bringen StudiVZ in Verruf [online]. Verfügbar bei: http://www.spiegel.de/netzwelt/web/0,1518,druck-448340,00.html [Zugang am 16.04.2008]

MEYER, R. 2006. 700 Stalker und der Datenschutz [online]. Verfügbar bei: http://blogbar.de/archiv/2006/11/23/studivz-700-stalker-und-der-datenschutz/ [Zugang am 24.02.2008]

MIESEN, T. 2008. StudiVZ abgemahnt [online]. Verfügbar bei: http://www.thomasmiesen.de/verbraucherschutzer-mahnen-studivz-ab/ [Zugang am

15.03.2008]

MOHR, N. 2007. Die Bedeutung von Social Communities: Überhöhte Erwartungen oder tatsächliches Potential? [online]. Verfügbar bei: http://www.accenture-countdown.com/wms//customers/acc/pdf/MedientageUGCv5_2007.pdf [Zugang am 20.02.2008]

MOOK, N. 2005. Cross-Site Scripting Worm Hits MySpace [online]. Verfügbar bei: http://www.betanews.com/article/CrossSite_Scripting_Worm_Hits_MySpace/1129232391 [Zugang am 24.03.2008]

MUHR, R. 2007. Das österreichische WORT des Jahres 2007 – Begründung [online]. Verfügbar bei: http://www-oedt.kfunigraz.ac.at/oewort/2007/01_Begr07/1Wort07Begr.htm [Zugang am 27.03.2008]

MÜLLER, G. & REICHENBACH M. 2001. *Sicherheitskonzepte für das Internet.* Berlin Heidelberg: Springer-Verlag.

NIELSEN//NETRATINGS, 2006. Successful Sites Drive High Visitor Retention Rates [online]. Verfügbar bei: http://www.nielsen-netratings.com/pr/pr_060511.pdf [Zugang am 12.03.2008]

O'REILLY, T. 2005. Web 2.0: Compact Definition? [online]. O'Reilly Radar. Verfügbar bei: http://radar.oreilly.com/archives/2005/10/web_20_compact_definition.html [Zugang am 11.01.2007]

OTTO, P. 2007. Nach StudiVZ kommt SchülerVZ – Gruscheln statt Datenschutz? [online]. Verfügbar bei: http://www.e-recht24.de/news/datenschutz/420.html [Zugang am 28.03.2008]

POSTINETT, A. 2008. Demografische Marktforschung wird irrelevant in der Online-Welt [online]. Verfügbar bei: http://blog.handelsblatt.de/webwatcher/eintrag.php?id=325 [Zugang am 11.03.2008]

POGUNTKE, W und BALZERT, H. 2006. *Sicherheit im Internet*. Bochum: W3L-Verlag.

POULSEN, K. 2008a. MySpace Bug Leaks 'Private' Teen Photos To Voyeurs [online]. Verfügbar bei: http://www.wired.com/print/politics/security/news/2008/01/myspace [Zugang am 20.02.2008]

POULSEN, K. 2008b. Pillaged MySpace Photos Show Up in Massive BitTorrent Download [online]. Verfügbar bei: http://www.wired.com/print/politics/security/news/2008/01/myspace_torrent [Zugang am 24.02.2008]

REISSMANN, O. 2008. Facebook setzt StudiVZ unter Druck [online]. Verfügbar bei: http://medienlese.com/2008/01/31/facebook-setzt-studivz-unter-druck/ [Zugang am 24.02.2008]

RIBAROV, G. (Auf Wunsch keine E-Mail-Adresse veröffentlicht), 08.05.2008. *Fragen zum Datenschutz in Social Communities.* e-Mail to J. NAGL. (se07m015@technikum-wien.at)

SCHMIDT, H. 2008. Verweildauer in sozialen Netzwerken sinkt. *Frankfurter Allgemeine Zeitung*. 10. März (Nummer 59), S. 19

SCHONFELD, E. 2008. WordPress: The Social Network [online]. Verfügbar bei: http://www.techcrunch.com/2008/03/04/wordpress-the-social-network/ [Zugang am 09.05.2008]

SCHOOLMANN, J. und RIEGER, H. 2005. *Praxishandbuch IT-Sicherheit*. Düsseldorf: Symposion Publishing GmbH

SCHORMANN, T. 2007. Die (gar nicht so) heimliche Lust am „Ausgooglen“ [online]. Verfügbar bei: http://www.heise.de/newsticker/meldung/97873 [Zugang am 16.03.2008]

SCHROEDER, S. 2008. Secret Crush: First Serious Facebook Hack? [online]. Verfügbar bei: http://mashable.com/2008/01/04/secret-crush-first-serious-facebook-hack/ [Zugang am 24.02.2008]

SCHULZKI-HADDOUTI, C. 2005. Das Netz als Falle: Internetsucht [online]. Verfügbar bei: http://www.das-parlament.de/2005/03/Thema/039.html [Zugang am 16.04.2007]

SCHUMACHER, T. und ERNSTSCHNEIDER, T. und WIEHAGER, A. 2002. *Domain-Namen im Internet*. Berlin Heidelberg: Springer.

SCHWAN, B. 2008. Freunde zum Mitnehmen [online]. Verfügbar bei: http://www.taz.de/nc/1/leben/internet/artikel/1/freunde-zum-mitnehmen [Zugang am 20.02.2008]

SIEBERT, S. 2008. StudiVZ mahnt “VZ”-Seiten ab [online]. Verfügbar bei: http://www.e-recht24.de/news/abmahnung/774.html [Zugang am 16.04.2008]

SMARR, J. und CANTER, M. und SCOBLE, R. und ARRINGTON, M. 2007. A Bill of Rights for Users of the Social Web [online]. Verfügbar bei: http://opensocialweb.org/2007/09/05/bill-of-rights/ [Zugang am 20.02.2008]

SOLTAU, T. 2008. Profiteure des Protests [online]. Verfügbar bei: http://www.stern.de/computer-technik/internet/607520.html [Zugang am 20.02.2008]

SPIEGEL, 2008. Vote-Auswertung: Personalisierte Online-Werbung [online]. Verfügbar bei: http://www1.spiegel.de/active/vote/fcgi/vote.fcgi?voteid=4803 [Zugang am 20.02.2008]

STAEDELE, K. 2008. StudiVZ will gegen StasiVZ-Video vorgehen [online]. Verfügbar bei: http://www.presseportal.de/print.htx?nr=1123060 [Zugang am 24.03.2008]

STEINER, P. 2006. *Effektiv arbeiten mit dem Internet.* Darmstadt: Wissenschaftliche Buchgesellschaft

STÖCKER, C. 2006. Sex-Stalker im Studentennetz [online]. Verfügbar bei: http://www.spiegel.de/netzwelt/web/0,1518,druck-450866,00.html [Zugang am 24.02.2008]

STÖCKER, C. 2007a. IT-Giganten stricken am Menschen-Netz [online]. Verfügbar bei: http://www.spiegel.de/netzwelt/web/0,1518,druck-507689,00.html [Zugang am 20.02.2008]

STÖCKER, C. 2007b. Google gewinnt schon wieder [online]. Verfügbar bei: http://www.spiegel.de/netzwelt/web/0,1518,druck-515036,00.html [Zugang am 20.02.2008]

SPECK, H. 2007. Social Network Analysis. [online] Verfügbar bei: http://www.egs.edu/faculty/speck/files/presentation2007akwmsocialnetworks.pdf [Zugang am 01.03.2008]

SPECK, H. 2008. Gastbeitrag von Prof. Hendrik Speck: “Mehr Profildaten verfügbar als zu Stasi-Zeiten” [online]. Verfügbar bei: http://www.deutsche-startups.de/2008/02/27/gastbeitrag-von-prof-hendrik-speck-mehr-profildaten-verfuegbar-als-zustasi-zeiten/ [Zugang am 16.03.2008]

VON AHN, L. und BLUM, M und LANGFORD, J. 2004. Telling Humans And Computers Apart Automatically. *Communications of ACM. Volume 47 (2), 57.*

WEIGERT, M. 2007a. Über 100 Social Networks in Deutschland [online]. Verfügbar bei: http://www.zweinull.cc/uber-100-social-networks-aus-deutschland/ [Zugang am 06.04.2008]

WEIGERT, M. 2007b. MySpace aufgepasst: Jetzt kommt Facebook [online]. Verfügbar bei: http://www.zweinull.cc/myspace-aufgepasst-jetzt-kommt-facebook/ [Zugang am 06.04.2008]

WEIGERT, M. 2008a. Streitthema „Datenschutz im Social Web“ – Umfrage will Klarheit schaffen [online]. Verfügbar bei: http://www.zweinull.cc/streitthema-datenschutz-im-social-web-%E2%80%93-umfrage-will-klarheit-schaffen/ [Zugang am 09.04.2008]

WEIGERT, M. 2008b. Sind Micropayments der Segen für das Web 2.0? [online]. Verfügbar bei: http://www.zweinull.cc/sind-micropayments-der-segen-fur-das-web-20/ [Zugang am

20.04.2008]

WELT ONLINE. 2007a. EU prüft Spionage-Reklame von Facebook und Co. [online]. Verfügbar bei: http://www.welt.de/webwelt/article1401201/EU_prueft_Spionage-Reklame_von_Facebook_und_Co..html [Zugang am 20.02.2008]

WELT ONLINE. 2007b. Das Geschäft mit den Nutzerdaten [online]. Verfügbar bei: http://www.welt.de/webwelt/article1459528/Das_Geschaeft_mit_den_Nutzerdaten.html [Zugang am 20.02.2008]

WELZEL, K. 2007. Hintergründe zu den neuen AGB bei studiVZ [online]. Verfügbar bei: http://www.backview.eu/hochschule/hochschule/hintergrunde-zu-den-neuen-agb-bei-studivz.html [Zugang am 08.04.2008]

WHATSYOURPLACE, 2008. Wo ist die “kritische Masse”? [online]. Verfügbar bei: http://www.whatsyourplace.de/blog/?p=159 [Zugang am 20.02.2008]

XING, 2007a. Communication and Networking on the Internet [online]. Verfügbar bei: http://corporate.xing.com/fileadmin/image_archive/pressrelease_3rd_international_XING_survey_2007_english.pdf [Zugang am 20.02.2008]

XING, 2007b. XING öffnet Plattform für Werbung [online]. Verfügbar bei: http://corporate.xing.com/no_cache/deutsch/presse/willkommen/news-detailansicht/article/pressemitteilungbrxing-oeffnet-plattform-fuer-werbung/ [Zugang am 10.04.2008]

XING, 2008. Update: Keine Werbung auf den Profilseiten der Premium-Mitglieder [online]. Verfügbar bei: https://www.xing.com/news/2008-01-07.html [Zugang am 20.02.2008]

ZUCKERBERG, M. 2006. An Open Letter from Mark Zuckerberg [online]. Verfügbar bei: http://blog.facebook.com/blog.php?post=2208562130 [Zugang am 25.02.2008]

Anhang

- Ausgewählte Screenshots vom Vergleich der Social Communities:
  - MYSPACE1
  - MYSPACE2
  - FACEBOOK1
  - XING1
- Ausdruck eines Fragebogens der durchgeführten Online-Befragung
- E-Mail Gespräch mit Herrn Malte Cherdron, CMO studiVZ Ltd.
- Experteninterview Mag. Gregor Ribarov

Vorwort

Datenschutz in Social Communities

Hallo und vielen Dank, dass du dir die Zeit nimmst und eine Umfrage im Rahmen meiner Master Thesis (Diplomarbeit) ausfüllst. Das Thema meiner Arbeit lautet "Datenschutz in Social Communities" und sie beleuchtet die vielen datenschutzrechtlichen Aspekte im Zusammenhang mit der Nutzung von Social Communities.
Social Communities sind Plattformen im Internet, die das aktive Mitwirken der Benutzer in den Vordergrund stellen. Bekannte Beispiele für solche Plattformen sind studiVZ, MySpace oder Facebook.

In 36 Fragen möchte ich dich zu deiner Meinung und und deinen Gewohnheiten im Bezug auf die Nutzung von Social Communities und den damit verbundenen datenschutzbezogenen Themen befragen. Ich würde dich bitten nach dem Ausfüllen der Umfrage den Link an Bekannte/Verwandte/Freunde weiterzuleiten. Je mehr Personen an der Umfrage teilnehmen, desto aussagekräftiger und interessanter sind unsere Ergebnisse.

PS: Keine Sorge, deine Daten werden natürlich nicht missbräuchlich verwendet und nach Beendigung der Auswertung gelöscht. :-)

Verantwortlich für den Fragebogen:

Johannes Nagl, FH Technikum Wien, Masterstudiengang Multimedia und Softwareentwicklung

Frage 1

Bei welcher der folgenden Social Communities bist du regelmäßig aktiv?

Mehrfachantwort möglich

- [ ] MySpace
- [ ] Facebook
- [ ] Kaioo
- [ ] Xing
- [ ] studiVZ
- [ ] Keine der hier angeführten.

Frage 2

Bei wie vielen Social Communities bist du zur Zeit registriert?

Frage 3

Wie viele Social Communities nutzt du täglich | wöchentlich | monatlich?

	0	1	2	3	4	5	> 5
täglich							
wöchentlich							
monatlich							

Frage 4

Wie viel Zeit (in Minuten) verbringst du täglich in Social Communities?

Frage 5

Aus welchen Gründen nutzt du Social Communities?

Mehrfachantwort möglich - Maximal 7 Antworten

- privat
- geschäftlich
- sowohl privat als auch geschäftlich
- Networking
- Zeitvertreib
- Dating

- [ ] Einfaches Kommunikationsmittel
- [ ] Wissensaustausch
- [ ] Etwas über Andere erfahren

Frage 6

Hast du Bedenken, deine privaten Daten (wie Name, Adresse, E-Mail-Adresse, Telefonnummer, ...) in Social Communities zu veröffentlichen?

- ( ) ja
- ( ) nein

Frage 7

Wenn Ja, worauf beziehen sich deine Bedenken?

Mehrfachantwort möglich

- [ ] kommerzielle Nutzung der Daten
- [ ] Daten könnten in falsche Hände geraten
- [ ] Daten könnten von fremden Personen (Jahre später) über Suchdienste gefunden werden
- [ ] Vermehrter Empfang von Spam
- [ ] Sonstige

Frage 8

Ist es für dich relevant, in welchem Land Daten, die du über dich veröffentlichst, gespeichert werden?

- ( ) Ja
- ( ) Nein
- ( ) Habe mich noch nicht damit auseinander gesetzt

Frage 9

Erwartest du dir von einer geschäftlichen Community (bsp: Xing) mehr oder weniger Datenschutz als von einer Plattform für Freizeitnutzung (bsp: MySpace)?

- ○ Mehr
- ○ Gleich
- ○ Weniger

Frage 10

Erwartest du dir von einer (teilweise) kostenpflichtigen Community (bsp: Xing) mehr oder weniger Datenschutz als von einer gratis Plattform?

- ○ Mehr
- ○ Gleich
- ○ Weniger

Frage 11

Aus welchen Gründen entscheidest du dich für eine bestimmte Community?

Mehrfachantwort möglich

- ☐ angebotene Features
- ☐ Mitgliederzahl
- ☐ bereits angemeldete Freunde
- ☐ Image der Community
- ☐ Informationsgewinn
- ☐ Sonstiges

Frage 12

Hast du dich schon mal bei einer Community nicht registriert, weil du mit den AGBs nicht einverstanden warst?

- ja
- nein

Frage 13

Vertraust du darauf, dass dich die Betreiber der Communities genau über die Verwendung deiner Daten informieren?

- ja
- nein

- Weiss nicht/Keine Angabe

Frage 14

Würdest du dich bei Communities registrieren, die deine Daten an Drittanbieter für Werbezwecke weitergeben?

- ja
- nein
- nur mit falschem Namen

Frage 15

Angenommen, du bist bei mehreren Communities registriert. Möchtest du, dass deine Daten von einer zur anderen Community automatisch mitgenommen werden können?

- Ja, wäre toll
- Finde ich bedenklich
- Kein Interesse

Frage 16

Wenn ja, welche Daten möchtest du zu anderen Communities mitnehmen können?

Mehrfachantwort möglich

- [ ] Profildaten
- [ ] Freunde/Netzwerk
- [ ] Fotos
- [ ] Nachrichtenhistorie mit einzelnen Personen

Frage 17

Registrierst du dich mit deinem richtigen Namen in Communities?

- ( ) ja
- ( ) nein
- ( ) manchmal

Frage 18

Welchen Anteil der Profilfelder, die notwendig sind, um ein neues Benutzerprofil in einer Community anzulegen, füllst du aus?

- ( ) Alle
- ( ) Mehr als die Hälfte
- ( ) Weniger als die Hälfte
- ( ) Nur Pflichtfelder

Frage 19

Gibst du bei Registrierungen in Social Communities immer das gleiche Passwort an?

- ( ) ja
- ( ) nein

Frage 20

Gibst du bei Registrierungen in Social Communities immer die gleiche E-Mail-Adresse an?

- ja
- nein

Frage 21

Welche E-Mail-Adressen verwendest du bei der Registrierung in einer Social Community?

Mehrfachantwort möglich

- Firmen-E-Mail-Adresse (bzw. Uni-Adresse)
- Privat-E-Mail-Adresse
- Eigene E-Mail-Adresse für Social Communities
- Fake-E-Mail-Adresse

Frage 22

Communities bieten oftmals die Möglichkeit zur variablen Festlegung deiner Privatsphäre (Wer darf welche Teile deines Profils sehen?) für definierte Personengruppen. Findest du, diese Möglichkeiten ....

- ... reichen vollkommen aus
- ... sind viel zu oberflächlich
- ... unnötig (benutze ich nicht)
- ... sind viel zu aufwendig

Frage 23

Wenn du Bedenken bezüglich der Sicherheit deiner Daten (bsp: Zugriff durch unbefugte Dritte) hättest, welche Schritte würdest du unternehmen?

- Keine
- Reduzierung der persönlichen Daten
- Löschen des Profils

- ○ Gar nicht erst anmelden

Frage 24

Sprichst du mit Freunden über etwaige Bedenken im Bezug auf die Verwendung deiner Daten in Social Communities?

- ○ ja
- ○ nein

Frage 25

Über welche Dienste suchst du aktiv nach Bekannten/Freunden im Internet?

Mehrfachantwort möglich

- ☐ allgemeine Suchmaschinen (wie Google, Yahoo, Live Search, ...)
- ☐ Personensuchmaschinen (wie 123people, yasni, ...)
- ☐ Social Communities
- ☐ Gelbe Seiten
- ☐ Ich suche nicht nach Personen im Internet

Frage 26

Welche Teile von Social Communities benutzt du?

Mehrfachantwort möglich

- ☐ Freunde definieren
- ☐ Eigene Fotos hochladen
- ☐ Nachrichtenversand
- ☐ Nach neuen Bekannten suchen
- ☐ etwas über das Privatleben anderer herausfinden
- ☐ Kontakte pflegen

Frage 27

Wurden schon einmal (vielleicht Jahre später) Daten von dir im Internet gefunden, die dir unangenehm waren?

- ja
- nein

Frage 28

Löscht du dein Profil, wenn du nicht mehr in der Community aktiv bist?

- ja
- nein

Frage 29

Aus welchen Gründen würdest du dein Profil in Social Communities löschen?

Mehrfachantwort möglich

- Missbräuchliche Verwendung meiner Daten
- Gründe für die Registrierung sind weggefallen
- Andere Community gefunden
- Keine Zeit mehr
- Geänderte AGBs sind nicht akzeptabel
- möchte nicht mit der Social Community in Verbindung gebracht werden
- möchte nicht, dass Daten später wieder gefunden werden
- Freunde sind nicht mehr auf der Plattform aktiv

Frage 30

Findest du es selbstverständlich, dass bei dem Löschen deines Profils alle Daten tatsächlich gelöscht werden?

- ja
- nein

Frage 31

Wie genau hast du dich bereits mit dem Thema Datenschutz auseinander gesetzt?

- immer
- sehr oft
- oft
- gelegentlich
- selten
- sehr selten
- nie

Frage 32

Welche der folgenden Aussagen machen eine Community im Bezug auf datenschutzrechtliche Aspekte deiner Meinung nach am effektivsten "sicher"? (max. 4)

Mehrfachantwort möglich - Maximal 4 Antworten

- [ ] Gelöschte Daten werden tatsächlich gelöscht
- [ ] klare vertragliche Datenschutzbestimmungen (bsp. AGB)
- [ ] Gesetzliche Datenschutzbestimmungen werden eingehalten
- [ ] Bei der Anmeldung besteht nur die Pflicht der Eingabe von zweckmäßigen Daten
- [ ] Daten werden nicht an Dritte weitergegeben
- [ ] Daten können nicht von unbefugten Dritten (bsp. Hacker) ausgelesen werden
- [ ] Die Betreiber verzichten auf personalisierte Werbung/Targeting
- [ ] Die Betreiber informieren aktiv über Mechanismen zum Datenschutz/-sicherheit
- [ ] Daten werden verschlüsselt abgespeichert
- [ ] Einstellbare Sichtbarkeit bestimmter Profildaten

Frage 33

Glaubst du, dass deine Daten in den Social Communities "sicher" sind?

- sehr sicher
- sicher
- es geht
- manchmal unsicher
- unsicher
- sehr unsicher

Frage 34

Ich bin zur Zeit ...

- ... Schüler
- ... Lehrling
- ... Student
- ... Arbeiter/Angestellter
- ... Selbstständig
- ... ohne Beschäftigung
- ... Sonstiges

Frage 35

Dein Geschlecht?

- Männlich
- Weiblich

Frage 36

Dein Land?

- Deutschland
- Österreich
- Schweiz
- Sonstiges

Danke!

Datenschutz in Social Communities

Herzlichen Dank für deine Beantwortung der Fragen. Solltest du Interesse an den Resultaten dieser Umfrage haben, schicke bitte eine E-Mail mit dem Betreff **"Datenschutz in Social Communities - Umfrageergebnisse"** und deinen Kontaktdaten (Name, Mailadresse) an die Adresse: **se07m015@technikum-wien.at**.
Nach Veröffentlichung meiner Master Thesis schicke ich dir die Ergebnisse gerne zu.

Hier noch mal kurz der Hinweis: Bitte schicke den Link zur Umfrage an Bekannte/Verwandte/Freunde weiter :-).

Solltest du in der Zwischenzeit bereits Interesse an dem Ergebnis der Umfrage "private Nutzung von Social-Networking-Services in Deutschland" haben, empfehle ich dir einen Besuch auf der Seite http://www.kooperationssysteme.de/2008/02/17/erste-ergebnisse-der-sns-umfrage/.

Verantwortlich für den Fragebogen:
Johannes Nagl, FH Technikum Wien, Masterstudiengang Multimedia und Softwareentwicklung