Privatsphäre im Internet

Sabine Trepte & Tobias Dienlin

Die Ära der Privatsphäre ist abgelaufen, das Zeitalter der Post-Privacy hat begonnen. Würde man den Anhängern dieses Axioms – beispielsweise Christian Heller (2011) oder Jeff Jarvis (2011) – bedingungslos folgen, dann müssten wir das Kapitel Privatsphäre im Internet bereits an dieser Stelle beenden. Dass die Angelegenheit scheinbar doch nicht so eindeutig ist, lässt sich beispielsweise anhand des Bandes „Privacy Online“ (Trepte & Reinecke, 2011b) erkennen: Kein einziger der einunddreißig beteiligten Wissenschaftler kommt zu derselben Einschätzung des aktuellen Status von Privatsphäre wie Heller oder Jarvis. Vielmehr zeigt die aktuelle Forschungslage, dass Privatsphäre ein sehr dynamisches und vielschichtiges Konzept ist, das eine differenziertere Betrachtung erfordert. In diesem Sinne werden wir im vorliegenden Kapitel das Phänomen Privatsphäre grundlegend betrachten, aktuelle Forschungsergebnisse präsentieren und eine abschließende Bewertung vornehmen.

Viele Menschen, Parteien und Unternehmen sprechen über Privatsphäre, viele Menschen haben dementsprechend auch eine ganz eigene und unterschiedliche Vorstellung von Privatsphäre. Aufgrund dieser Begebenheit beginnen wir im ersten Abschnitt anhand ausgewählter Forschungsarbeiten mit einer Definition von Privatsphäre. Privatsphäre im Online-Bereich ist keine neue psychologische Variable, kein revolutionärer Prozess, sondern ein klassischer psychologischer Vorgang, der sich nun im Online-Kontext in einem neuen strukturellen Rahmen entfaltet. Dementsprechend werden wir im ersten Abschnitt das Phänomen Privatsphäre ganz allgemein darlegen. Im nächsten Abschnitt werden wir daraufhin den Blick auf die Privatsphäre im Internet erweitern: Warum genau ist in den letzten Jahren die Thematik der Privatsphäre im Internet überhaupt so relevant geworden? Welche Besonderheiten bringt die Privatsphäre im Kontext Internet mit sich? Im darauf folgenden Abschnitt beleuchten wir mit Schwerpunktlegung auf aktuelle Forschungsergebnisse den Umgang mit und die Gestaltung von Privatsphäremaßnahmen, die Nutzer im Internet konkret umsetzen. Im anschließenden Abschnitt werden wir eine Evaluation der aktuellen Situation vornehmen und konkrete Vorschläge zur eigenen Privatsphäregestaltung anbieten. Mit einer Zusammenfassung im letzten Abschnitt schließen wir das Kapitel.

Was ist Privatsphäre?

Bevor wir Privatsphäre in seinen Bestandteilen definieren, stellen wir folgende Bemerkung voran, die in den allgemeinen Medien und in populärwissenschaftlichen Betrachtungen oftmals nicht beachtet wird: Privatsphäre ist in der wissenschaftlichen Prüfung in erster Instanz immer neutral und wertfrei zu definieren. Privatsphäre ist ein Zustand oder Prozess und kein Wert. Erst in einem zweiten Schritt kann eine Ausprägung oder Veränderung der Privatsphäre – in Form einer Zu- oder Abnahme – im jeweiligen Kontext interpretiert und bewertet werden. Bereits im Jahre 1980 hielt Ruth Gavison diesen Ansatz wie folgt fest: "First, we must have a neutral concept of privacy that will enable us to identify when a loss of privacy has occurred so that discussions of privacy and claims of privacy can be intelligible. Second, privacy must have coherence as a value, for claims of legal protection of privacy are compelling only if losses of privacy are sometimes undesirable and if those losses are undesirable for similar reasons" (Gavison, 1980, S. 423).
In diesem Sinne ergeben sich zwei Ansätze (vgl. Nissenbaum, 2010): zum einen der deskriptive (definierende), und zum anderen der normative (regulierende). Beispielhaft lassen sich beide wie folgt illustrieren: „Auf Facebook nimmt die Privatsphäre ab" entspricht dem deskriptiven Ansatz, „Auf Facebook ist die Privatsphäre bedroht" spiegelt den normativen Ansatz wider. In diesem Kapitel werden wir in den ersten drei Abschnitten einen deskriptiven Ansatz verwenden und abschließend im vierten Abschnitt in unserer Evaluation des aktuellen Zustandes eine normative Vorgehensweise anwenden.

Viele verschiedene Ansätze zur Definition von Privatsphäre liegen mittlerweile vor (Altman, 1975; Burgoon, 1982; Gavison, 1980; Petronio, 2002; Warren & Brandeis, 1890; Westman & Eden, 1997). Eine Definition von Privatsphäre ist nicht unmittelbar offensichtlich und führt dementsprechend oft zu uneinheitlichen Ergebnissen (Margulis, 2011). Pointiert umschreibt Helen Nissenbaum (2010) die Situation wie folgt: „One point on which there seems to be near-unanimous agreement is that privacy is a messy and complex subject" (S. 67). Nichtsdestoweniger lassen sich drei zentrale Konzepte ausfindig machen, die sowohl dem Zahn der Zeit als auch der empirischen Überprüfung stand gehalten haben: Als erstes der Ansatz von Westin (1967), der Privatsphäre in verschiedene Zustände unterteilt; als zweites die Arbeiten von Altman (1975), der Privatsphäre als Regulationsprozess versteht; als drittes die Definition nach Burgoon (1982), in der sie Privatsphäre in vier verschiedene Dimensionen einteilt. Gerade die ersten beiden Ansätze teilen viele Gemeinsamkeiten (Margulis, 2011)

und lassen sich gut mit den Dimensionen von Burgoon (1982) erweitern. Im Folgenden werden wir diese Definitionen kurz einzeln darstellen. Anschließend diskutieren wir das Privatsphäre-Prozess-Modell (Dienlin, in Vorbereitung), welches Aspekte der genannten Definitionen aufgreift und modelliert.

Welche bekannten und bewährten Definitionen von Privatsphäre gibt es?

Westin (1967) definiert Privatsphäre wie folgt: „Privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means" (S. 7). Es resultieren vier verschiedene Zustände: die Einsamkeit (Freiheit von Beobachtung durch andere), Intimität (Freiheit für persönliche Beziehungsgestaltung), Anonymität (Freiheit von Identifikation) und die Zurückgezogenheit (Limitierung der Selbstoffenbarung). Westin skizziert somit einen klassischen Ansatz, der Privatsphäre in verschiedene Aggregatszustände unterteilt. Wichtig ist zu betonen, dass Privatsphäre gemäß Westin vor allem ein Rückzugsprozess aus gesellschaftlichen Interaktionen ist.

Die Definition von Altman (1975) deckt sich zu großen Teilen mit der Westins (1967), erweitert den Ansatz aber um einen entscheidenden Punkt: Aus der sozialpsychologischen Schule kommend, legt Altman Gewicht auf die Betonung des Prozesses der dialektischen und dynamischen Regulation von Privatsphäre. Demgemäß sind nicht gewisse und absolute Zustände der Privatsphäre das erklärte Ziel, sondern die Möglichkeit, Privatsphäre situationsspezifisch auf ein optimales Maß regulieren zu können. Privatsphäre verhält sich folglich wie ein Thermostat: Wird in einem ersten Schritt der Privatsphärebewertung ein Zuviel an Privatsphäre festgestellt, erfolgt in einem zweiten Schritt der Privatsphäreregulation ein Öffnen von Grenzen und Weitergeben von Informationen; hieraus resultiert wiederum ein angenehmes Maß an Privatsphäre. Der Umkehrschluss gilt ebenso: Ein Zuwenig an Privatsphäre kann durch einen selektiven Rückzug und das Behalten von Informationen erfolgreich hinauf adjustiert werden. Dies lässt sich gut an einem alltäglichen Beispiel nachvollziehen. Stellen wir uns vor, wir befinden uns auf der Geburtstagsfeier eines Freundes. Eine unbekannte Person erblickt uns, nähert sich rasch, kommt uns in einer elanvollen Begrüßung sehr nahe. Wir werden diese Nähe höchstwahrscheinlich als unangenehm bewerten und unwillkürlich einen kleinen Schritt zurückweichen. Wir haben unmittelbar unsere Privatsphäre reguliert, haben etwas mehr Distanz hergestellt und damit unser eigenes Wohlbefinden verbessert. Dass physische Nähe

als genereller Zustand natürlich nicht grundsätzlich schlecht ist, wird spätestens dann deutlich, wenn wir auf derselben Party einen alten Freund nach langer Zeit voll Freude innig in die Arme schließen. Wichtig ist gemäß Altman darüber hinaus, dass Menschen überhaupt von der Möglichkeit Gebrauch machen, ihre Privatsphäre zu regulieren. Dies dient dem Zweck, den gewünschten Zustand der Privatsphäre und damit gleichzeitig Wohlbefinden herzustellen. Veranschaulicht wurde dieses Prinzip in einer wegweisenden Studie von Vinsel, Brown, Altman und Foss (1980). Studenten, die während eines Jahres an der Universität ihre Privatsphäre willkürlich regulierten – beispielsweise in dem sie ihre Tür entweder öffneten oder schlossen, zum Lernen entweder einen belebten oder einen ruhigen Raum bewusst aufsuchten – zeigten eine höhere Wahrscheinlichkeit, das erste Studienjahr auch erfolgreich abzuschließen.

Der nächste entscheidende Schritt in der Definition von Privatsphäre wurde durch Judee Burgoon (1982) erreicht. Burgoon erkannte in einer Meta-Analyse bis dato publizierter Abhandlungen über Privatsphäre, dass sich vier verschiedene Bereiche (Dimensionen) der Privatsphäre unterscheiden lassen: (1) informationale Privatsphäre, welche die Kontrolle über die Erhebung der über einen selbst gesammelten Daten umfasst; (2) soziale Privatsphäre, welche die Kontrolle darüber beschreibt, mit welchen Personen man kommuniziert; (3) psychische Privatsphäre, welche die Kontrolle der inhaltlichen Tiefe und des Selbstoffenbarungsgrades von Kommunikation beinhaltet und (4) physische Privatsphäre, welche definiert, inwiefern der territoriale Zugang zu der eigenen Person kontrolliert wird, z. B. der Zugang in ein Land, in eine Straße, in eine Wohnung und die Berührung des Körpers einer Person. Gemäß Burgoon (1982) geht es innerhalb der Dimensionen vor allem um die Kontrollmöglichkeit der Privatsphäre – sobald sie sich kontrollieren lässt, ist die Privatsphäre hoch, sobald keine Freiheit der Kontrolle vorliegt, ist sie niedrig. Es lässt sich gut nachvollziehen, dass bei unserem Geburtstagsfeier-Beispiel das Zurückweichen während der Begrüßung den Bereich der physischen Privatsphäre betrifft. Ein Beispiel für die psychische Privatsphäre wäre der Inhalt eines möglichen Gespräches mit der Person. Da wir die Person nicht kennen, werden wir sehr wahrscheinlich nur über unpersönliche Dinge wie das Wetter sprechen können. Dementsprechend läge eine niedrige psychische Privatsphäre vor. Würden wir die Person hingegen schon lange kennen, könnten wir auch über persönliche Ansichten, unsere Gefühle oder unsere Meinung zum Gastgeber sprechen. Kommen wir zur sozialen Privatsphäre: Bezogen auf unser Beispiel der

Geburtstagsfeier ist man in der Wahl seines Gesprächspartners in der Regel frei, weswegen eine hohe soziale Privatsphäre vorliegt. Anders sieht dies bei einem offiziellen Empfang aus: Hier ist man oftmals dazu verpflichtet ist, mit bestimmten Personen formale Gespräche zu führen – folglich liegt hier eine geringere soziale Privatsphäre vor. In sämtlichen Situationen, in denen Menschen überwacht werden oder Verhalten protokolliert wird, und sie diesen Zustand nicht verändern können, liegt eine niedrige informationale Privatsphäre vor. Dies betrifft beispielsweise die Bewohner von Pflegeheimen, über die viele Informationen (z. B. Krankenakten) gesammelt werden. In privaten Räumen hingegen kann gemeinhin von einer höheren informationalen Privatsphäre ausgegangen werden. Die Tatsache, dass diese vier postulierten Dimensionen einer Meta-Analyse und nicht einer einzelnen theoretischen Abhandlung Burgoons entspringen, führt unter anderem dazu, dass die Dimensionen sehr zeitlos sind. Gleichzeitig sind sie auch flexibel genug, um sie auf das heutige Internetzeitalter übertragen zu können.

Ursprünglich haben alle drei Definitionen den Anspruch, Privatsphäre vollständig zu erklären, die genannten drei Ansätze thematisieren neben den hier ausgeführten Kernaussagen noch viele weitere wichtige Aspekte. Jeder Ansatz hat einzeln gesehen Vor- und Nachteile, in der Summe betrachtet ergibt sich allerdings folgendes stimmiges Bild: Privatsphäre ist ein individueller Zustand (Westin, 1967) sowie ein Prozess, der einer stetigen Regulierung von Zuviel und Zuwenig Privatsphäre unterliegt (Altman, 1975), wobei sich zu jedem Zeitpunkt vier verschiedene Privatsphäredimensionen unterscheiden lassen: informationale, soziale, psychische und physische Privatsphäre (Burgoon, 1982). Um diese Erkenntnisse zu integrieren und um Privatsphäre in seiner vollständigen Funktionsweise abzubilden, stellen wir im Folgenden das Privatsphäre-Prozess-Modell vor.

Das Privatsphäre-Prozess-Modell

Aus den bisher genannten Arbeiten lassen sich wie bereits dargelegt die Gegebenheit eines Privatsphärezustandes, der Prozess der Privatsphäreregulation sowie die Unterscheidung in die vier Dimensionen (informational, sozial, psychisch, physisch) extrahieren. In dem Privatsphäre-Prozess-Modell (Dienlin, 2013; siehe Abbildung 1) werden diese Aspekte in einem einzelnen Modell gemeinsam abgebildet und zueinander in Beziehung gesetzt. Das Modell berücksichtigt, dass sich die Variablen in einer zeitlichen Abfolge zueinander befinden – dies zielt darauf ab, den dynamischen Anteilen der Privatsphäre Rechnung zu

tragen. Der Privatsphärezustand wird hierzu im Privatsphäre-Prozess-Modell in die Elemente des Privatsphärekontextes, der Privatsphärewahrnehmung und des Privatsphäreverhaltens ausdifferenziert. Demgemäß führt eine gegebene Situation (Privatsphärekontext) im ersten Schritt zu einer bestimmten Empfindung an Intimität und Vertrautheit (Privatsphärewahrnehmung), welches den Grad einer darauf folgenden möglichen Selbstoffenbarung (Privatsphäreverhalten) bedingt. Diese zeitliche Abfolge ist das erste zentrale Prozessmerkmal und wird als Privatsphäreprozess bezeichnet.

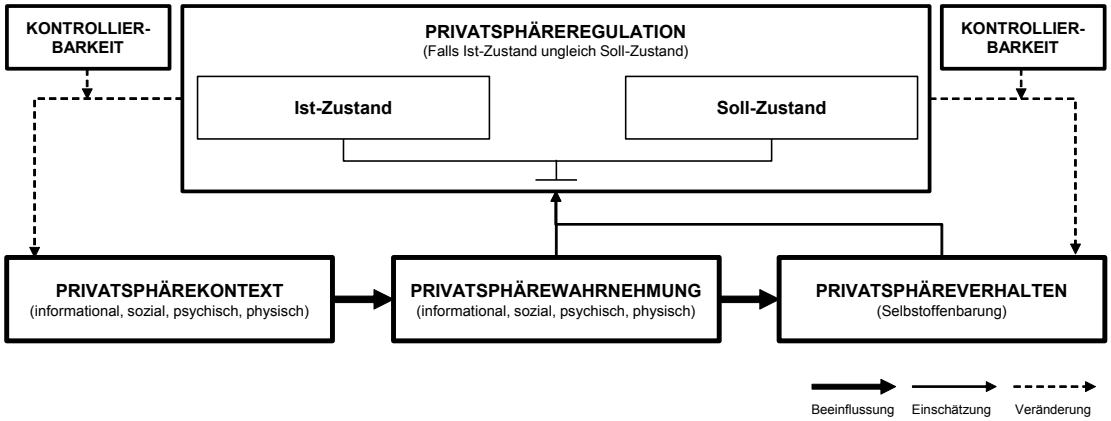

Abbildung 1: Das Privatsphäre-Prozess-Modell

Im Folgenden gehen wir kurz auf die einzelnen Elemente ein: Der Privatsphärekontext entspricht einer objektiven Erfassung der Situation, in der sich Menschen augenblicklich befinden. Als Privatsphärekontext bezeichnen wir den situativen Rahmen, innerhalb dessen man sich bewegt, kommuniziert und interagiert. Als objektiv soll der Privatsphärekontext bezeichnet werden, um zu verdeutlichen, dass die Wahrnehmung der Situation interindividuell unterschiedlich ist. Der Privatsphärekontext kann dementsprechend beispielsweise eine Familienfeier, ein Geschäftsessen oder auch die Situation einer Beichte in der Kirche sein. Gleichzeitig lässt sich der Privatsphärekontext auf die digitale Welt von Twitter, einer Facebook-Gruppe oder einem öffentlichen Forum übertragen. Der Privatsphärekontext ist folglich als Disposition gegeben. Der Privatsphärekontext wird in die vier Dimensionen des informationalen, sozialen, psychischen und physischen Privatsphärekontextes unterschieden. Die Dimensionen sind dabei weitgehend unabhängig voneinander. So gibt es Kontexte, in denen gleichzeitig eine niedrige informationale und psychische Privatsphäre, dafür eine hohe soziale und physische Privatsphäre vorherrschen.

Innerhalb des Privatsphärekontextes und auch aufgrund des Privatsphärekontextes entwickeln Menschen daraufhin eine Privatsphärewahrnehmung. Die Privatsphärewahrnehmung beschreibt somit die subjektive Empfindung der individuellen, persönlichen Privatsphäre. Allgemein betrachtet ist die Privatsphärewahrnehmung der wichtigste Bestandteil von Privatsphäre: Fragt man, was genau Privatsphäre ist, so meint dies vor allem die individuelle Wahrnehmung, inwiefern sich Menschen frei von Überwachung fühlen (informationale Privatsphäre), wie viele andere und welche Menschen sie in ihrer Umgebung wahrnehmen (soziale Privatsphäre), ob in der jeweiligen Situation eher Persönliches oder Unpersönliches mitgeteilt wird (psychische Privatsphäre), und wie stark sie sich territorial abgegrenzt fühlen (physische Privatsphäre). Dass die Unterscheidung in Privatsphärekontext und Privatsphärewahrnehmung nicht redundant ist, lässt sich an folgendem Beispiel illustrieren: Ein Unternehmer lädt seinen Geschäftspartner zu einem vertraulichen Gespräch persönlich in sein Büro ein. Der Eingeladene wird sehr wahrscheinlich eine hohe informationale Privatsphäre wahrnehmen. Wird das Gespräch dabei in ungeahnter Weise mit einer Videokamera gefilmt, so liegt demgegenüber objektiv ein niedriger informationaler Privatsphärekontext vor. Die Berücksichtigung der Privatsphärewahrnehmung erscheint folglich wichtig, um Verhalten von Menschen erklären zu können – gerade im Bereich der Nutzung von Social Networking Sites (SNS) ist hier eine Divergenz von dem gegebenen, objektiven Privatsphärekontext und der subjektiven Privatsphärewahrnehmung zu beobachten.

Unter Privatsphäreverhaltensweisen verstehen wir sämtliche Vorgänge, die eine Selbstoffenbarung beinhalten. Wheeles und Grotz (1976) definieren Selbstoffenbarung wie folgt: „a self-disclosure is any message about the self that a person communicates to another. Consequently, any messages or message unit may potentially vary in the degree of self-disclosure present depending upon the perception of the message by those involved“ (S. 338). Hierunter fallen also unter anderem das Erzählen von persönlichen Erlebnissen, aber auch das Posten einer Statusmitteilung auf SNSs. Studien zeigen, dass sich gerade bei hoher Privatsphäre Menschen anderen viel von sich preisgeben (Trepte, 2012). In privaten Räumen haben Menschen die Möglichkeit, sich auszuprobieren, unsichere Ansichten zu äußern und zu hinterfragen, erfinderisch zu sein und kreativ zu werden (Margulis, 2003). Dies zeigt, dass die Selbstoffenbarung somit eine direkte Funktion von Privatsphäre sein kann (Derlega & Chaikin, 1977).

Wie bereits erwähnt, eruieren Menschen durchgängig, automatisch und meist unbewusst, ob ihr derzeitiger Ist-Zustand an Privatsphäre auch dem Soll-Zustand entspricht. Sobald ein spezifischer Ist-Zustand der Privatsphärewahrnehmung oder des Privatsphäreverhaltens von dem gewünschten Soll-Zustand abweicht, steigt die Wahrscheinlichkeit einer Privatsphäreregulation. Hierzu werden – je nach Möglichkeit und Kontrollierbarkeit – entweder das Privatsphäreverhalten oder der Privatsphärekontext aktiv verändert. Betrachten wir einmal das Privatsphäreverhalten: Ein Mitarbeiter streift im Gespräch mit seinem Vorgesetzten mehr oder weniger zufällig den Themenbereich schwerwiegender Krankheiten. Der Mitarbeiter wird überprüfen, ob ein solches Thema hinsichtlich des damit verbundenen Intimitätsgrades – also dem Ausmaß seiner Selbstoffenbarung – einem gewünschten und vertretbaren Soll-Wert entspricht. Dieser Vergleich hat zwei potenzielle Ergebnisse: Entspricht der Ist-Zustand dem Soll-Zustand, bleibt das Verhalten unverändert. Liegt allerdings ein Ungleichgewicht vor, erfolgt die Privatsphäreregulation. Diese Regulation kann entweder in Form einer Veränderung des Privatsphäreverhaltens oder des Privatsphärekontextes geschehen. Bei unserem Beispiel bleibend würde der Mitarbeiter – falls er seine Selbstoffenbarung als zu hoch empfindet – das Gespräch daraufhin wahrscheinlich auf ein neutraleres Thema lenken, also sein Privatsphäreverhalten regulieren. Im Gesamten betrachtet ist der Vorgang der Privatsphäreregulation das zweite zentrale Prozessmerkmal des Privatsphäre-Prozess-Modells. Zum Gestalten von Privatsphäre führen Menschen ein ständiges Adjustieren von Verhaltensweisen und ein selektives Anpassen von Kontextvariablen durch. Aus dieser Begebenheit resultiert im Umkehrschluss ein entscheidendes Moment: Damit der Prozess der Privatsphäregestaltung überhaupt von statten gehen kann, muss die Kontrollierbarkeit des Verhaltens oder des Kontextes notwendigerweise gewährleistet sein.

Eingangs erwähnten wir, dass im ersten Schritt eine deskriptive Betrachtung von Privatsphäre einer normativen vorzuziehen ist. Übertragen auf das Privatsphäre-Prozess-Modell bedeutet dies, dass keine allgemein geltenden Soll-Zustände für erstrebenswertes Privatsphäreverhalten zu artikulieren sind. Beispielsweise wird häufig in populären Medien ein restriktiveres Selbstoffenbarungsverhalten auf SNSs gefordert. Das Setzen von allgemein gültigen Vorgaben erscheint hier schwierig; beispielsweise zeigen Studien, dass Selbstoffenbarung auf SNSs sogar eher mit erhöhten Werten an Wohlbefinden und positiver Gefühlslage einhergehen (Trepte & Dienlin, 2013). Wichtig erscheint vor allem, dass der Ist-

Zustand des subjektiven Privatsphäreverhaltens so nahe wie möglich am gewünschten Soll-Zustand liegt. Um dies zu erreichen, muss die Kontrollierbarkeit des Privatsphärekontextes und des Privatsphäreverhalten gewährleistet sein. Zusammenfassend lassen sich die Aussagen des Privatsphäre-Prozess-Modell in sieben Axiomen fassen:

1. Eine gegebene, objektive Situation (Privatsphärekontext) führt zu einer bestimmten Wahrnehmung der Intimität und Vertrautheit (Privatsphärewahrnehmung).
2. Resultierend aus der Privatsphärewahrnehmung zeigen Menschen unterschiedliche Ausmaße an Selbstoffenbarung (Privatsphäreverhalten). Die ersten beiden Axiome beschreiben den sogenannten Privatsphäreprozess.
3. Bei dem Privatsphärekontext und der Privatsphärewahrnehmung werden informationale, soziale, psychische und physische Dimensionen unterschieden.
4. Für die beiden Elemente der Privatsphärewahrnehmung und des Privatsphäreverhaltens lassen sich ein wahrgenommener Ist-Zustand und ein erstrebenswerter Soll-Zustand differenzieren.
5. Sobald eine Diskrepanz zwischen Ist-Zustand und Soll-Zustand vorliegt, wird eine Privatsphäreregulation angestrebt. Hierfür werden entweder der Privatsphärekontext oder das Privatsphäreverhalten angepasst.
6. Damit eine Privatsphäreregulation vonstattengehen kann, bedarf es der Kontrollierbarkeit entweder des Privatsphärekontextes oder des Privatsphäreverhaltens.
7. Die Ausprägungen sämtlicher Elemente sollten zuerst deskriptiv (und nicht normativ) betrachtet werden.

Das Privatsphäre-Prozess-Modell setzt somit bekannte Definitionen, Aspekte und Wirkmechanismen von Privatsphäre miteinander in Verbindung, differenziert drei verschiedene Privatsphäreelemente und konzeptualisiert den durchgängigen Prozesscharakter von Privatsphäre.

Warum ist Privatsphäre im Internet relevant?

Naturgemäß stellt sich die Frage: Wie kann es sein, dass der Privatsphäre derzeit eine so große Bedeutung zugemessen wird? Auch wenn im Zuge des Privatsphärediskurses durchaus vielfältige und unterschiedliche Aspekte adressiert werden, so liegt das Hauptaugenmerk auf der Privatsphäre im Internet – beispielhaft wird Google oftmals als Datenkrake skizziert

(Reißmann, 2010), oder Facebook als profitorientierter Privatsphärenverweigerer wahrgenommen (Lindner, 2010). Dass diese Aussagen in den letzten Jahren virulent wurden, ist vor allem einer simplen, aber tiefgreifenden Tatsache geschuldet: Ein massiver Anteil regulärer alltäglicher Vorgänge verlagerte sich langsam aber sicher in das World Wide Web. Mit Facebook entstand ein neues Medium für Kommunikation, mit Amazon eine neue Form des Einkaufens. Den meisten revolutionären Neuerungen gemein ist die Tatsache, dass altbekannte Prozesse in neue Strukturen gebettet werden, die daraufhin eigene Charakteristika mit sich bringen. Facebook macht die Interaktion unabhängig von zeitlichen und räumlichen Bedingungen und damit frei von der Notwendigkeit des synchronen Kommunizierens, Amazon stellt Waren aller Art nun rund um die Uhr und nur einen Mausklick entfernt zum Kauf bereit. Veränderungen wirken ferner auf den eigentlichen Prozess zurück und konstituieren diesen neu. Entfernte Verwandte müssen nicht mehr besucht werden, es kann zu selbstgewählten Zeiten kommuniziert werden, Bücher können noch nach Ladenschluss vom Arbeitsplatz aus bequem bestellt werden.

Es ist an dieser Stelle ratsam, sich die neuen Strukturen, die durch das Internet generiert und geprägt wurden, einmal genauer zu betrachten. Im ersten Schritt analysieren wir Strukturen, die das Internet ganz allgemein kennzeichnen. Im zweiten fokussieren wir daraufhin konkrete, spezifische Angebote des Internets. Im dritten Schritt werden wir anhand des Privatsphäre-Prozess-Modells untersuchen, inwiefern diese Strukturveränderungen schlussendlich den Bereich der Privatsphäre tangieren.

Welche neuen Strukturen bringt das Internet generell mit sich?

danah boyd (2008b) klassifiziert folgende vier Strukturen der digitalen Kommunikation: (1) Persistenz, (2) Replizierbarkeit, (3) Skalierbarkeit und (4) Durchsuchbarkeit. Persistenz meint, dass das Internet nie vergisst. Das Vergreifen im Ton ist in einer analogen Kommunikation nur für den Moment verletzend, aber meist schnell vergessen und verziehen. Das sinnbildliche Vergreifen auf der Tastatur kann allerdings noch Jahre später wortwörtlich rezipiert werden und damit stets neu emotionale Reaktionen, wie Kummer oder Freude, erzeugen. Persistenz gilt nicht nur für die geschriebene Kommunikation, sondern genauso auch für Bilder, Videoaufnahmen, Forenbeiträge, usw. Was heute adäquat erscheint, kann morgen im besten Fall peinlich und im schlimmsten Fall rufschädigend sein. Eine weitere Struktur ist die Replizierbarkeit von Informationen. Mittels Copy-and-Paste können Texte,

Bilder und mit etwas mehr Aufwand auch Videos leicht vervielfältigt werden. Sobald eine beliebige digitale Information den nur bedingt geschützten Rahmen einer privaten Kommunikation verlässt, öffentlich abrufbar und an anderer Stelle replizierbar wird, ist der Umlauf nicht mehr zu kontrollieren. Skalierbarkeit meint, dass die Verbreitung von Inhalten andere als die intendierten Ausprägungen und Maßstäbe erreichen kann. Sobald eine Information virulent wird, können leicht tausende Kontaktpunkte zu ihr generiert werden. Ein bekanntes Beispiel hierfür ist das Phänomen der Facebook-Partys, bei denen virtuelle Einladungen schnell die Runde machen, innerhalb kurzer Zeit große Menschenmassen zueinander finden und schlussendlich oftmals auch aneinander geraten. Zuletzt nennt boyd (2008b) das Prinzip der Durchsuchbarkeit. Es beschreibt die Tatsache, dass kommunizierte Informationen von Suchmaschinen erfasst und somit für andere Nutzer auch potenziell zugänglich gemacht werden können. Jeder Arbeitnehmer hat die Möglichkeit, den Namen des Bewerbers in eine Suchmaschine einzugeben und sich damit dezentral verteilte Informationen zentral gesammelt zugänglich zu machen.

Neben den vier genannten Strukturen von boyd (2008b) gibt es zahlreiche weitere Aspekte, die alltägliche Begebenheiten verändert haben (vergleiche Kapitel 6 aus diesem Band zum Thema Cybermobbing). Zuletzt und beispielhaft sei an dieser Stelle noch das Anlegen von sogenannten Cookies genannt: Cookies sind lokale Speichereinheiten, die Eingaben von Nutzern ablegen und damit ein individualisiertes Browsen ermöglichen. Passwörter oder Adresseingaben können so gemerkt, häufige Suchanfragen gespeichert werden. Vielfach sind sich Nutzer der Existenz dieser Cookies nicht bewusst, da sie latent und unbemerkt angelegt werden. Facebook nutzt beispielsweise den sogenannten Social Graph: dieser ermöglicht Facebook, auf externen Seiten, die auf Facebook verweisen (beispielsweise über den Like-Button), Informationen der Freundesliste des Nutzers zu extrahieren und auf der externen Seite darzustellen. Somit kann Facebook Protokolle von Nutzern erstellen, welche Seiten sie wie lange besucht haben. Indirekt können auf diese Weise über Cookies Nutzungsprofile von Menschen angelegt und gepflegt werden, so denn Nutzer nicht die Funktion der Cookies deaktivieren oder den Speicher regelmäßig löschen. Anhand der genannten Beispiele wird ersichtlich, dass vielfältige Aspekte der individuellen Privatsphäre allein durch die allgemeinen Strukturen des Internets tangiert werden. Im Folgenden werden nun spezifische Angebote des Word Wide Webs betrachtet, die besonders relevant im Zusammenhang mit Privatsphäre sind.

Welche neuen Strukturen stellen spezifische Angebote des Internets bereit?

Einer der zentralen Empfänger medialer und persönlicher Aufmerksamkeit im Internet sind SNSs, und mit über einer Milliarde Nutzern weltweit vor allem Facebook (Facebook, 2012). SNSs werden aktuell wie folgt definiert: „A social network site is a *networked communication platform* in which participants 1) have *uniquely identifiable profiles* that consist of user-supplied content, content provided by other users and/or system-level data; 2) can *publicly articulate connections* that can be viewed an traversed by others; and 3) can consume, produce and/or interact with *streams of user-generated content* provided by their connections on the site" (Ellison & boyd, 2013, S. 158). Menschen legen auf SNSs Profile von sich an, hinterlegen persönliche Angaben wie Namen, E-Mail Adresse oder Fotos, kontaktieren sich über die Suchfunktion und schließen digitale Freundschaften. Um SNSs nutzen zu können, bedarf es also per definitionem einer Offenbarung von persönlichen Informationen, weswegen die Selbstoffenbarung als Treibstoff von SNS bezeichnet werden kann (Trepte & Reinecke, 2010). Betreiber von SNSs haben als marktwirtschaftliche Unternehmen das Ziel, neue Nutzer zu gewinnen, um Werbeerlöse zu generieren und den Verkauf von Apps anzukurbeln. Da neue Nutzer nur über ein attraktives und florierendes soziales Netzwerk zu erreichen sind, streben die Betreiber danach, die Selbstoffenbarung der Nutzer bereits durch die grundlegende Struktur der Website zu maximieren. Burke, Marlow und Lento (2009) betonen: „Social networking sites (SNS) are only as good as the content their users share. Therefore, designers of SNS seek to improve the overall user experience by encouraging members to contribute more content" (S. 1). Die Selbstoffenbarung ist also eine Voraussetzung für die Gratifikationen, die mit der Nutzung von SNS einhergehen.

Doch welche Gratifikationen stellen SNS bereit, so dass Menschen gewillt sind, persönliche Daten zu veröffentlichen? Hierzu zählen vor allem die Pflege von Sozialkontakten, das Generieren von Sozialkapital, Identitätsmanagement, Unterhaltung und Vertreibung von Langeweile sowie praktische Nutzen wie die Erinnerung an Geburtstage und die Einladungsmöglichkeit zu Partys (Wilson, Gosling, & Graham, 2012). Exemplarisch stellen wir eine Studie von Gonzales und Hancock (2011) vor: Die Wissenschaftler baten Nutzer, einen Fragebogen bezüglich ihres eigenen Selbstwertes auszufüllen. Neben einer weiteren, die an dieser Stelle allerdings nicht maßgeblich ist, hatte das Experiment zwei Bedingungen: Die Kontrollbedingung bestand darin, dass Versuchspersonen lediglich den Fragebogen auszufüllen hatten; die Experimentalbedingung darin, dass die Versuchspersonen gebeten

wurden, ihr Facebook-Profil aufzurufen und sich ihre Chronik/Pinnwand zu betrachten. Nach drei Minuten kam der Versuchsleiter mit dem Fragebogen und der Bitte, diesen auszufüllen, zurück in den Raum. Die Profilseite blieb während des Ausfüllens im Hintergrund geöffnet und sichtbar. Die Ergebnisse zeigen, dass Nutzer, die vor und während des Ausfüllens des Fragebogens ihr Facebook-Profil betrachtet hatten, signifikant erhöhte Werte an Selbstwert vorweisen konnten. Generell gilt, dass der Selbstwert in Zusammenhang mit vielen positiven psychologischen Variablen steht. Verhaltensweisen, die diesen verbessern können, sind somit höchst attraktiv für Menschen – der Preis der Angabe von persönlichen Informationen und die damit einhergehende Reduzierung von informationaler und psychischer Privatsphäre können im Gegensatz dazu sehr gering erscheinen.

Eine weitere strukturelle Veränderung geschieht durch die stetige Zunahme der Verfügbarkeit digitaler Medien, vor allem aufgrund der erhöhten Anzahl an Smartphones, ausgestattet mit mobilem Internetzugang. Während 2010 noch 8 Prozent aller deutschen Jugendlichen mobil online waren, stieg dieser Anteil im Jahr 2011 auf 22 Prozent. 2012 wurde der Anteil bereits auf 40 Prozent beziffert, Tendenz weiter steigend (Medienpädagogischer Forschungsverbund Südwest, 2012; vergleiche Kapitel 2 aus diesem Band zum Thema Mediennutzung). Aufgrund dieser Entwicklung werden die oben genannten Verstärkungsmechanismen noch leichter abrufbar und damit umso tiefer in die Alltagsabläufe integriert. Die fortwährende Nutzung von mobilen Online-Angeboten bringt wiederum eigenständige, aufs Neue die Privatsphäre betreffende Aspekte mit sich. Applikationen wie Google Latitude oder Foursquare erfassen regelmäßig den Aufenthaltsort und Bewegungsraum der Anwender. Immer konkretere Verhaltensprofile können so erstellt werden, immer genauer kann menschliches Verhalten dokumentiert, erklärt und vorhergesagt werden. Der Dienst Google Now beispielsweise erkennt, wenn die Arbeitsstelle verlassen wird, unmittelbar werden Zugverbindungen herausgesucht, die Stau- und Verkehrssituation visualisiert und passende Lokalitäten für das Abendessen empfohlen. Eine anschauliche, positivistische Illustration hierzu findet sich bei Blogger Carsten „Caschy“ Knobloch (Knobloch, 2013). Knobloch schildert in einem Blog-Post exemplarisch eine Busfahrt von Las Vegas zu einem angrenzenden Messegebiet. Während der Fahrt empfiehlt ihm der Dienst naheliegende Sehenswürdigkeiten sowie fotogene Orte; die zeitliche Entfernung zum Hotel wird automatisch berechnet, weitere Verbindungen an nahen

Busstopps herausgesucht; die Prognose des Wetters wird eingeblendet, ebenso ein Fenster zur Deutsch-Englisch Übersetzung bereit gestellt.

Ein weiterer Faktor ist die verbreitete Nutzung von sogenannten Cloud-Diensten, die Daten serverseitig zentral lagern und somit orts- und geräteunabhängig verfügbar machen. Dienste wie Dropbox, Google Drive, Skydrive oder iCloud bieten so in der Regel kostenfrei Online-Speicherplatz an. Auf diesen Speicherplatz können Nutzer private Daten hochladen, sichern und ortsunabhängig verfügbar machen. Dergestalt legen Nutzer private Dokumente, Bilder, Videos und vieles Weitere online ab. Die Privatsphäre wird hierbei insofern berührt, als Betreiber wiederum Nutzerprofile erstellen und statistisch auswerten können, beispielsweise hinsichtlich des vorliegenden Musikgeschmacks. Viele Dienste des Internets erfordern generell das Anmelden mittels eines Benutzeraccounts – sogar einige Internet-Browser bieten mittlerweile eine Einlogg-Möglichkeit, beispielsweise Google Chrome. Diese Accounts ermöglichen einen individualisierten Zugang zu digitalen Angeboten, der implizite Vorlieben sowie explizite Favoriten abspeichert, nichtgenutzte Inhalte ausblendet, insgesamt einen personalisierten Gebrauch ermöglicht. Mittels dieser Profile können Unternehmen leichter verschiedene Bereiche zueinander führen und marktwirtschaftlich nutzen. Google lancierte 2012 den Dienst Google Play, kann somit den Musikgeschmack eines Nutzers zugehörigen Angaben auf dem SNS Google+, Inhalten aus E-Mails von Googlemail oder persönlichen Bilder auf Google Picasa zuordnen.

Welche Bereiche der Privatsphäre werden durch das Internet verändert?

Wie eingangs angesprochen, werden wir im Folgenden anhand des Privatsphäre-Prozess-Modells Besonderheiten kennzeichnen, die sich durch das Internet für die Privatsphäre ergeben haben. Hierzu werden wir anhand der vier verschiedenen Privatsphäredimensionen den Einfluss auf die drei Elemente des Privatsphäreprozesses untersuchen.

In erster Linie ist bei Nutzung des Internets die Dimension der informationalen Privatsphäre berührt. Die Strukturen des Internets (Persistenz, Replizierbarkeit, Skalierbarkeit und Durchsuchbarkeit) beeinflussen hier vor allem den informationalen Privatsphärekontext. Qua Nutzung des Internets werden Informationen gesammelt und in Nutzerprofilen zusammengeführt. Dies geschieht in einem Ausmaß, das neuartig und herausfordernd ist. Diese Veränderung des Kontextes führt bei vielen Nutzern zu einer messbar reduzierten informationalen Privatsphäre (Mohamed & Ahmad, 2012), im Privatsphäre-Prozess-Modell

abgebildet durch die informationale Privatsphärewahrnehmung. Nutzer, deren Soll-Wert an informationaler Privatsphärewahrnehmung dadurch unterschritten wird, sind folglich mit einem Problem konfrontiert: Da sie die Strukturen der Websites nicht modifizieren können – folglich keine Kontrollierbarkeit des informationalen Privatsphärekontextes vorliegt –, bleibt ihnen nur die Veränderung des Privatsphäreverhaltens, um ein Gleichgewicht zu erreichen. Doch angesichts der großen Menge an Gratifikationen und Nutzen, die verschiedene Angebote bereithalten, ist auch dies für die meisten so gut wie ausgeschlossen. Alternativ können Nutzer falsche Informationen bereitstellen, um einer Verbreitung authentischer personenbezogener Daten vorzubeugen. Eine Studie aus Amerika konnte beispielsweise zeigen, dass vierzig Prozent aller Internetnutzer mindestens einmal bewusst falsche Daten bereitgestellt haben (Hoffman, Novak, & Peralta, 1999). Wenn auch auf rechtlich zweifelhaften Weg, so scheinen Nutzer folglich ihr Privatsphäreverhalten anzupassen.

Der soziale Privatsphärekontext ist in SNSs ebenso automatisch reduziert. Werden Inhalte in Statusnachrichten mitgeteilt, so sehen diese durchschnittlich 190 befreundete Nutzer (Ugander, Karrer, Backstrom, & Marlow, 2011). Die Möglichkeit vieler Personen, sich gegenseitig anzunähern und mit anderen in Kontakt zu treten, kann folglich mit einer geringeren sozialen Privatsphäre einhergehen. Im Gegensatz zur informationalen Privatsphäre besteht allerdings hier die Option zur Regulation des Privatsphärekontextes – Nutzer haben die Möglichkeit, Freundschaftslisten anzulegen. Anhand dieser können Sie kommunizierte Inhalte nur ausgewählten Subgruppen zugänglich machen. Die SNS Google+ hat dieses Prinzip mittels der Funktion der Kreise tief in die Struktur der SNS eingebettet – was zu einer Erhöhung des sozialen Privatsphärekontextes führt.

In Bezug auf psychische Privatsphäre zeigt sich ein mittlerweile vielfach bestätigtes Phänomen: Sobald sich Menschen digital miteinander austauschen – was als sogenannte Computervermittelte Kommunikation (CvK) bezeichnet wird – sind sie bereit, mehr persönliche Inhalte von sich zu offenbaren (Qiu, Lin, Leung, & Tov, 2012). Adam Joinson (2001) konnte dies in einer wegweisenden Studie ebenso feststellen. Vierzig Probanden wurden mit dem folgenden Dilemma konfrontiert: „Es gibt in dem weltweit einzigen 100 Prozent atomsicheren Bunker nur Platz für fünf Menschen – welche sollte man wählen?“ Eine Hälfte der Probanden sollte dies in einem „face-to-face“ Gespräch erörtern, die andere räumlich getrennt aber per Chat verbunden. Die Ergebnisse zeigen, dass in der Bedingung

des Chats, also im Rahmen einer computervermittelten Kommunikation, Menschen mehr Informationen über sich preisgaben – beispielsweise identifizierende Informationen wie „Ich bin ein Psychologiestudent“. Bei der Betrachtung des Privatsphärekontextes lässt sich folglich konstatieren, dass User hier mehr über sich selbst kommunizieren, dementsprechend eine erhöhte objektive psychische Privatsphäre vorliegt. Zu der Wahrnehmung der psychischen Privatsphäre liegen bisher keine Erkenntnisse vor.

Der Transfer der physischen Privatsphäre in den Bereich des Internets gestaltet sich schwierig (Trepte & Reinecke, 2011b). Da das Internet einem digitalen Raum entspringt, lassen sich keine tatsächlichen, territorialen Grenzen bestimmen. In einer Studie zur Überprüfung der vier Dimensionen stellten Ruddigkeit, Penzel und Schneider (2013) fest, dass sich physische Privatsphäre nur dann auf SNSs übertragen lässt, wenn es im Sinne des sich der Schaulust anderer aussetzen oder dem Anspruch auf Schutz des eigenen Profils vor unbefugter Einmischung verstanden wird. Da diese beiden Ansätze eine gewisse Schnittmenge mit den Dimensionen der sozialen und psychischen Privatsphäre implizieren, scheint eine Berücksichtigung der physischen Privatsphäre auf Weiteres nicht zielführend.

Hinsichtlich des Privatsphäreverhaltens – also der Bereitschaft, intime Dinge zu offenbaren – lassen sich folgende zwei Beobachtungen feststellen: (1) Nutzer können hier gut regulieren, wie intim die Inhalte ihrer Statusmitteilungen sind. Es besteht somit die Möglichkeit, nur diejenigen Inhalte zu kommunizieren, die sie selbst als angemessen empfinden. (2) Studien zeigen, dass sich das große theoretische Repertoire an Selbstoffenbarungsverhalten auch in einer großen Bandbreite empirischen Verhaltens niederschlägt – Nutzer legen demgemäß tatsächlich eine differenzierte Selbstoffenbarung an den Tag (Ellison, Vitak, Steinfield, Gray, & Lampe, 2011).

Abschließend möchten wir noch auf eine weitere Besonderheit der Privatsphäre im Online-Kontext hinweisen. Wie eingangs erwähnt, bahnt der Privatsphärekontext die Privatsphärewahrnehmung. Auf SNSs scheint dieses nicht durchgängig der Fall zu sein: Obwohl Nutzer mit vielen Menschen gleichzeitig kommunizieren, haben sie den Eindruck einer hohen sozialen Privatsphäre. Dies liegt daran, dass viele Nutzer, die Statusnachrichten lesen können, auf diese nicht reagieren. Da sie folglich nicht auf Inhalte eingehen und im Verborgenen bleiben, verlieren die Kommunikatoren das Bewusstsein über ihre Existenz. danah boyd bezeichnet diesen Vorgang als Context Collapse (boyd, 2008a).

Die in diesem Abschnitt genannten Punkte unterstreichen, dass fast sämtliche Aktionen von Anwendern im Internet mittlerweile mit Privatsphäre zusammenhängen. Die ursprüngliche Nutzung des Internets – das unidirektionale Abrufen von Informationen – ist obsolet. Nutzer treten in einen fortwährenden Dialog, tauschen Informationen aus, kaufen Dienstleistungen durch das Bereitstellen von persönlichen Informationen. In welchem Ausmaß Nutzer dies genau tun, welche Bedenken sie dabei haben und welche psychologischen Nebenerscheinungen damit einhergehen, werden wir im folgenden Kapitel behandeln.

Wie gehen Menschen mit ihrer Privatsphäre im Internet um?

Der Umgang mit Privatsphäre im Internet hat in den letzten Jahren erhebliche Aufmerksamkeit erhalten und umfassende Forschungsaktivitäten hervorgerufen (Trepte & Reinecke, 2011b). Beim Umgang mit der Privatsphäre im Internet ist ebenso wie in anderen Kontexten die gesamte Bandbreite der menschlichen Kommunikation und Interaktion angesprochen. Besonders zentral sind in diesem Kontext die auf die Privatsphäre bezogenen Einstellungen sowie das konkrete, privatsphärebezogene Verhalten. Darüber hinaus stellt sich gerade in den letzten Jahren auch das Wissen über Privatsphäre im Internet als wichtiges Thema heraus. Allen drei Aspekten werden wir uns in diesem Abschnitt widmen. Zunächst betrachten wir die Einstellungen, in der Annahme, dass daraus das Verhalten im Umgang mit den eigenen Daten im Internet resultiert. Dass dies nicht immer der Fall ist, sondern sogar Widersprüche zwischen Einstellungen und Verhalten feststellbar sind, diskutieren wir danach und bieten eine Reihe von Erklärungen für diese Widersprüche an.

Einstellungen zur Privatsphäre im Internet

Im Hinblick auf die Einstellungen zur eigenen Privatsphäre im Internet zeigen aktuelle Studien, dass die meisten Menschen besorgt sind, was mit ihren Daten geschieht und wie verletzlich sie aufgrund im Internet preisgegebener Daten sind. In einer repräsentativen europäischen Studie stimmen 64 % aller Deutschen sowie 58 % aller Europäer der Aussage zu, dass es keine Alternative zur Offenbarung persönlicher Informationen geben würde, wenn man im Internet Produkte oder Dienstleistungen einkaufen möchte (Eurobarometer, 2011). Gleichzeitig beklagen die meisten Personen die geringe informationale Privatsphäre im Internet. 68 % aller Deutschen und 63 % der Europäer geben in dieser Befragung an, dass die Offenbarung persönlicher Informationen aus ihrer Sicht ein großes Problem sei (Eurobarometer, 2011). Insbesondere Personen, die den Eindruck gewonnen haben, bereits

unnötig Daten von sich preisgegeben zu haben, um an Online Services teilzunehmen oder einzukaufen, sind besorgt über den weiteren Umgang mit ihren Daten. Immerhin 73 % der Deutschen und 72 % der Europäer geben an, „ziemlich“ oder „sehr“ besorgt zu sein (Eurobarometer, 2011).

Sorgen um die eigene Privatsphäre betreffen Computer-Viren, Spam, Spyware, Hacker-Angriffe. Dies stellten Paine, Reips, Stieger, Joinson, und Buchanan (2007) in einer qualitativen Studie mit 498 Usern heraus. Weniger bedeutsam waren demgegenüber Identitätsdiebstahl oder generelle Sicherheitsbedenken. In repräsentativen europäischen Studien zeigt sich darüber hinaus ganz deutlich, dass ein großer Anteil der Europäer (73 %) sehr besorgt darüber ist, was überhaupt mit ihren persönlichen Daten geschieht. Die meisten würden gern informiert werden, wofür ihre Daten genutzt werden und zu diesen spezifischen Nutzungsformen ihre Zustimmung geben (Eurobarometer, 2011).

Die Sorgen um die eigene Privatsphäre sind also insgesamt hoch. Welche Faktoren beeinflussen diese Sorgen um die eigene Privatsphäre und gibt es Unterschiede zwischen verschiedenen Personengruppen?

Es wurde immer wieder versucht zu zeigen, dass Menschen verschiedener Länder und Kulturen mit ihren Sorgen um die Privatsphäre im Netz unterschiedlich umgehen. Es wird angenommen, dass Menschen in individualistischen Kulturen, in denen das Individuum ein größeres Gewicht im Wertekanon hat, sich mehr Sorgen um ihre Privatsphäre machen als Personen in kollektivistischen Kulturen, in denen die Gemeinschaft eher im Vordergrund steht und Organisationen eher zugestanden wird, auf das private Leben zuzugreifen. Diese Annahme kann jedoch nicht eindeutig bestätigt werden. In einer Studie mit Usern in New York, Singapur, Bangalore, Seoul und Sidney beispielsweise wurden nur marginale Unterschiede zwischen Bangalore und den anderen Städten gefunden (Cho, Rivera-Sanchez, & Lim, 2009). In einer großangelegten Studie mit 538 Befragten aus 38 Ländern zeigte sich ebenfalls kein Zusammenhang von Individualismus und der Besorgnis über Privatsphäre (Bellman, Johnson, Kobrin, & Lohse, 2004). Denkbar ist, dass im Internet aufgrund des globalen (und rechtlich übergreifenden) Anspruchs auch die User eine globalere Perspektive auf Privatsphäre haben als in anderen Kontexten.

Im Hinblick auf das Geschlecht wurde in verschiedenen Studien ein deutlicher Unterschied dahingehend nachgewiesen, dass Frauen sich mehr Sorgen um ihre Privatsphäre machen

(Cho et al., 2009; Christofides, Muise, & Desmarais, 2009; Yao & Zhang, 2008). Auch schätzen Frauen das Risiko größer ein, aufgrund von Datenschutzverletzungen Opfer von feindseligen oder aggressiven Botschaften in sozialen Medien zu sein (Trepte & Dienlin, 2013). Mit seinem Modell zum geschlechtsspezifischen Umgang mit Privatsphäre zeigt Thelwall (2011) anschaulich auf, dass Frauen besorgter sein sollten, weil sie ihre physische Sicherheit eher schützen müssen und weil sie andere Kommunikationsbedürfnisse haben als Männer. Während Männer grundsätzlich mehr online sind und eine höhere Quantität an Informationen preisgeben, wünschen sich Frauen eher tiefergehende Interaktionen im Internet, die wiederum im Hinblick auf die Privatsphäre auch eher gefährdet sind (Thelwall, 2008, 2011).

Interessant ist, dass die meisten User ihre Sorgen vor allem auf andere zu projizieren scheinen. Die Sorgen um die gesellschaftliche Umgangsweise sind wesentlich höher ausgeprägt als die Sorgen um die eigene Person. Damit verbunden sind die User davon überzeugt, dass sie besser informiert sind und ihre Privatsphäre selbst besser unter Kontrolle haben als andere User (Debatin, Lovejoy, Horn, & Hughes, 2009). Anhand einer Studie mit 910 Usern aus Singapur zeigen Cho, Lee und Chung (2010), dass die Sorgen um die Privatsphäre sich zum einen auf die eigene Privatsphäre beziehen und zum anderen auf die generelle Sorgen darum, wie sich die Gesellschaft im Hinblick auf die Einstellung zur Privatsphäre weiterentwickeln wird. Insbesondere solche Personen, die stark davon überzeugt sind, ihre Privatsphäre unter Kontrolle zu haben, unterliegen einem sogenannten optimistic bias. Dieser Beurteilungsfehler mit der Tendenz zum Optimismus beinhaltet, dass Menschen generell die Risiken für sich selbst als geringer einstufen als für andere.

Diese Ergebnisse zeigen, dass sich Menschen in Europa und international grundsätzlich große Sorgen um ihre Privatsphäre machen und dass sie der Verwendung ihrer Daten skeptisch gegenüber stehen. Demgegenüber sind uns keine Studien bekannt, die diese Art von Sorgen um die eigene Privatsphäre in anderen Kontexten (Familie, Arbeitsleben, Freizeitorganisationen) untersucht haben. Im Hinblick auf die Einstellungen zur Privatsphäre erscheinen längsschnittliche Daten besonders nennenswert. Diese zeigen auf der einen Seite, dass Konsumenten zunehmend besorgt um den Umgang mit ihren Daten sind. Während 1970 nur 30 % angaben, sich Sorgen zu machen, so sind es in den 2000er Jahren 80 % (Cho et al., 2010). Auf der anderen Seite zeigt eine Längsschnittstudie zu sozialen

Netzwerkseiten, dass diese Auseinandersetzung die Einschätzung der Risiken über den Zeitraum von einem Jahr (2010-2011) signifikant senkt (Trepte & Dienlin, 2013). Diese sinkende Auseinandersetzung mit den Risiken, die aus der Nutzung sozialer Netzwerke resultieren, könnte unterschiedliche Gründe haben. Vielleicht liegt es daran, dass es für die User zur Gewohnheit wird, ihre privaten Daten als Währung für die Nutzung der SNSs einzutauschen und die Reflektion über dieses Erlösmodell abnimmt, weil es keine Alternativen gibt. Möglicherweise hängt diese abnehmende Risikoeinschätzung aber auch mit der zunehmenden Nutzung der Privatsphäre-Settings zusammen, die in dem gleichen Zeitraum steigt (ebd.). Dieser verhaltensbezogenen Regulierung der Privatsphäre – zum Beispiel mithilfe der Privatsphäre-Settings – widmen wir uns im folgenden Abschnitt.

Verhalten im Umgang mit der eigenen Privatsphäre im Internet

In ihrem Verhalten spiegeln sich die Sorgen der User nicht immer wider. Fast 90 % aller Europäer geben ihren Namen und ihre Adresse und 18 % sogar ihre Ausweis- oder Reisepass-Identifikationsnummer an, um im Internet einkaufen zu können (Eurobarometer, 2011). Auf sozialen Netzwerkseiten wie Facebook oder Google+ hinterlassen die meisten Europäer regelmäßig Fotos von sich (51 % der Europäer) oder die eigene Adresse (38 %). Unter den Nutzern der sozialen Netzwerke ist diese Offenherzigkeit sogar noch stärker ausgeprägt: In einer deutschen Studie mit 327 Nutzern haben 93 % der User ein Foto von sich und 83 % ihre Adresse angegeben (Trepte & Dienlin, 2013). Die Bereitschaft, diese Art von Daten auf soziale Netzwerkseiten zu stellen, stieg in den letzten zwei Jahren signifikant an. Insbesondere Intensivnutzer und Männer posten zunehmend private Informationen auf SNSs (Trepte & Dienlin, 2013). Neben der informationalen Privatsphäre, die mit der Preisgabe der hier genannten Daten messbar gemacht wurde, ist auch die psychische Privatsphäre relevant. Diese wurde in verschiedenen Studien vor allem mit der psychologischen Dimension der Selbstoffenbarung erfasst (vgl. im Überblick Nguyen, Bin, & Campbell, 2012). Wie im ersten Abschnitt erläutert, erfasst dieses Maß die Kommunikation persönlicher und intimer Dinge. Hier zeigt sich analog zur informationalen Privatsphäre, dass Menschen in den letzten Jahren zunehmend bereit waren, auch emotionale Inhalte von sich preiszugeben (Trepte & Dienlin, 2013).

Warum sind Menschen trotz ihrer Sorgen zunehmend bereit, ihre informationale, soziale und psychische Privatsphäre im Internet zu lockern? Aktuelle Forschung legt zur

Beantwortung dieser Frage weitestgehend ein Rational Choice-Paradigma zu Grunde. Man nimmt an, dass Menschen rational kalkulieren und gut abwägen, welche Risiken sie haben. Überwiegen Nutzen und Gratifikationen, so werden sich Menschen entscheiden, die Risiken offenen Auges zu akzeptieren (Ellison et al., 2011).

Als zentrale Nutzenfunktionen der Preisgabe privater Informationen gelten soziale Unterstützung und Sozialkapital, Identitätsmanagement und Selbstdarstellung sowie die Beteiligung am aktuellen gesellschaftlichen Diskurs und am sozialen Leben (vgl. ausführlich: Taddicken & Jers, 2011). Diese Gratifikationen gelten im Internet ebenso wie in anderen Kontexten (vgl. zweiter Abschnitt). Im Internet unterliegt jedoch die Preisgabe privater Informationen anderen Risiken. Die Strukturen des Internets – (1) Persistenz, (2) Replizierbarkeit, (3) Skalierbarkeit und (4) Durchsuchbarkeit (vgl. zweiter Abschnitt) – bringen es mit sich, dass die Gratifikationen möglicherweise mit höheren Kosten verbunden sind. Die User gehen ein Geschäft mit den Betreibern von Internetseiten ein, dessen Rahmenbedingungen nicht immer deutlich sind. Wichtig erscheint jedoch an dieser Stelle, die Nutzenfunktionen zu verstehen. Wir skizzieren deshalb kurz, welche Gratifikationen möglicherweise dazu führen, dass User auch Privatsphäre-Risiken in Kauf nehmen.

Soziale Unterstützung erweist sich insbesondere aufgrund der Strukturen spezifischer Internetangebote als zentrale Gratifikation (vgl. zweiter Abschnitt). Viele Studien weisen darauf hin, dass insbesondere in sozialen Netzwerkseiten ein erhebliches Maß an Aufmerksamkeit erzielt werden kann und dass kurzfristige Kontakte sowie lose soziale Beziehungen (bridging social capital) weitaus effizienter geknüpft und aufrecht erhalten werden können als ohne mediale Unterstützung. Wenn es um die Vertiefung dieser Kontakte in feste Freundschaften (bonding social capital) geht, gestaltet sich die Situation anders: Viele Studien zum Sozialkapital in SNSs weisen darauf hin, dass zwar lockere Beziehungen, aber keine festen Bindungen geknüpft werden können (Ellison et al., 2011; Steinfield, Ellison, & Lampe, 2008). Im Hinblick auf feste Beziehungen sind die Forschungsergebnisse dementsprechend pessimistischer. Diese können nur im Internet geknüpft und aufrechterhalten werden, wenn sie von face-to-face Begegnungen flankiert werden. In einer Studie mit Computerspielern wurde gezeigt, dass insbesondere der physische Kontakt die Voraussetzung für feste Freundschaftsbeziehungen im Internet und für soziale Unterstützung in anderen Kontexten ist (Trepte, Reinecke, & Juechems, 2012). Ebenso für

Online-Rollenspiele wurde gezeigt, dass feste soziale Bindungen nur von einem sehr geringen Anteil der Spieler geknüpft werden, und auch nur dann, wenn das Online Spiel mit Treffen in der realen Welt gekoppelt wird (Williams, 2007). Ausschließlich in diesen Fällen werden die sozialen Beziehungen aus dem Internet fassbar und nutzbar für das echte Leben. Eine einjährige Längsschnittstudie mit 488 Internetnutzern stellt heraus, dass die Nutzungsintensität, die Selbstoffenbarung und die Gewinnung neuer Freundschaften als reziproker, sich selbst verstärkender Prozess zu verstehen sind: Je häufiger User soziale Netzwerke nutzen, umso mehr geben sie von sich preis – dieser Prozess wird durch das erfolgreiche Knüpfen von Freundschaften verstärkt, er gilt nur für solche User, die auch erfolgreich Freundschaften knüpfen und pflegen können (Trepte & Reinecke, 2013).

Das Identitätsmanagement und die Selbstdarstellung sind ebenfalls wichtige Gratifikationen der Beteiligung an sozialen Netzwerkseiten und rechtfertigen die Preisgabe persönlicher Informationen (Krämer & Haferkamp, 2011). User erhalten aufgrund der Struktur der Netzwerke den Eindruck, dass sie den öffentlichen Eindruck und damit einhergehend auch ihre Identität nach eigenen Wünschen gestalten können. Sie tendieren dazu, sich möglichst positiv darzustellen (Toma & Hancock, 2010, 2011; Toma, Hancock, & Ellison, 2008). Diese strategische Form der Selbstdarstellung ist motiviert durch die Verbesserung des Selbstkonzeptes und ist in diesem Punkt im Internet nicht anders als in anderen Kontexten (Krämer & Haferkamp, 2011). Der zentrale Unterschied liegt jedoch darin, dass mit der medialen Vermittlung der Eindruck, der auf Zielpersonen gemacht werden soll, vielfältiger (z. B. durch Texte, Fotos, Mitteilung von Interessen), gezielter und dauerhafter gestaltet werden kann. Zwei zentrale Methoden dieser strategisch nutzbaren Eindruckssteuerung sind die Kontrolle über Inhalte und die Kontrolle über Interaktionspartner (Trepte & Reinecke, 2011a). Größere Kontrolle über die Inhalte der Selbstdarstellung entsteht zunächst aufgrund der Tatsache, dass Inhalte vor dem online Stellen länger reflektiert werden können, bevor sie anderen präsentiert werden, als das in offline Kontexten der Fall ist. Bevor eine Statusmeldung auf Facebook online gestellt oder ein Foto hochgeladen wird, kann der User kurz darüber nachdenken, ob dieses Posting den eigenen Identitätsinteressen entspricht. Darüber hinaus können einzelne Meldungen und Posts im Nachhinein gelöscht werden. Identität ist damit einfacher editierbar als im offline Kontext. Darüber hinaus ist auch das soziale Umfeld, also das Publikum für die Selbstdarstellung und das Identitätsmanagement, beeinflussbar. Über Freundschaftslisten oder andere Einstellungen in den Settings können

spezifische Personen angesprochen werden. Im realen Leben sind die Publika der eigenen Selbstdarstellung erstens kleiner und zweitens weniger einfach editierbar. Die Interessen der Selbstdarstellung stehen mit den Privatsphäreinteressen häufig im Widerspruch (Krämer & Haferkamp, 2011). Für eine erfolgreiche Selbstdarstellung ist ein großes Publikum wünschenswert. Um die Privatsphäre zu schützen, ist es jedoch sinnvoller, die Publika in Abhängigkeit von den Inhalten der Preisgabe mit Bedacht auszuwählen.

Insgesamt können wir festhalten, dass die Preisgabe persönlicher Informationen im Internet über die Zeit deutlich steigt und dass der Nutzen, der aus diesen Preisgaben für die User erwächst, auf den ersten Blick recht hoch erscheint. Gleichzeitig wird gerade in aktuellen Studien darauf hingewiesen, dass User zunehmend auch die Angebote der Anbieter zur Regulierung ihrer Privatsphäre über die Privatsphäre-Settings in Anspruch nehmen (Dey, Jelveh, & Ross, 2012). Während also die Preisgabe persönlicher Informationen über Zeit deutlich ansteigt, so steigt jedoch auch die Regulierung der Privatsphäre im Internet. Im Zeitverlauf befassen sich User zunehmend damit, den Zugang zu ihren persönlichen Daten auf sozialen Netzwerkseiten zu beschränken (Trepte & Dienlin, 2013). Diese Widersprüche in den Verhaltensweisen der User widmen wir uns im nächsten Abschnitt.

Paradoxien von privatsphärebezogenen Einstellungen und Verhalten

Bisher haben wir die Einstellungen und das Verhalten im Hinblick auf die Privatsphäre im Internet betrachtet. Insgesamt können wir feststellen, dass Menschen sich zunehmend Sorgen um ihre Privatsphäre machen und diesen Sorgen auch mit der Regulierung ihrer Privatsphäre-Settings auf sozialen Netzwerkseiten begegnen, dass sie jedoch immer mehr preisgeben und ihre informationale ebenso wie die psychische Privatsphäre reduzieren. Auf den ersten Blick stehen also das Verhalten der User und ihre Einstellungen in Widerspruch zueinander. Dieser Widerspruch von laxem Privatsphäre-Verhalten auf der einen Seite und der Besorgnis um die eigene Privatsphäre auf der anderen Seite wird als das Privatsphäre-Paradox bezeichnet (Barnes, 2006).

Dass Einstellungen und Verhalten nicht immer konsistent sind, wissen wir aus der psychologischen Forschung zum Umweltschutzverhalten, zum Rauchen oder Vegetarismus. Wie sieht es aber aus, wenn User als Folge der Preisgabe ihrer Informationen schlechte Erfahrungen machen? Aktuelle Studien zeigen, dass trotz negativer Erfahrungen zwar die Einstellungen, nicht jedoch der langfristige Umgang mit Privatsphäre geändert wird. In einer

Längsschnittstudie mit *N* = 327 deutschen Internetnutzern, die über ein Jahr lang befragt wurden, stellte sich Folgendes heraus: User, die negative Erfahrungen (in Form von feindseligen und aggressiven Mails oder Posts anderer User) gemacht haben, schützen erstens ein halbes Jahr später ihre informationale Privatsphäre intensiver als solche, die keine negativen Erfahrungen gemacht haben, und schätzen zweitens auch ihr Risiko als höher ein, eine solche negative Erfahrung wieder zu machen. Auf der anderen Seite zeigt sich allerdings ebenso, dass User, die negative Erfahrungen dieser Art gemacht haben, ein halbes Jahr später ihre psychische oder soziale Privatsphäre nicht besser schützen als User, die keine negativen Erfahrungen gemacht haben (Trepte, Dienlin, & Reinecke, 2013). Hier zeigt sich also ein Risiko-Paradox, welches umschreibt, dass trotz konkreter negativer Erfahrungen im Internet weiterhin intime Inhalte mit anderen geteilt werden, und dass diese Inhalte nicht für bestimmte, ausgewählte Personenkreise angepasst werden.

Ein weiterer Widerspruch im Umgang mit Privatsphäre erscheint uns hier relevant und beschreibt Folgendes: Wenn Menschen kontrollieren können, mit wem sie ihre Daten online teilen (Release), denken sie nicht weiter darüber nach, wie (Use) und von wem (Access) diese Daten weiter genutzt werden. Dieser Widerspruch wird als das Kontroll-Paradox bezeichnet (Brandimarte, Acquisti, & Loewenstein, 2010). Brandimarte et al. (2010) haben verschiedene Experimente durchgeführt, in denen studentischen Probanden gesagt wurde, sie hätten die Möglichkeit, Daten für ein neues soziales Netzwerk der Universität online zu stellen. Einer Gruppe der Probanden wurde mitgeteilt, dass die Daten automatisch online gestellt würden. Einer anderen Experimentalgruppe wurde gesagt, dass nur 50 % der Profile online gestellt würden. Hier zeigte sich, dass Personen der ersten Gruppe mehr und privatere Informationen von sich preisgaben, weil sie den Eindruck hatten, genauer zu wissen, was mit ihren Daten geschieht. In einem zweiten Experiment wurde einer weiteren Gruppe darüber hinaus mitgeteilt, dass ihre Daten nicht nur an der eigenen, sondern auch einer anderen Universität online gestellt würden. Trotz dieser größeren Öffentlichkeit gaben Studenten mehr von sich preis, wenn sie davon ausgingen, dass ihre Informationen in jedem Fall öffentlich gemacht wurden. In einem weiteren Experiment derselben Studienreihe wurde Probanden mitgeteilt, dass sie an einer Studie zu ethischem Verhalten teilnehmen, und dass ihre Antworten im Anschluss an das Experiment in einem „Research Bulletin“ veröffentlich würden. Das Publikum oder die Inhalte dieses Bulletins wurden nicht weiter ausgeführt. Ihnen wurden zehn Fragen dazu gestellt, ob sie lügen, stehlen oder andere

Verhaltensweisen ausüben, die generell als sozial unerwünscht gelten. Drei Möglichkeiten, die eigene Privatsphäre zur regulieren, wurden den Probanden gegeben: (1) Keine Kontrolle: Den Probanden wurde mitgeteilt, dass sie den Forschern die Rechte ihrer Antworten übertragen; (2) teilweise Kontrolle: Die Probanden konnten ankreuzen, ob sie den Forschern ihre Rechte an den Antworten überlassen; und (3) hohe Kontrolle: Die Probanden konnten neben jeder der zehn Fragen ankreuzen, ob sie den Forschern ihre Rechte an den Antworten überlassen. Personen der dritten Gruppe gaben signifikant mehr von sich preis als die Personen der anderen Gruppen. Sie reflektierten dabei weder, wie mit ihren Daten weiter verfahren wird, noch wer Kenntnis über ihre Daten erhält. Die dritte Bedingung simuliert eine typische Abfrage der Privatsphäre, wie wir sie in SNSs vorfinden, in denen zu einzelnen Aktionen die Zustimmung der User abgefragt wird. So bietet beispielsweise Facebook an zu regulieren, welchen Personen man die Präferenzen für einzelne Medien preisgeben möchte. Es resultieren sehr detaillierte Möglichkeiten, die eigene Privatsphäre über die Privatsphäre-Settings der SNS-Anbieter zu regulieren. Es ist zu vermuten, dass die Kontrolle der Privatsphäre-Settings eine ähnliche Wirkung hat wie die Kontrollmöglichkeiten in dem zuvor geschilderten Experiment und dass ein Kontroll-Paradox auf SNSs täglich in ähnlicher Weise stattfindet.

Die verschiedenen Paradoxien legen dar, dass User und Konsumenten im Internet nicht immer logisch und konsistent mit ihrer eigenen Privatsphäre umgehen. Diese Ergebnisse sind alarmierend im Hinblick auf den Umgang mit privaten Daten im Internet. Zu diskutieren ist hier, welche Motive einer derart laxen Umgangsweise mit Privatsphäre zu Grunde liegen. Erklärt werden diese Paradoxien in der Regel damit, dass der Nutzen (vgl. die im Vorigen genannten Dimensionen der sozialen Unterstützung, des Sozialkapitals, der Selbstdarstellung und des Identitätsmanagement) der Preisgabe persönlicher Informationen so hoch ist, dass die Sorgen und Risiken gern in Kauf genommen werden. Nun zeigt sich aber in Studien zum Wissen über Privatsphäre im Internet, dass diese rationale Herangehensweise möglicherweise nicht vertretbar ist. Das Wissen der User ist denkbar gering. So macht jeder einzelne User Fehler bei der Einstellung seiner Privatsphäre-Settings auf sozialen Netzwerkseiten. Dies zeigte eine Studie mit *N* = 65 Usern, die zunächst nach ihren Intentionen und Prioritäten der Privatsphäre auf ihrem sozialen Netzwerk gefragt wurden (Madejski, Johnson, & Bellovin, 2012). Im nächsten Schritt wurden die Privatsphäre-Settings dieser User daraufhin geprüft, ob sie die Prioritäten und Intentionen entsprechend

widerspiegeln. Mindestens ein Fehler lag bei jedem der Befragten vor: Zum Beispiel teilten 94 % der User Informationen, die sie eigentlich zurückhalten wollten und 84 % hielten Informationen zurück, die sie eigentlich teilen wollten.

Ebenso wenig wissen User über die Erlös- und Geschäftsmodelle, die hinter den verschiedenen Internetservices stehen. In einer für die USA repräsentativen Studie wurden *N* = 1.500 Jugendliche gefragt, ob sie wissen, dass ihr Nutzungsverhalten im Internet verfolgt wird und welche Erlösmodelle hinter diesem Tracking stehen (Turow, Feldman, & Meltzer, 2005). Die Mehrzahl der Befragten (84 %) wusste darüber Bescheid, dass ihr eigenes Surfverhalten über Cookies nachvollzogen werden kann und dass die Anbieter (z. B. soziale Netzwerke, Reiseportale, Händler) protokollieren, welche Websites genutzt werden. Die Hälfte der Befragten wusste jedoch nicht, dass die eigenen Adressdaten an Drittanbieter weitergegeben werden, dass keine Informationen darüber erhältlich sind, welche persönlichen Daten bei einem Anbieter gespeichert sind und dass die persönlichen Daten von den Anbietern nicht wieder zurückgefordert können oder eine Löschung bewirkt werden kann. Insgesamt ist vor allem das Unwissen darüber groß, wie die eigenen Daten zwischen verschiedenen Anbietern kursieren und wie sie für Targeting (gezieltes Ausspielen von Werbung aufgrund von soziodemographischen Daten, die bei der Registrierung für einen Dienst und aufgrund von Surfgewohnheiten hinterlassen werden), Real-Time Bidding (gezieltes Ausspielen von Werbung aufgrund des Surfverhaltens; die Kosten der Werbeplätze richten sich nach der zuvor berechneten Erfolgsrate, also danach wie viel geklickt und gekauft wird) und Affiliate Marketing (sog. Affiliates, also Werbetreibende, erhalten von Portalbetreibern eine Provision, wenn auf die Werbung des Portals geklickt wird oder ein Kauf erfolgt) genutzt werden. Ähnlich zeigen Hoofnagle, King und Turow (2010) in einer Studie mit *N* = 975 US-Amerikanern, die in einer Telefonbefragung interviewt wurden, dass das Wissen über die Erlösmodelle denkbar gering ist. Fünf Fragen sollten mit „Falsch“ oder „Richtig“ beantwortet werden: Weist die Datenschutzerklärung einer Website darauf hin, dass (1) deine Daten nicht ohne dein Einverständnis mit den Betreibern anderer Websites geteilt werden?; (2) deine Einkäufe und deine Adresse nicht den Betreibern anderer Websites mitgeteilt werden?; (3) deine Daten (Name, Einkäufe, andere Einträge) gelöscht werden, wenn du das möchtest?; (4) du die Website-Betreiber verklagen kannst, wenn sie ihre Datenschutzerklärung verletzen?; (5) dein Einverständnis eingeholt werden muss, wenn der Betreiber dein Surfverhalten über verschiedene Websites nachverfolgen möchte? Die

richtige Antwort auf alle fünf Fragen ist „Falsch“. 3 % der Befragten konnten alle Fragen richtig beantworten und 30 % der Befragten konnten keine der Fragen richtig zuordnen. Insbesondere Jugendliche und jungen Erwachsene waren nur selten in der Lage die rechtlichen und wirtschaftlichen Rahmenbedingungen richtig einzuschätzen. Hier zeigt sich demnach Handlungsbedarf, mit dem möglicherweise die derzeitigen Widersprüche und Paradoxien aufgeklärt werden können.

Welche Handlungsimplikationen bestehen zur Sicherung der Privatsphäre im Internet?

Europäer machen sich erhebliche Sorgen um ihre Privatsphäre, das zeigen viele internationale Studien sehr eindeutig. Darüber hinaus sind die Geschäftspraktiken der derzeitigen Online-Dienste im Umgang mit privaten Daten für die Nutzer nicht eindeutig nachvollziehbar. Die intensive Weiterverwendung von privaten Daten für Behavioral Targeting, Real-Time Bidding oder Affiliate Marketing überschreitet zum Teil Grenzen, die User in anderen Konsumkontexten (z. B. Werbemailings per Post oder Anrufe) nicht akzeptieren würden. An den im vorigen Abschnitt dargestellten Paradoxien (Privatsphäre-Paradox, Risiko-Paradox, Kontroll-Paradox) wird deutlich, dass diese Sorgen nicht immer in konkretes Verhalten umgesetzt werden. Wir vermuten auf der einen Seite, dass der Nutzen der angebotenen Dienste für die User dazu führt, dass sie ihren Sorgen zu wenig Raum geben. Auf der anderen Seite ist denkbar, dass das Wissen nicht ausreicht, um sich gegen die Bedrohungen, aus denen die Sorgen resultieren zu schützen. Handlungsoptionen liegen insbesondere in der inhaltlichen Aufklärung der User auf diesen zwei Ebenen: Wissen über die individuellen Nutzenfunktionen und Wissen über die Erlösmodelle der Website-Betreiber.

Auf der Ebene der Aufklärung über Nutzenfunktionen ist aus unserer Sicht sinnvoll, die verschiedenen psychologischen Gratifikationen der Online-Dienste klar zu benennen. Werden User direkt nach ihren Motiven der Nutzung spezifischer Dienste gefragt, so geben sie beispielsweise für soziale Netzwerkseiten an, dass sie „Kontakte knüpfen“ möchten. Dieser individuelle Eindruck ist jedoch aus psychologischer Sicht zu oberflächlich. Die tieferliegenden Nutzenfunktionen hatten wir im vorausgegangenen Abschnitt ausführlich erläutert. Es erscheint deshalb sinnvoll, im Kontext von Privatsphäre-Maßnahmen den erweiterten psychologischen Nutzen sowie den Preis, der für Privatsphäre gezahlt wird, zu

verdeutlichen. Wir vermuten, dass die Kosten-Nutzen-Relation mit vier Fragen bewusst gemacht werden kann:

1. Individueller Nutzen: Warum nutze ich einen bestimmten Dienst gern? Welche Vorteile entstehen für mich?
2. Individuelle Kosten: Welche Daten gebe ich genau preis? Wie viel sind mir diese Daten finanziell und ideell wert?
3. Nutzen des Website-Betreibers: Wie generiert der Anbieter mit diesen preisgegebenen Daten Erlöse? Welchen Wert haben in diesem Erlösmodell meine Daten? Welche Erlöse werden mit meinen Daten erzielt?
4. Kosten-Nutzen Abwägung: In welchem Verhältnis steht der Nutzen, den ich mit der Preisgabe meiner Daten erziele zu den Kosten?

Um diese Kosten-Nutzung Abwägung betreiben zu können, ist ein konkreter Algorithmus erforderlich, mit dem vor allem die Erlöse, die aus den Daten eines einzelnen Users resultieren, berechnet werden können. Dies ist vor dem Hintergrund der Preismargen, die im Affiliate Marketing erzielt werden, in Form einer Simulation durchaus denkbar. Mittels Coachings in Schulklassen, Universitätsseminaren oder öffentlichen Kursen können auf diese Weise auch der Wert der Privatsphäre einer ganzen Gruppe kalkuliert werden, um die Berechnung anschaulicher zu machen.

Hinsichtlich des Wissenserwerbs sind einerseits konkrete Schulungen zum Umgang mit Privatsphäre auf konkreten Websites und andererseits Informationen zu Erlös- und Geschäftsmodellen erforderlich. Derzeit werden viele Informationen angeboten, diese scheinen jedoch dem einzelnen User noch nicht ausreichend zugänglich zu sein. Folgende Seite stellen gute Ressourcen bereit, um eine tiefergehende Auseinandersetzung zu ermöglichen:

- Bundesprüfstelle für jugendgefährdende Medien (www.bundespruefstelle.de)
- Landesmedienanstalten (www.die-medienanstalten.de)
- Informationsbroschüre der Landesmedienanstalt Hamburg Schleswig-Holstein (www.ma-hsh.de/cms/upload/downloads/Publikationen/MA_HSH_Broschre.pdf)
- Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (www.datenschutzzentrum.de)
- Scout – das Magazin für Medienkompetenz (www.scout-magazin.de)

- Dunkelziffer e.V. – Seminar und Informationsmaterial Sicher im Netz (www.dunkelziffer.de/fortbildung/SicherimNetz.html)

Zusammenfassung

Betrachtet man die Privatsphäre im Internet, so hat man es nicht mit einem neuen Phänomen zu tun. Die Vorgänge der Privatsphäre sind bereits bekannt, allein der Privatsphärekontext hat sich stark verändert. Im ersten Abschnitt stellten wir als zentrale Variablen innerhalb dieses Vorganges den Privatsphärekontext, die Privatsphärewahrnehmung und das Privatsphäreverhalten vor. Entscheidend ist, dass eine stetige Privatsphäreregulation vonstattengeht, die das tatsächliche Maß (Ist-Zustand) an Privatsphäre einem gewünschten Maß (Soll-Zustand) anpasst und somit individuell angenehme Privatsphärezustände ermöglicht. Privatsphäre lässt sich dabei für den Privatsphärekontext und die Privatsphärewahrnehmung in die Dimensionen informationale, soziale, psychische und physische Privatsphäre einteilen. Die Ausprägungsgrade der Privatsphäre sind deskriptiv und damit neutral zu beurteilen – eine größere Privatsphäre bedeutet nicht eine bessere Privatsphäre. Positiv einzuschätzen ist vielmehr, wenn das gewünschte Maß an Privatsphäre auch dem tatsächlichen entspricht und negativ, wenn sich das erwünschte und tatsächliche Ausmaß an Privatsphäre nicht in Balance befinden.

Der neue Kontext des Internets birgt hier aufgrund vielfältiger struktureller Veränderungen (vgl. zweiter Abschnitt) eine große Herausforderung in sich. Neue und soziale Online-Dienste eröffnen Nutzengratifikationen wie beispielsweise die zeitlich und räumlich unabhängige Kommunikation, die jedoch mit verschiedenen Risiken für die Privatsphäre einhergehen. Wie wir im dritten Abschnitt aufzeigten, liegt ein Gleichgewicht der Privatsphäre nicht immer vor, vielmehr scheint das Privatsphäreverhalten manchmal paradox. Obwohl Nutzer große Bedenken bezüglich ihrer Privatsphäre im online Kontext haben, schützen sie diese oftmals nicht entsprechend (Privatsphäre Paradox); obwohl Nutzer negative Erfahrungen im Internet sammeln, verändern sie nicht ihr Verhalten (Risiko Paradox); sobald Nutzer den Eindruck haben, sie verfügen über die Kontrolle ihrer Daten, sind sie automatisch bereit, mehr von sich preiszugeben (Kontrollparadox). Studien zeigen darüber hinaus, dass Nutzer schlecht über die Weiterverarbeitung ihrer Daten informiert sind (vgl. vierter Abschnitt). Dies unterstreicht die Notwendigkeit, mehr Wissen über Datenverarbeitungsvorgänge, Praktiken

und dahinterliegende Geschäftsmodelle zu vermitteln. Viele Nutzer sind sich beispielsweise nicht der Tatsache bewusst, dass sie für vermeintlich kostenfreie Angebote des Internets in Form der Bereitstellung personenbezogener Informationen zahlen. Die Währung und der Wert dieser Daten sind dementsprechend in der Öffentlichkeit klar zu kommunizieren. Angemerkt sei, dass auch dieses vorliegende Geschäftsprinzip an sich neutral zu bewerten ist, solange der Nutzer über die zugrundeliegenden Prozesse ausreichend informiert ist und sein Handeln bewusst anpassen kann. Angesichts des durchschlagenden subjektiven Mehrwerts von entsprechenden Interaktionen innerhalb des Internets, muss allerdings in Frage gestellt werden, ob eine Verhaltensmodifikation im Sinne einer Reduzierung der Datenweitergabe für viele überhaupt noch möglich erscheint. Das Bereitstellen alternativer Zahlungsmodelle – beispielsweise monetärer Natur – durch Betreiber von Websites für ihre Angebote wäre hier eine wünschenswerte Entwicklung. Dann wären Nutzer nicht verpflichtet, ihre persönlichen Daten anzugeben, könnten also ihre Privatsphäre freier regulieren, was gemäß des Privatsphäre-Prozess-Modells (vgl. Abbildung 1) eine entscheidende Grundvoraussetzung für eine individuell stimmige und ausgeglichene Privatsphäre ist.

Arbeitsaufgaben zur Vertiefung des Themas

1. Reflektieren Sie Ihren Umgang mit Privatsphäre in unterschiedlichen Kontexten und in verschiedenen Szenarien.
2. Betrachten Sie Ihre Privatsphäre hinsichtlich der vier verschiedenen Dimensionen informationale, psychische, soziale und physische Privatsphäre. Unterscheiden sich die gewünschten Ausprägungsgrade voneinander?
3. Entwerfen Sie die Gliederung für einen Schulungstag für Jugendliche im Alter von 16-18 Jahren mit dem Titel „Privatsphäre im Internet“.
4. Führen Sie einen Test aufs Exempel durch: Fragen Sie Menschen ihrer Umgebung danach, wie stark sie ihre jeweiligen Privatsphäredimensionen eigentlich im Internet wahren möchten. Lassen Sie anhand von Profilen in SNSs überprüfen, ob sich diese Vorstellungen auch tatsächlich in den Profilen widerspiegeln.
5. Formulieren Sie Ihre wichtigsten Wissensfragen, die Sie gern im Hinblick auf die Funktionsweise des Internets und Datenschutz beantworten möchten. Recherchieren

Sie die Informationen mit den im vierten Abschnitt angegebenen Quellen und versuchen Sie auf diese Weise, Ihre Fragen zu beantworten.

Literaturverzeichnis

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Monterey, CA: Brooks/Cole Publishing Company.

Barnes, S. B. (2006). A privacy paradox: Social networking in the Unites States. *First Monday, 11*(9). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society, 20*, 313-324. doi:10.1080/01972240490507956

boyd, d. (2008a). Facebook's privacy trainwreck: Exposure, invasion, and social convergence. *Convergence: The International Journal of Research into New Media Technologies, 14*(1), 13–20. doi:10.1177/1354856507084416

boyd, d. m. (2008b). *Taken out of context: American teen sociality in networked publics*. PhD Dissertation. Berkeley.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2010). *Privacy Concerns and Information Disclosure: An Illusion of Control Hypothesis*. Paper presented at the Workshop on the Economics of Information Security (WEIS), Harvard University, USA.

Burgoon, J. K. (1982). Privacy and communication. In M. Burgoon (Ed.), *Communcation yearbook 6* (pp. 206-249). Beverly Hills: Sage.

Burke, M., Marlow, C., & Lento, T. (2009). Feed me: Motivating newcomer contribution in social networking sites. *Proceedings of the 27th International Conference on Human Factors in Computing Systems* (pp. 945–995). New York, NY: ACM.

Cho, H., Lee, J.-S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior, 26*, 987-995. doi:10.1016/j.chb.2010.02.012

Cho, H., Rivera-Sanchez, M., & Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. *New Media & Society, 11*(3), 395-416. doi:10.1177/1461444808101618

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on facebook: Are they two sides of the same coin or two different processes? *CyberPsychology & Behavior, 12*(3), 341-345. doi:10.1089/cpb.2008.0226

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*, 83-108. doi:10.1111/j.1083-6101.2009.01494.x

Derlega, V. J., & Chaikin, A. L. (1977). Privacy and self-disclosure in social relationships. *Journal of Social Issues, 33*(3), 102-115. doi:10.1111/j.1540-4560.1977.tb01885.x

Dey, R., Jelveh, Z., & Ross, K. (2012). *Facebook users have become much more private: A large-scale study*. Paper presented at the 4th IEEE International Workshop on Security and Social Networking (SESOC), Lugano, Switzerland.

Dienlin, T. (2013). *The privacy process model*. Manuskript in Vorbereitung.

Ellison, N. B., & boyd, d. m. (2013). Sociality through social network sites. In W. H. Dutton (Ed.), *The Oxford handbook of Internet studies* (pp. 151–172). Oxford: Oxford University Press.

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte & L. Reinecke (Eds.), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (pp. 19-32). Berlin: Springer.

Eurobarometer. (2011). *Attitudes on data protection and electronic identity in the European Union*. Brussels: European Commission. Retrieved from http://ec.europa.eu/public_opinion/archives/ebs/ebs_335_en.pdf

Facebook. (2012). *Quartely Earnings Slides Q3 2012*. Retrieved from http://investor.fb.com/common/download/download.cfm?companyid=AMDA-

NJ5DZ&fileid=607756&filekey=74bd3d97-525b-4a9f-8a4d-7b1b764c71cd&filename=FB_Q3_Investor_Deck.pdf

Gavison, R. (1980). Privacy and the limits of law. *The Yale Law Journal, 89*(3), 421–471. Retrieved from http://www.jstor.org/stable/795891

Gonzales, A. L., & Hancock, J. T. (2011). Mirror, mirror on my Facebook wall: Effects of exposure to Facebook on self-esteem. *Cyberpsychology, Behavior, and Social Networking, 14*(1-2), 79–83. doi:10.1089/cyber.2009.0411

Heller, C. (2011). *Post Privacy: Prima leben ohne Privatsphäre*. München: Beck.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM, 42*(4), 80–85. doi:10.1145/299157.299175

Hoofnagle, C., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policy. Retrieved from http://ssrn.com/abstract=1589864

Jarvis, J. (2011). *Public parts: How sharing in the digital age improves the way we work and live*. New York, NY: Simon & Schuster.

Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology, 31* (2), 177-192. doi: 10.1002/ejsp.36

Knobloch, C. (2013, 13. Januar). Google Now: mit Googles Geheimwaffe in Las Vegas. Retrieved from http://stadt-bremerhaven.de/google-now-mit-googles-geheimwaffe-in-las-vegas/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+stadt-bremerhaven%2FdqXM+%28Caschys+Blog%29

Krämer, N. C., & Haferkamp, N. (2011). Online self-presentation: Balancing privacy concerns and impression construction on social networking sites. In S. Trepte & L. Reinecke (Eds.), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (pp. 127-142). Berlin: Springer.

Lindner, R. (2010, 18. Januar). Datenschutz: Umstrittene Privatsphäre à la Facebook. FAZ. Retrieved from http://www.faz.net/aktuell/wirtschaft/unternehmen/datenschutz-umstrittene-privatsphaere-a-la-facebook-1983538.html

Madejski, M., Johnson, M., & Bellovin, S. M. (2012). *A Study of Privacy Settings Errors in an Online Social Network.* Paper presented at the Tenth Annual IEEE International Conference on Pervasive Computing and Communications, Lugano, Switzerland.

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues, 59*(2), 243-261. doi:10.1111/1540-4560.00063

Margulis, S. T. (2011). Three theories of privacy: An overview. In S. Trepte & L. Reinecke (Eds.), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (pp. 19-18). New York: Springer.

Medienpädagogischer Forschungsverbund Südwest. (2011). *JIM-Studie 2012*. Stuttgart.

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior, 28*(6), 2366–2375. doi:10.1016/j.chb.2012.07.008

Nguyen, M., Bin, Y. S., & Campbell, A. (2012). Comparing online and offline self-disclosure: A systematic review. *Cyberpsychology, Behavior and Social Networking, 15*(2), 103-111. doi: 10.1089/cyber.2011.0277

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Palo Alto, CA: Stanford University Press.

Paine, C., Reips, U.-D., Stieger, S., Joinson, A. N., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies, 65*, 526-536. doi:10.1016/j.ijhcs.2006.12.001

Petronio, S. (2002). *Boundaries of Privacy*. Albany, NY: State University of New York Press.

Qiu, L., Lin, H., Leung, A. K., & Tov, W. (2012). Putting their best foot forward: Emotional disclosure on Facebook. *Cyberpsychology, Behavior, and Social Networking*, *15*(10), 569–572. doi:10.1089/cyber.2012.0200

Reißmann, O. (2010, 26. März). Verzicht auf Google: Es geht auch ohne. SPIEGEL ONLINE. Retrieved from http://www.spiegel.de/netzwelt/web/verzicht-auf-google-es-geht-auch-ohne-a-683256.html

Ruddigkeit, A., Penzel, J., & Schneider, J. (2013). *Ich sehe was, was Du nicht siehst… Konditionale Selbstauskunft als Grundprinzip der Privacyregulierung von Facebooknutzern.* Manuskript eingereicht zur Publikation.

Steinfield, C., Ellison, N. B., & Lampe, C. (2008). Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. *Journal of Applied Developmental Psychology, 29*, 434-445. doi:10.1016/j.appdev.2008.07.002

Taddicken, M., & Jers, C. (2011). The uses of privacy online: Trading a loss of privacy for social web gratifications? In S. Trepte & L. Reinecke (Eds.), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (pp. 143-158). Berlin: Springer.

Thelwall, M. (2008). Social networks, gender, and friending: An analysis of myspace member profiles. *Journal of the American Society for Information Science and Technology, 59*(8), 1321-1330. doi:10.1002/asi.20835

Thelwall, M. (2011). Privacy and gender in the social web. In S. Trepte & L. Reinecke (Eds.), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (pp. 251-266). Berlin: Springer.

Toma, C. L., & Hancock, J. T. (2010). Looks and lies: The role of physical attractiveness in online dating self-presentation and deception. *Communication Research, 37*, 335-351. doi:10.1177/0093650209356437

Toma, C. L., & Hancock, J. T. (2011). A new twist on love's labor: Self-presentation in online dating profiles. In K. B. Wright & L. M. Webb (Eds.), *Computer-mediated communication in personal relationships* (pp. 41-55). New York: Peter Lang.

Toma, C. L., Hancock, J. T., & Ellison, N. B. (2008). Seperating fact from fiction: An Examination of deceptive self-presentation in online dating profiles. *Personality and Social Psychological Bulletin, 34*(8), 1023-1036. doi:10.1177/0146167208318067

Trepte, S. (2012). Privatsphäre aus psychologischer Sicht. In J. Schmidt & T. Weichert (Eds.), *Datenschutz. Grundlagen, Entwicklungen und Kontroversen* (pp. 59-66). Bonn: Bundeszentrale für politische Bildung.

Trepte, S., & Dienlin, T. (2013). *Consequences and Correlates of Social Media Use: A research report.* Stuttgart: University of Hohenheim.

Trepte, S., Dienlin, T., & Reinecke, L. (2013). *Risky Behaviors – Der Einfluss negativer Erfahrungen in sozialen Netzwerken auf die informationale, psychische und soziale Privatsphäre.* Manuskript in Vorbereitung.

Trepte, S., & Reinecke, L. (2010). Unterhaltung online – Motive, Erleben, Effekte. In W. Schweiger & K. Beck (Eds.), *Handbuch Onlinekommunikation* (pp. 211-233). Wiesbaden: VS Verlag.

Trepte, S., & Reinecke, L. (2011a). The social web as shelter for privacy and authentic living. In S. Trepte & L. Reinecke (Eds.), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (pp. 61-74). Berlin: Springer.

Trepte, S., & Reinecke, L. (Eds.). (2011b). *Privacy online: Perspectives on privacy and self-disclosure in the social web*. New York: Springer.

Trepte, S., & Reinecke, L. (2013). The reciprocal effects of social network site use and the disposition for self-disclosure: A longitudinal study. *Computers in Human Behavior*, *29*(3), 1102–1112. doi:10.1016/j.chb.2012.10.002

Trepte, S., Reinecke, L., & Juechems, K. (2012). The social side of gaming: How playing online computer games creates online and offline social support. *Computers in Human Behavior, 28*, 832–839. doi:10.1016/j.chb.2011.12.003

Turow, J., Feldman, L., & Meltzer, K. (2005). Open to exploitation: America's shoppers online and offline. Report from the Annenberg Public Policy Center of the University of Pennsylvania. *Annenberg School for Communication Departmental Papers (ASC)*. Philadelphia: University of Pennsylvania.

Ugander, J., Karrer, B., Backstrom, L., & Marlow, C. (2011). The anatomy of the facebook social graph. Retrieved from http://arxiv.org/pdf/1111.4503.pdf

Vinsel, A., Brown, B. B., Altman, I., & Foss, C. (1980). Privacy regulation, territrorial displays, and effectiveness of individual functioning. *Journal of Personality and Social Psychology, 39*(6), 1104-1115. doi:10.1037/h0077718

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.

Westin, A. F. (1967). *Privacy and freedom.* New York: Atheneum.

Westman, M., & Eden, D. (1997). Effects of a respite from work on burnout: Vacation relief and fade-out. *Journal of Applied Psychology, 82*(4), 516-527. doi:10.1037/0021-9010.82.4.516

Williams, D. (2007). The impact of time online: Social capital and cyberbalkanization. *Cyber Psychology & Behavior, 10*(3), 398-406. doi:10.1089/cpb.2006.9939

Wilson, R. E., Gosling, S. D., & Graham, L. T. (2012). A review of Facebook research in the social sciences. *Perspectives on Psychological Science, 7*(3), 203–220. doi: 10.1177/1745691612442904

Wheeless, L. R., Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. *Human Communication Research, 2*(4), 338-346.

Yao, M. Z., & Zhang, J. (2008). Predicting user concerns about online privacy in Hong Kong. *CyberPsychology & Behavior, 11*(6), 779-781. doi:10.1089/cpb.2007.0208