3-4-2015

Datenschutzbedenken in Sozialen Netzen – ein Strukturgleichungsmodell

Maike Kuckertz

Burkhardt Funk

Datenschutzbedenken in Sozialen Netzen – ein Strukturgleichungsmodell

Maike Kuckertz, Burkhardt Funk

Leuphana Universität Lüneburg, Scharnhorststr.1, D-21339 Lüneburg

maike.kuckertz@stud.leuphana.de
funk@uni.leuphana.de

Abstract. Nicht erst mit den Enthüllungen des ehemaligen US-Geheimdienstmitarbeiters Edward Snowden werden in Deutschland zunehmend Bedenken zum Datenschutz von onlinebasierten Sozialen Netzwerken geäußert. Aufbauend auf der Studie von Malhotra et al. (2004) zu Datenschutzbedenken im E-Commerce untersucht die vorliegende Arbeit die Auswirkungen der Datenschutzbedenken auf das faktische Nutzungsverhalten von Online Sozialen Netzwerken (OSN) mit Hilfe eines Strukturgleichungsmodells. Die durchgeführte empirische Studie mit 258 Teilnehmern belegt den direkten und indirekten Einfluss der von Malhotra et al. abgeleiteten Konstrukte (Erhebung, Kontrolle und Bewusstsein) auf das faktische Verhalten in OSN und bietet Unternehmen einen Leitfaden zur Diskussion von Gestaltungsmerkmalen und der Nutzung von OSN.

Keywords: Datenschutz, Soziale Netze, Risikowahrnehmung, Strukturgleichungsmodellierung

1 Einleitung

Seit dem Bekanntwerden der Ausspähaffäre des amerikanischen Geheimdienstes ist in Deutschland Datensicherheit und Datenschutz von Online Sozialen Netzwerken (OSN) ein kontroverses Thema. Benutzer schenken OSN ihr Vertrauen oder schätzen das Risiko zu groß ein, ihre persönlichen Daten preiszugeben. Für die OSN-Betreiber entscheidet dieses Vertrauensverhältnis über den wirtschaftlichen Erfolg eines Angebots, denn der Wert von Personenprofilen bspw. im Kontext der Online-Werbung hängt eng mit dem Umfang der bereitgestellten persönlichen Informationen zusammen [16]. Dem Internet User Information Privacy Modells (IUIPC) von Malhotra et al. [8] folgend werden Datenschutzbedenken durch die Art der Erhebung, die Kontrolle über die persönlichen Daten und das Bewusstsein beeinflusst, wie die Daten verwendet und behandelt werden.

Während Malhotra et al. (2004) Datenschutzbedenken im E-Commerce untersucht haben, ist das Ziel der vorliegenden Arbeit, die Datenschutzbedenken in OSN in Form eines Kausalmodells zu erklären und anhand eines Strukturgleichungsmodells die Abhängigkeiten zu quantifizieren.

12th International Conference on Wirtschaftsinformatik,
March 4-6 2015, Osnabrück, Germany

Kuckertz, M.; Funk, B. (2015): Datenschutzbedenken in Sozialen Netzen – ein Strukturgleichungsmodell, in: Thomas. O.; Teuteberg, F. (Hrsg.): Proceedings der 12. Internationalen Tagung Wirtschaftsinformatik (WI 2015), Osnabrück, S. 1771-1785

Der Beitrag der vorliegenden Arbeit liegt (i) in der Übertragung des IUIPC Modells auf den Kontext von OSN, (ii) der Betrachtung von faktischem Verhalten vs. der bisher untersuchten Verhaltensintention und (iii) der Durchführung einer empirischen Studie in Deutschland. Für die Studie wurde ein innovativer Crowd-Sourcing-Ansatz gewählt, der eine interessante Möglichkeit bietet, Studien auf eine breite, empirische Basis zu stellen.

Die Arbeit beginnt mit einer Einführung zur Datenschutzsituation in den OSN und der Darstellung von Datenschutzbedenken. Darauf folgt die Modellentwicklung sowie die Darstellung des theoretischen Rahmens und der Hypothesen. Anschließend werden die empirische Grundlage und die Datenerhebung mittels eines Crowdsourcing-Ansatzes vorgestellt. Das Modell wird mit Hilfe einer zweistufigen PLS-Modellschätzung geschätzt und im Vergleich mit den Ergebnissen von Malhotra et al. [8] diskutiert.

2 Grundlagen

2.1 Datenschutz in Sozialen Netzwerken

Der englische Begriff „privacy“ kann sowohl mit Datenschutz als auch mit Privatsphäre übersetzt werden. Der Datenschutz ist das Sicherstellen für das Aufrechterhalten der Privatsphäre. Die Privatsphäre beschreibt das Recht, alleine gelassen zu werden [13]. Allerdings bezieht sich der Begriff „privacy“ meistens auf persönliche Informationen. Er beschreibt eine Forderung nach der Selbstbestimmung wann, wie und in welchem Ausmaß die persönlichen Informationen an andere freigegeben werden [8]. Das Eindringen in die Privatsphäre wird üblicherweise als unerlaubte Sammlung, Offenlegung oder weitere Verwendung der persönlichen Informationen interpretiert[13]. „Der europäische und internationale Datenschutz sichert die Datenerfassung, -weitergabe, -speicherung und –bearbeitung mit dem Ziel des Schutzes der Persönlichkeitssphäre des einzelnen Bürgers.“ [11]

Das Bundesdatenschutzgesetz regelt in § 4 Abs. 1, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur dann zulässig ist, wenn das Gesetz dies erlaubt, anordnet oder der Individuelle zugestimmt hat [2]. Darüber hinaus ist laut § 4 Abs. 2 das Erheben von personenbezogenen Daten nur beim Betroffenen erlaubt. Hat dieser der Erhebung nicht eingewilligt, dürfen Daten nur in Ausnahmefällen erhoben werden. Dementsprechend wird jedem einzelnen Bürger das Grundrecht auf „informationelle Selbstbestimmung“ zugesprochen. Er darf somit über die Speicherung und Weitergabe seiner Daten weitestgehend selbst entscheiden [11].

2.2 Datenschutzbedenken der User

Facebook erzielte lt. Jahresbericht 2013 Erträge von rund 7,9 Milliarden US-Dollar, wovon knapp 90% aus der personalisierten Werbung resultierten [12]. Für das Ausliefern personenbezogener Werbung sind vor allem das Sammeln und Auswerten der persönlichen Informationen notwendig. Obwohl die OSN in ihren Datenschutzrichtlinien die Erhebung und Verwendung der persönlichen Informationen offenlegen, gibt es umfangreichen Bedenken ggü. der personalisierten Werbung [5].

Fuchs schätzt in „Facebook, Web 2.0 und ökonomische Überwachung“ die Komplexität der Nutzungs- und Datenschutzbedingungen als zu hoch ein und äußert Zweifel daran, ob Nutzer, die den Datenschutzbestimmungen zustimmen, diese wirklich

gelesen, geschweige denn ihnen bewusst zugestimmt haben. Dies liegt oftmals auch an den in juristischer Sprache verfassten Bestimmungen. Zusätzlich beschränken Zwangswerbungen und Opt-Out-Werbelösungen die freie Auswahlmöglichkeit.

Die damit verbundenen Bedenken und der Fall Edward Snowden haben gerade in Deutschland die Befürchtungen vor einer umfassenden Überwachung wachsen lassen, so dass eine Untersuchung, welche Faktoren die Datenschutzbedenken von Nutzern bedingen für Plattformbetreiber, werbetreibende Unternehmen und die Politik gleichermaßen von Interesse ist.

3 Modellentwicklung

3.1 Theoretischer Rahmen

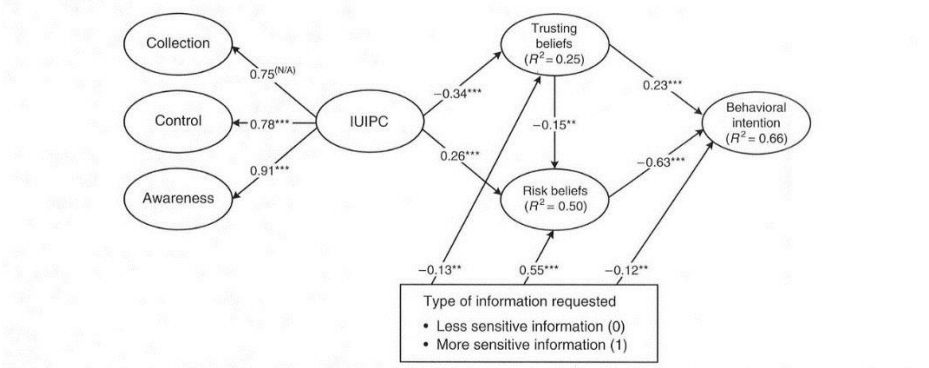
In zahlreiche Studien wurden die Datenschutzbedenken im Onlinehandel und in OSN untersucht. Die Studie von Fogel und Nehmad [4] „Internet social network communities: Risk taking, trust, and privacy concerns“ belegt, dass Personen mit Profilen in Sozialen Netzwerken größere Risikobereitschaften aufweisen. Außerdem haben Männer die größere Bereitschaft, Risiken einzugehen. Frauen haben demnach die größeren Datenschutzbedenken. Young und Quan-Haase [15] zeigen, dass die Größe des persönlichen Netzwerkes einen positiven Zusammenhang mit der Freigabe von Informationen aufweist. Zudem stellen die Autoren fest, dass die Datenschutzbedenken im Internet negativ mit der Informationsfreigabe korrelieren.

Im Vordergrund stehen bei diesen Studien die Zusammenhänge zwischen demografischen Daten und dem Nutzungsverhalten oder den Datenschutzbedenken. In ihrer Arbeit „Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model“ entwickeln Malhotra et al. ein konzeptionelles Modell (Abb. 1), das die kausalen Zusammenhänge zwischen den latenten Variablen Datenschutzbedenken, Vertrauen, Risikowahrnehmung und der Verhaltensintention im Online Handel untersucht. Die Datenschutzbedenken entstehen danach aus dem Zusammenwirken der Dimensionen „Erhebung“, „Kontrolle“ und „Bewusstsein über Praktiken im Datenschutz“.

Die Dimensionen sind die Erhebung, die Kontrolle und das Bewusstsein über die Praktiken im Datenschutz. Die Erhebung definiert sich als Verhältnis zwischen dem Sammeln von persönlichen Informationen und dem daraus entstandenen Profit für den einzelnen User [8]. Diese Informationen umfassen die E-Mail-Adresse des Users, dessen benutzte Software, seine Internetzugriffshistorie, private Dateien etc. [13]

Die Kontrolle über die eigenen Daten ist ein wichtiger Faktor, da die User eher persönliche Informationen von sich preisgeben, wenn sie ihre Daten zurückziehen können, wenn sie die Möglichkeit für einen Opt-Out haben. Demnach ist anzunehmen, dass eine fehlende Kontrolle die Datenschutzbedenken erhöht [8].

Die dritte Dimension ist das Bewusstsein über die Praktiken im Datenschutz. Wenn den Usern erklärt wird, was mit den Daten, die sie angeben, geschieht, sind diese eher bereit, solche anzugeben. Dieses Phänomen wurde unter anderem auch in der Studie von Culnan und Armstrong festgestellt [3].



Notes. Completely standardized estimates, controlled for seven variables in the proposed model (Figure 1), model fit [$x^2(290) = 574.75$; CFI = 0.95; CFI = 0.92; RMSEA = 0.047; CAIC = 1,399.16], $^*p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$ (two-tailed).

Abb. 1. IUIPC Modell nach Malhotra et al. [8] und Ergebnisse

Das in Abb. 1 dargestellte Modell verdeutlicht den negativen Zusammenhang zwischen Risikowahrnehmung und Vertrauen und den vor- und nachgelagerten Konstrukten Datenschutzbedenken und Verhaltensintention. Des Weiteren werden die Variablen Risikowahrnehmung, Vertrauen und Verhaltensintention durch eine Kontextvariable beeinflusst, die die Vertraulichkeit/Sensibilität der abgefragten Daten repräsentiert.

Hier ist das Vertrauen eine Variable, die beschreibt, in welchem Grad die Nutzer glauben, dass Soziale Netzwerke verlässlich im Schutz der persönlichen Informationen sind. Wenn die Datenschutzbedenken hoch sind, ist zu erwarten, dass das Vertrauen in das Soziale Netzwerk niedrig ist und deshalb auch wenige Informationen tatsächlich preisgegeben werden.

Die Risikoeinschätzung bezieht sich auf die Erwartung, dass eine hohe Wahrscheinlichkeit besteht, gegen die Betreiber zu verlieren, was in Verbindung mit dem tatsächlichen Freigeben von Informationen steht.

Das Vertrauen hat außerdem Auswirkungen auf die Risikoeinschätzung. Das bedeutet, je mehr Vertrauen ein User einem Sozialen Netzwerk schenkt, desto weniger wird er das Risiko einschätzen können, welches die Angabe der persönlichen Daten betrifft [8].

Insgesamt erscheint eine Übertragung des Modells von Malhotra et al. auf OSN möglich. Im Gegensatz zur Studie von Malhotra et al. untersuchen wir jedoch das faktische Verhalten, das sich auf die tatsächliche Freigabe von Informationen bezieht. Dazu zählt, ob die Nutzer ihre Posts auf Facebook öffentlich schalten, ob sie sich beim Verlassen der Website oder der mobilen App eines Sozialen Netzwerks immer ausloggen, oder ob man sich auf fremden Webseiten eher mit seinem Facebook Konto einloggt, als seine manuelle Registrierung durchzuführen.

Die Forschungsfrage dieser Arbeit lautet: Wie ist der Einfluss von Datenschutzbedenken auf das *faktische* Verhalten in *Online Sozialen Netzwerken*? Ob die oben aufgezeigten Zusammenhänge tatsächlich bestehen wird im empirischen Teil dieser Studie untersucht.

3.2 **Hypothesen**

Es wird angenommen, dass die Datenschutzbedenken Auswirkungen sowohl auf das Vertrauen als auch auf die Risikowahrnehmung und letztendlich das faktischen Verhalten in OSN haben. So haben Nutzer mit niedrigen Datenschutzbedenken ein hohes Vertrauen in die Sicherheit ihrer Daten, und Nutzer mit höheren Datenschutzbedenken sehen ein hohes Risiko bezüglich der Datensicherheit. Dementsprechend ergeben sich folgende Hypothesen:

H1: Je größer die Datenschutzbedenken sind, desto niedriger ist das Vertrauen.

H2: Je größer die Datenschutzbedenken sind, desto höher ist die Risikoeinschätzung.

Die Variablen Vertrauen und Risiko wirken allerdings auch aufeinander, denn je mehr ein Nutzer Vertrauen in das OSN hat desto geringer ist auch das wahrgenommene Risiko.

H3: Je höher das Vertrauen ist, desto niedriger ist das wahrgenommene Risiko.

Das Vertrauen und die Risikoeinschätzung haben letztendlich (mit unterschiedlichem Vorzeichen) Einfluss auf das faktische Verhalten, das sich in dieser Studie auf Nutzungsgewohnheiten (s.o.) bezieht. Hat man ein höheres Vertrauen in das OSN, stärkt das die Nutzung des Angebots. Im Gegensatz dazu ist anzunehmen, dass bei einer hohen Risikoeinschätzung das faktische Verhalten eher niedrig sein wird.

H4: Je höher das Vertrauen ist, desto ausgeprägter und umfangreicher ist die Nutzung des OSN.

H5: Je höher das wahrgenommene Risiko ist, desto geringer ist die Nutzung des OSN.

Das resultierende Modell entspricht mit den zuvor genannten Änderungen dem von Malhotra et al. vorgeschlagenen Strukturgleichungsmodell zweiter Ordnung. Die höhere Ordnung ergibt sich dabei aus der Tatsache, dass Dimensionen wie Kontrolle selbst latent sind und Datenschutzbedenken damit ein Konstrukt zweiter Ordnung, das also nicht „direkt über reflektive Messmodelle mit manifesten Variablen gemessen werden“ kann [14]. Abb. 2 zeigt das Strukturgleichungsmodell inkl. der Abhängigkeit der reflektiven Konstrukte Bewusstsein, Erhebung und Kontrolle, die selbst latent sind. Die Datenschutzvariable wird durch die drei vorgelagerten Konstrukte messbar.

Die Erhebung repräsentiert die persönliche Einschätzung und Bereitschaft zur Angabe von personenbezogenen Daten. Sie ist ein Maß dafür, wie umfangreich die befragte Person bereit ist umfangreiche personenspezifische Daten anzugeben und damit den OSN Chancen zur Nutzung einzuräumen [8].

Das Konstrukt Kontrolle misst, in wie weit der Nutzer von OSN die Verwendung und Speicherung seiner Daten selbst bestimmen kann. Nutzer sind lt. Malhotra et al. weniger besorgt um die Datenerhebung, wenn sie selbst explizit der Erhebung zustimmen oder eine Opt-Out-Lösung in Anspruch nehmen können. Die Kontrolle hat somit einen negativen Einfluss auf die Datenschutzbedenken. Sie wird durch Items gemessen, die nach der persönlichen Wichtigkeit der Kontrolle, nach dem Recht auf

informationelle Selbstbestimmung und nach der Überzeugung fragen, dass die Privatsphäre verletzt wird, wenn die zugeschriebene Kontrolle eingeschränkt wird.

Das Bewusstsein über die Praktiken im Datenschutz ist im Gegensatz zur Kontrolle keine aktive Dimension. Es bezieht sich auf die beiden Empfindungen der Transparenz und der wahrgenommenen Fairness. Die Items beziehen sich vor allem auf das Bekanntgeben der Datenschutzrichtlinien seitens der OSN-Betreiber.

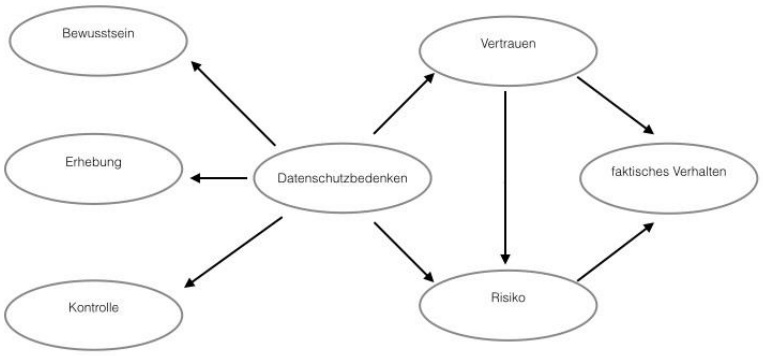


Abb. 2: Strukturgleichungsmodell

4 Empirische Daten

Die Stichprobe umfasst 258 Teilnehmerinnen und Teilnehmer, von denen 200 über die Crowdsourcing Plattform Clickworker [7] und die übrigen 58 über das private Netzwerk in Facebook generiert wurde. Die Umfrage fand vom 13. bis zum 18. Juni 2014 statt.

Dem Fragebogen[1] war eine kurze Abfrage vorgeschaltet, ob der Befragte überhaupt in Sozialen Netzwerken aktiv ist. So wurde sichergestellt, dass der Befragte in der Lage ist, den Fragebogen kompetent zu beantworten.

Zu jedem latenten Konstrukt wurden mehrere Fragen gestellt, die mit monopolen Intervallskalen mit Zahlenvergabe von 1 bis 5 und der verbalen Extrempunktbeschreibung „ich stimme überhaupt nicht zu“ bzw. „ich stimme voll zu“ die persönlichen Einschätzungen der Befragten messbar machen.

Zusätzlich zu den die Konstrukte betreffenden Fragen wurden demographische Daten und Daten zur Erfahrung im Umgang mit OSN abgefragt. Die deskriptiven Merkmale der Stichprobe sind in Tabelle 1 zusammengefasst.

Drei Fragebögen werden nicht im Rahmen der folgenden Analyse berücksichtigt, da sie über alle Items eine sehr geringe Varianz aufwiesen und somit keinen Beitrag zur Untersuchung leisten.

[1] Vgl. Anhang.

Tabelle 1: Eigenschaften der Stichprobe (n = 258)

Geschlecht	*Weibl.*	*Männl.*				
Anzahl	142	116				
Prozent	55,0	45,0				
Alter in Jahren	*< 24*	*25 - 34*	*35 - 44*	*45 - 54*	*55 - 64*	*> 65*
Anzahl	86	107	42	11	5	7
Prozent	33,3	41,5	16,3	4,3	1,9	2,7
Höchster Abschluss	*Hauptschule*	*Realschule*	*Abitur*	*Ba-chelor*	*Master*	*Promot.*
Anzahl	7	49	128	40	33	1
Prozent	2,7	19,0	49,6	15,5	12,8	0,4
Soziales Netzwerk	*Facebook*	*Google+*	*Xing*	*andere*		
Anzahl	226	7	8	17		
Prozent	87,6	2,7	3,1	6,6		
Anzahl Kontakte	*< 50*	*50 - 99*	*100 - 199*	*200 - 500*	*> 500*	
Anzahl	41	52	72	79	14	
Prozent	15,9	20,2	27,9	30,6	5,4	
Nutzungsdauer in Jahren	*< 1*	*1 - 2*	*2 - 3*	*3 - 4*	*4 – 5*	*5 - 6*	*6 - 7*	*> 7*
Anzahl	11	15	45	53	50	35	25	24
Prozent	4,3	5,8	17,4	20,5	19,4	13,6	9,7	9,3
Angabe falscher Identifikation	*Nie*	*1% - 25%*	*26% - 50%*	*51% - 75%*	*> 75%*	
Anzahl	71	114	50	14	9	
Prozent	27,5	44,2	19,4	5,4	3,5	

5 Ergebnisse

Das Strukturgleichungsmodell wird mit Hilfe des PLS-Algorithmus geschätzt. Dazu haben wir Smart-PLS verwendet [10]. Die Ergebnisse sind in Abb. 3 dargestellt.

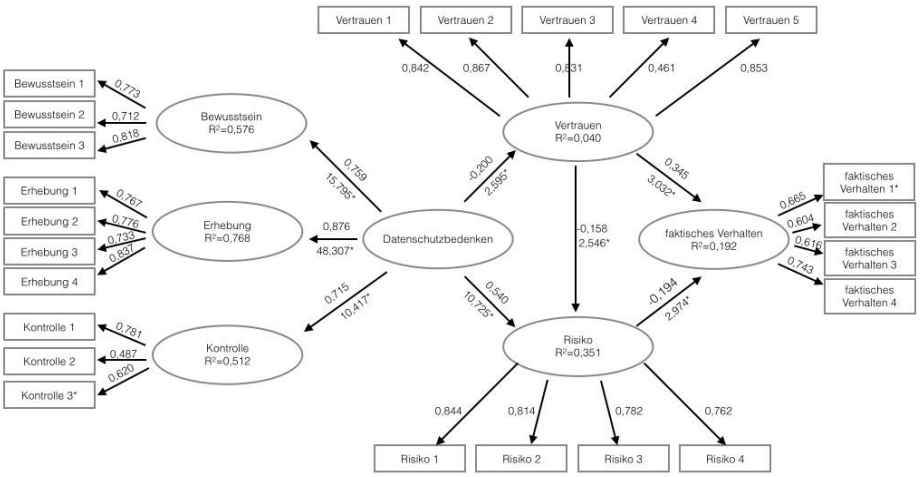


Abb. 3: Pfadkoeffizienten des Strukturgleichungs- und Messmodell (die zwei mit * gekennzeichneten Items werden in der Analyse ausgeschlossen)

5.1 **Evaluation der Modellgüte**

Für das PLS-Verfahren gibt es keine allgemeingültigen Kriterien zur Beurteilung der Modellgüte, weshalb analog zur Modellschätzung das innere und das äußere Modell getrennt voneinander zu beurteilen sind. Bei der Beurteilung der Modellgüte werden zuerst die Messmodelle überprüft. Anschließend wird auf dieser Grundlage das Strukturmodell und dessen Pfadbeziehungen getestet [9,14].

Evaluation der Messmodelle

Bei der Evaluation orientieren wir uns an dem von Weiber und Mühlhaus vorgeschlagenen Vorgehen [14]. Zunächst werden die Messmodelle auf ihre Güte überprüft, genauer die Reliabilität und Validität. Reliabilität ist die Zuverlässigkeit oder Genauigkeit eines Messinstruments und Validität ist das Ausmaß, mit dem ein Messinstrument auch das misst, was es messen sollte, also dessen Gültigkeit.

Zur Prüfung der Eindimensionalität wird die Explorative Faktorenanalyse (EFA) eingesetzt. Führt man die EFA mit Hilfe der Hauptachsenanalyse basierend auf der Promax Rotation für jedes Messmodell der ersten Generation durch, erhält man das Kaiser-Meyer-Olkin-(KMO) Maß der Stichprobeneignung von 0,51 für den Faktor „Kontrolle“, 0,64 für „Bewusstsein“ und 0,77 für „Erhebung“. Demnach ist der Indikatorsatz für den Faktor „Kontrolle“ nur eigeschränkt geeignet.

Ob die einzelnen Indikatoren für die EFA geeignet sind, lässt sich anhand der Measure of Sampling Adequacy (MSA) bewerten. Bei Werten kleiner als 0,5 werden einzelne Indikatoren ausgeschlossen. Sowohl die MSA als auch die Faktorladungen aller Indikatoren zeigen, dass diese mit Ausnahme eines Indikators des Faktors Kontrolle geeignet sind, die Faktoren zu beschreiben.

Der nächste Schritt der Reliabilitätsprüfung besteht in der gemeinsamen konfirmatorischen Faktorenanalyse (KFA) der Messmodelle. Hierfür wird erst die Eindimensionalität simultan über alle Konstrukte mit Hilfe der EFA betrachtet. Es wird festgestellt, dass der gemeinsame KMO (=0,84) größer als 0,7 ist und damit ein gutes Maß

der Stichprobeneignung liefert. Auch die Werte der MSA liegen für alle Indikatoren über dem Schwellenwert von 0,5.

In der KFA wird festgestellt, ob die Indikatoren und die Faktoren reliabel sind, und wie viel Prozent der Streuung eines latenten Konstrukts durchschnittlich über die Indikatoren erklärt werden kann. Ein Indikator ist reliabel, wenn seine Ladung auf den Faktor größer als 0,7 ist. Dies ist bei allen Indikatoren der Fall außer bei den Indikatoren „Kontrolle 2“, „Vertrauen 4“ und „faktisches Verhalten 2“.

Nach Prüfung der Reliabilität soll die Konvergenz-, Diskriminanz- und nomologische Validität untersucht werden [14]. Da in der Erhebung nur eine einzige Messmethode eingesetzt wurde, lässt sich die Konvergenzvalidität ausschließlich über die Faktorreliabilität ableiten, welche oberhalb des Schwellenwertes von DEV > 0,5 (extrahierte Varianz) liegt.

„Die Diskriminanzvalidität liegt vor, wenn sich die Messungen unterschiedlicher Konstrukte signifikant unterscheiden.“ [14] Dies erfolgt vor allem mit einem Vergleich der quadrierten Korrelation zu der DEV. Die quadrierte Korrelation wird auch als gemeinsame Varianz dieser Faktoren interpretiert und sollte in einem validen Fall größer sein als die DEV der jeweiligen Faktoren. Bei allen Konstrukten liegt die Diskriminanzvalidität vor.

Mit der nomologischen Validität werden die hypothetischen kausalen Beziehungen zwischen verschiedenen Konstrukten bestätigt. Da hier ein Strukturgleichungsmodell zweiter Ordnung gebildet wird, können die zu Anfang aufgestellten Hypothesen mit der „Datenschutz“-Variable zweiter Ordnung verglichen werden. Hierfür wird mit der KFA gezeigt, dass das Modell eine gute Anpassungsgüte besitzt. Dabei sollen die Regressionskoeffizienten zwischen den Konstrukten den Effekten aus den Hypothesen entsprechen. Dieser Schritt kann allerdings erst im Zusammenhang mit der Evaluation des Gesamtmodells festgestellt werden und wird daher zurückgestellt und im folgenden Kapitel wieder aufgegriffen.

Evaluation des Strukturmodells

Nachdem die Prüfung der Messmodelle abgeschlossen ist, wird nun auf die Prüfung des Struktur- und letztendlich auf die Prüfung des Gesamtmodells eingegangen.

Das Bestimmtheitsmaß R^2 und die signifikanten Pfadkoeffizienten sind die wichtigsten Punkte in der Beurteilung des inneren Modells. Mit der Bootstrapping-Methode wird die Signifikanz der Pfadkoeffizienten anhand von t-Werten überprüft [1].

Die Testhypothese, ob ein Parameter keinen gewichtigen Beitrag zur Bildung der Modellstruktur liefert, wird bei einem Wert kleiner als 1,96 verworfen, wenn eine Irrtumswahrscheinlichkeit von 5 Prozent zugelassen wird.

Tabelle 2: Bootstrapping-Methode zur Signifikanzbeurteilung der Pfadkoeffizienten

	Pfadkoeffizienten	*t-Werte*
Datenschutzbedenken → Bewusstsein	0,748	15,795
Datenschutzbedenken → Erhebung	0,886	48,307
Datenschutzbedenken → Kontrolle	0,605	10,417
Datenschutzbedenken → Risiko	0,535	10,725

Datenschutzbedenken → Vertrauen	-0,169	2,595
Risiko → Faktisches Verhalten	-0,206	2,974
Vertrauen → Faktisches Verhalten	0,221	3,032
Vertrauen → Risiko	-0,176	2,546
Schwellenwerte		> 1,96

Es weisen demnach alle Pfade signifikante t-Werte auf. Sie liefern einen signifikanten Beitrag zur Bildung der Modellstruktur. Alle Vorzeichen der Pfadkoeffizienten entsprechen den erwarteten Effektrichtungen aus den aufgestellten Hypothesen in Abbildung 2. Daraus resultiert eine hohe Anpassungsgüte, und die nomologische Validität aus dem vorhergegangenen Kapitel ist ebenfalls bestätigt.

Die Erklärungs- und Prognosekraft sowie die Robustheit eines PLS-Modells werden mit dem Bestimmtheitsmaß R^2 begründet. Da das R^2 den Anteil der erklären Varianz des latenten Konstrukts beschreibt, gibt es die Anpassungsgüte der Regressionsfunktion zu den empirisch gewonnenen manifesten Items an [1]. Dabei liefert ausschließlich die Variable „Erhebung" einen substantiellen Anteil, „Datenschutzbedenken", „Vertrauen" und „faktisches Verhalten" liefern leider nur einen sehr schwachen Anteil.

Des Weiteren kann mit der Blindfolding-Methode in SmartPLS die Prognoserelevanz reflektiv gemessener latent endogener Variablen bestimmt werden.

Die Prognoserelevanz wird anhand des Stone-Geisser-Kriteriums getestet. Es zeigt, wie gut das Modell und die PLS-Parameter die empirisch erhobenen Daten wiedergeben können. Die entsprechenden Werte weisen eine hinreichende Prognosefähigkeit auf.

5.2 **Interpretation**

Nachdem die Messmodelle und das Strukturmodell sowie das Gesamtmodell als akzeptabel eingestuft wurden, werden die Parameterschätzungen auf das Hypothesensystem abgeleitet.

Die Plausibilität und die Parameterbeurteilung werden in einem ersten Schritt interpretiert. Hierfür wurde bereits festgestellt, dass die Pfadkoeffizienten die gleichen Vorzeichen aufweisen, wie in den Hypothesen angenommen wurde. Die Faktorladungen sind allerdings nicht alle größer als 0,5 und weisen somit keine hinreichenden Werte auf.

Sind die Pfadkoeffizienten betragsmäßig größer als 0,2, so werden diese als bedeutungsvoll eingestuft [14]. In dieser Studie sind die beiden Pfade „Datenschutzbedenken → Vertrauen" und „Vertrauen → Risiko" demnach nicht bedeutungsvoll, da ihre Koeffizienten -0,17 und -0,18 betragen.

Die Prüfung der Kausalhypothesen und die Analyse kausaler Effekte ist ein weiterer Teil der Ergebnisinterpretation. Hier werden wieder die Vorzeichen der standardisierten Regressionsgewichte im Strukturmodell betrachtet. Wie auch schon bei der Plausibilitätsprüfung sind die beiden Pfade „Datenschutzbedenken → Vertrauen" und „Vertrauen → Risiko" auffällig. Betrachtet man die standardisierten multiplen Regressionsraten (R^2) so erklären die Variablen „Datenschutzbedenken", „Vertrauen" und „faktisches Verhalten" nur einen geringen Anteil der Varianz. Die Variablen

„Bewusstsein“, „Kontrolle“ und „Risiko“ weisen moderate R^2-Werte auf und „Erhebung“ erklärt 78 Prozent der Varianzen, was einem substantiellen Wert entspricht.

Die totalen Effekte setzen sich aus den direkten und den indirekten Effekten zusammen. Direkte Effekte liegen bei einer Beeinflussung vor, wenn ein Pfad zwischen den Konstrukten existiert. Indirekte Effekte existieren zwischen Konstrukten, wenn es keine direkte Verbindung zwischen ihnen gibt, sie aber über eine Zwischenvariable verbunden sind.

Neben den direkten Effekten (vgl. Pfadkoeffizienten) kann hier nur ein indirekter Effekt festgestellt werden: „Datenschutzbedenken → faktisches Verhalten“ beträgt -0,15. D.h., dass mit zunehmenden Datenschutzbedenken die Funktionalitäten zur Offenlegung von Informationen in OSN zurückhaltender genutzt werden.

Die Pfadkoeffizienten bestätigen die Erwartungen der Abhängigkeiten zwischen den vorgelagerten Konstrukten und den Datenschutzbedenken: Wenn der Umfang der erhobenen persönlichen Daten (*Erhebung*) steigt, wachsen auch die Angst vor einer Übervorteilung und damit die Datenschutzbedenken – oder der skizzierten Abhängigkeit folgend, sind erhöhte Datenschutzbedenken mit einem stärkeren Wunsch nach Einschränkung der erhobenen Daten verbunden. Wird dieser Wunsch nicht erfüllt, hat dies Einfluss auf den Umfang der Nutzung von OSN.

Analog dazu steigt mit den Datenschutzbedenken auch der Wunsch nach eigenen Kontrollmöglichkeiten Wenn der Nutzer von OSN über die Verwendung und Speicherung seiner Daten selbst bestimmen kann, ist dieser weniger besorgt über die Datenerhebung. Ist den Nutzern diese Kontrolle wichtig, sinken die Bedenken und die faktische Nutzung steigt.

Das Bewusstsein über die Datenschutzpraktiken des OSN beschreibt die Transparenz und wahrgenommene Fairness. Wenn Datenschutzrichtlinien dem Nutzer verständlich und fair angeboten werden, sinken die Datenschutzbedenken und die faktische Nutzung steigt ebenfalls.

Die Effekte die in diesem Strukturgleichungsmodell festgestellt wurden, stimmen demnach nicht nur mir den Hypothesen überein, sie sind vor allem mit dem praktischen Nutzungsverhalten in OSN erklärbar.

6 Vergleich des Strukturgleichungsmodells mit IUIPC

In diesem Kapitel wird das IUIPC Modell mit dem Modell dieser Studie verglichen. Interessant ist dies, da das IUIPC Modell zwar Grundlage der vorliegenden Studie ist, aber wichtige Unterschiede bestehen.

Neben einem Verzicht auf eine Mehrgruppenanalyse (Type of information requested) wurde ein anderer Ansatz zur Analyse benutzt: Malhotra et al. nutzten die LISREL-Software, welche einen kovarianzbasierten Schätz-algorithmus verwendet. Aus diesem Grund sind auch die Ergebnisse der beiden Analysen nur eingeschränkt vergleichbar. So ist es nur mit LISREL möglich, wahre Varianzen von Messfehlervarianzen zu unterscheiden [1].

Ein weiterer Unterschied zwischen den Modellen ist, dass Malhotra et al. die Verhaltensabsichten (Behavioral Intention) und diese Studie das faktische Verhalten betrachtet. Beide Studien belegen jedoch alle ihre Hypothesen: Die „Datenschutzbeden-

ken“ haben einen negativen Effekt auf das „Vertrauen“, und einen positiven Effekt auf das „Risiko“. Das „Vertrauen“ hat einen negativen Einfluss auf das „Risiko“. Außerdem hat das „Vertrauen“ einen positiven Effekt auf das „faktische Verhalten“ bzw. die „Verhaltensintention“, wogegen „Risiko“ einen negativen Einfluss auf das „Verhalten“ hat (Abb. 1).

Die Pfadkoeffizienten zwischen der „Datenschutzbedenken“-Variable zweiter Ordnung und den Variablen erster Ordnung sind bei Malhotra et al. in zwei Fällen („Kontrolle“ und „Bewusstsein“) stärker als in dieser Studie. Auch im Strukturmodell sind bei Malhotra et al. mehrere Beziehungen im Vergleich zu unserer Studie ausgeprägter. Dies betrifft die Pfadkoeffizienten: „Datenschutzbedenken → Vertrauen“, „Vertrauen → Risiko“ und „Risiko → faktisches Verhalten“ bzw. „Risiko → Verhaltensintention“.

7 Schlussbetrachtung

Diese Arbeit untersucht die Datenschutzbedenken der Nutzer von Sozialen Netzwerken. Das Ergebnis dieser Untersuchung ist nicht nur wichtig für Gesellschaft und Politik, welche über die Datenschutzrichtlinien entscheiden, sondern auch aus Sicht von Unternehmen, seien es werbetreibende Unternehmen oder die Betreiber von Sozialen Netzwerken. Sobald die Datenschutzbedenken bei den Nutzern geweckt sind und das Vertrauen zerstört ist, können sie keine Werbeeinnahmen von diesen Nutzern erwarten.

Obwohl die Nutzer durch Datenschutzgesetze geschützt werden sollen und ihnen ein Grundrecht auf informationelle Selbstbestimmung zusteht, haben die Sozialen Netzwerke rechtliche Hintertüren, um personenbezogene Daten erheben und speichern zu können.

7.1 Fazit der Untersuchung

Die Forschungsfrage ergründet den Einfluss von Datenschutzbedenken über die Variablen Vertrauen und Risiko und indirekt auf das faktische Verhalten in OSN. Die Strukturgleichungsmodellierung zeigt, dass die Datenschutzbedenken die Kontrolle, die Erhebung und das Bewusstsein positiv beeinflussen. Sie üben außerdem einen negativen Effekt auf das Vertrauen und einen positiven Effekt auf die Risikowahrnehmung aus. Das Vertrauen wiederum wirkt positiv auf das faktische Verhalten und das Risiko wirkt negativ auf das faktische Verhalten. Der indirekte Effekt zwischen den Datenschutzbedenken und dem faktischen Verhalten zeigt außerdem, dass bei einem Verzeichnen höherer Bedenken das faktische Verhalten verringert wird. Das bedeutet, dass Nutzer schlechter erreicht werden können.

Ähnliche Effekte sind neben dem Verhalten in Sozialen Netzwerken auch im Onlinehandel festzustellen. Die Effektstärke ist aufgrund der verschiedenen Modellbedingungen nicht unmittelbar vergleichbar, aber es ist zu sehen, dass die Wirkungsrichtungen der Pfade gleiche Effekte zeigen.

7.2 Grenzen und weitere Forschungen

Das Modell zeigt werbetreibenden Unternehmen und Betreibern von Sozialen Netzwerken, wie vorsichtig sie mit dem Vertrauen ihrer Nutzer umgehen müssen. Das

Vertrauen wird vor allem durch faire Erhebungspraktiken, große Kontrollmöglichkeiten und eine hohe Aufklärung über die Datenschutzpraktiken erreicht.

Das Modell weist jedoch an verschiedenen Stellen nicht akzeptable Güte-Kriterien auf. Zudem wurde es an verschiedenen Stellen im Vergleich zum IUIPC-Modell verändert. So bezieht diese Studie den Effekt von Datenschutzbedenken auf das tatsächliche Verhalten ein, wogegen Malhotra et al. den Einfluss auf die Verhaltensintention betrachten. Hier könnte man in einer weiteren Studie die tatsächlichen Nutzungsdaten von einem Sozialen Netzwerk wie Facebook einfügen, um das tatsächliche Verhalten als messbare manifeste Variable einzubinden. So bekommen Unternehmen ein noch besseres Werkzeug, mit dem sie feststellen können, wie groß ihr Spielraum in der Erhebung, Kontrollfreigabe und Aufklärung ihrer Datenschutzrichtlinien ist, um das tatsächliche Verhalten auszuweiten und die Streuverluste in der Werbeanzeigenauslieferung so gering wie möglich zu halten.

Anhang: Fragebogen

Erfahrungen mit Sozialen Netzwerken

(1) Welches Soziale Netzwerk nutzen Sie überwiegend?
(2) Wie viele Kontakte haben Sie in diesem Netzwerk?
(3) Wie lange nutzen Sie schon Soziale Netzwerke?

Kontrolle

(1) Im Vergleich zu meinen Freunden finde ich, dass die eigene Kontrolle persönlicher Informationen das Wichtigste in der Privatsphäre eines Users ist.
(2) Der Datenschutz gibt mir das Recht, meine persönlichen Informationen selbst zu kontrollieren und zu entscheiden, wie sie gesammelt, verwendet und weitergeteilt werden.
(3) Ich bin überzeugt davon, dass die Privatsphäre verletzt wird, wenn ich aufgrund einer Marketingaktion die Kontrolle über meine Daten teilweise oder komplett aufgeben musste.

Bewusstsein über Praktiken im Datenschutz

(1) Verglichen mit anderen bin ich stark davon überzeugt, dass Soziale Netzwerke immer bekanntgeben sollten, wie sie die Daten sammeln, bearbeiten und verwenden.
(2) Eine gute Datenschutzpolitik sollte eine eindeutige und unübersehbare Bekanntmachung zur Erhebung, Bearbeitung und Verwendung meiner Daten beinhalten.
(3) Es ist mir sehr wichtig, dass ich darüber informiert bin, wie meine persönlichen Informationen verwendet werden.

Erhebung

(1) Im Gegensatz zu anderen stört es mich normalerweise immer, wenn Soziale Netzwerke mehr Angaben über persönliche Informationen verlangen als nötig.
(2) Wenn Soziale Netzwerke persönliche Informationen abfragen, überlege ich manchmal zweimal, bevor ich diese angebe.
(3) Es stört mich, persönliche Informationen in mehreren verschiedenen Sozialen Netzwerken anzugeben.
(4) Ich bin besorgt, dass Soziale Netzwerke zu viele persönliche Informationen über mich sammeln.

Vertrauen

(1) Im Vergleich zu anderen finde ich, dass Soziale Netzwerke vertrauenswürdig im Umgang mit persönlichen Informationen sind.
(2) Soziale Netzwerke sagen die Wahrheit und erfüllen ihre Versprechen verbunden mit meinen persönlichen Informationen.
(3) Ich vertraue darauf, dass Soziale Netzwerke meine Informationen in meinem besten Interesse verwenden.

(4) Soziale Netzwerke sind generell berechenbar bezüglich der Verwendung meiner Informationen.
(5) Soziale Netzwerke sind immer ehrlich zu mir, wenn es um die Verwendung der Informationen geht, die ich dort angegeben habe.

Risiko

(1) Verglichen mit meinen Freunden bin ich eher der Meinung, dass es riskant ist, persönliche Informationen in Sozialen Netzwerken anzugeben.
(2) Man kann nur verlieren, sobald man seine Informationen in Sozialen Netz-werken angegeben hat.
(3) Es ist eine hohe Ungewissheit verbunden mit der Angabe von persönlichen Informationen.
(4) Die Angabe von Informationen in Sozialen Netzwerken bringt viele unerwartete Probleme mit sich.

Faktisches Verhalten

(1) Im Gegensatz zu meinen Freunden mache ich meine Posts immer für die gesamte Öffentlichkeit sichtbar, denn es ist mir egal, wer sie lesen kann.
(2) Wenn ich die Webseite des Sozialen Netzwerkes verlasse, bleibe ich immer mit meinem Benutzernamen eingeloggt.
(3) Ich nutze mobile Apps für ein schnelles Zugreifen auf mein Benutzerkonto in Sozialen Netzwerken und bin dort permanent eingeloggt.
(4) Bei bestimmten (unabhängigen) Anwendungen werden ebenfalls Benutzerkonten verlangt. Wenn möglich logge ich mich mit meinem bestehenden Konto aus Sozialen Netzwerken ein.

Angaben zur Person

(1) Geschlecht
(2) Alter
(3) Höchster Abschluss
(4) Angabe falscher Identifikationen: Soziale Netzwerke verlangen oftmals nach einer Registrierung mit persönlichen Informationen. Wie oft haben Sie schon falsche Informationen angegeben?
(5) Eindringen in die Privatsphäre: Wie oft wurde über Soziale Netzwerke in Ihre Privatsphäre eingedrungen?
(6) Enthüllungen: Wie oft haben Sie im letzten Jahr über die Verwendung und den potenziellen Missbrauch von Informationen in Sozialen Netzwerken gelesen?

Literaturverzeichnis

1. Bliemel, F., Eggert, A., Fassott, G., Henseler, J.: Handbuch PLS-Pfadmodellierung: Methode, Anwendung, Praxisbeispiele, Stuttgart (2005)
2. Bundesministerium der Justiz und für Verbraucherschutz: Bundesdaten-schutzgesetz, (1990), http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf (Zugriff 06.06.2014)
3. Culnan, M., Amstrong, P.: Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation In: Organization Science, 10(1) 104–115, (1999)
4. Fogel, J., Nehmad, E.: Internet social network communities: Risk taking, trust, and privacy concerns In: Computer in Human Behavior (25) 153–160, (2008)
5. Fuchs, C.: Facebook, Web 2.0 und ökonomische Überwachung In: Datenschutz und Datensicherheit, 34(7) 453–458 (2010)

6. Huber, F., Herrmann, A., Meyer, F., Vogel, J., Vollhardt, K.: Kausalmodellierung mit Partial Least Squares: eine anwendungsorientierte Einführung, Wiesbaden, (2007)
7. Leimeister, J. M., Zogaj, S.: Neue Arbeitsorganisation durch Crowdsourcing. Eine Literaturstudie In: Hans-Blöckler-Stiftung – Arbeitspapier 287, Düsseldorf (2013) http://pubs.wi-kassel.de/wp-content/uploads/2013/10/JML_443.pdf
8. Malhotra, N., Kim, S., Agarwal, J.: Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model In: Information Systems Research, Reihe ABI/INFORM Global, 15(4) 336–355, (2004)
9. Nitzl, C.: Eine anwendungsorientierte Einführung in die Partial Least Square (PLS)-Methode, (2010)
10. Ringle, C., Wende, S., Becker, J.: SmartPLS 3. Hamburg: SmartPLS. (2014) Retrieved from http://www.smartpls.com
11. Sjurts, I.: Gabler Lexikon Medienwirtschaft, (2011) http://link.springer.com/book/10.1007/978-3-8349-6487-8 (Accessed 27.06.2014)
12. United States Securities and Exchange Commition: Annual report pursuant to section 13 or 15(d) of the securities exchange act of 1934 - Facebook Inc., Washington D.C., (2013) http://investor.fb.com/annuals.cfm (Accessed 05.07.2014)
13. Wang, H., Lee, M., Wang, C.: Consumer Privacy Concerns about Internet Marketing In: Communication of the ACM 41(3) 63–70 (1998)
14. Weiber, R., Mühlhaus, D.: Strukturgleichungsmodellierung: eine anwendungsorientierte Einführung in die Kausalanalyse mit Hilfe von AMOS, SmartPLS und SPSS, Heidelberg, 2. Ausgabe, (2014)
15. Young, A., Quan-Haase, A.: Information Revelation and Internet Privacy Concerns on Social Netzwork Sites: A Case Study of Facebook In: Proceedings of the fourth international conference on Communities and technologies, 265-274 (2009)
16. Acquisti, A., Varian, H. R.: Conditioning prices on purchase history. Marketing Science, 24(3) 367–381 (2005)