



universität  
wien

# DIPLOMARBEIT

Titel der Diplomarbeit

„Der Einfluss der medialen Berichterstattung über die Möglichkeit der flächendeckenden Datenspeicherung und Analyse nahezu aller Internetaktivitäten auf das Sicherheitsverhalten von Internetnutzern: Der Zusammenhang mit Wissen, Besorgnis und Persönlichkeit.“

Verfasserin

Teresa Amelie Sittauer

Angestrebter akademischer Grad

Magistra der Naturwissenschaften (Mag. rer. nat.)

Wien, 2015

Studienkennzahl lt. Studienblatt: A 298

Studienrichtung lt. Studienblatt: Psychologie

Betreuerin / Betreuer: Prof. Dr. Michael Trimmel

# DANKSAGUNG

---

Zuerst danke ich meinem Betreuer Prof. Dr. Trimmel herzlich für seine Betreuung, sowie das gestellte Thema, das ich ohne seinen Input wohl nie so differenziert hätte bearbeiten können.

Dann möchte ich meinen Eltern für ihre emotionale sowie finanzielle Unterstützung während meiner gesamten Studienzzeit danken. Ohne sie wäre es mir nicht möglich gewesen dieses Studium überhaupt aufzunehmen und schon gar nicht es mit dieser Arbeit zu beenden!

Außerdem muss ich all meinen Freundinnen und Freunden danken, die meine letzten Jahre unvergesslich gemacht haben und ohne deren Zuspruch und Unterstützung ich nicht so weit gekommen wäre. Danke Anna, Susi, Jessi, Jens, Lukas und Karl - ihr seid die Besten!

Nicht zuletzt möchte ich mich bei allen bedanken, die an der Untersuchung für diese Arbeit teilgenommen und ihre Zeit zur Verfügung gestellt haben.

### **EHRENWÖRTLICHE ERKLÄRUNG**

Hiermit versichere ich, Teresa Sittauer, dass ich die vorliegende Arbeit selbstständig angefertigt habe und keine anderen als die angegebenen Quellen verwendet habe sowie die diesen Quellen wörtlich oder inhaltlich übernommenen Stellen als solche kenntlich gemacht habe. Darüber hinaus wurde die Arbeit weder in gleicher noch ähnlicher Form einer anderen Stelle zur Beurteilung vorgelegt und stimmt mit der vom Betreuer beurteilten Version überein.

-----

Ort, Datum

-----

Unterschrift

## Inhaltsverzeichnis

1.	Einleitung und Problemstellung.....	8
1.1	Online Privatsphäre .....	9
1.1.1	Definition von Online Privatsphäre .....	9
1.2	Sorgen um die Privatsphäre .....	10
1.3	Individuelle Differenzen in der Besorgnis .....	11
1.3.1	Fundamentalisten, Pragmatiker und Unbesorgte .....	11
1.3.2	Kulturelle Unterschiede in Sorgen um die Privatsphäre .....	12
1.3.3	Der Einfluss von Persönlichkeit auf Besorgnis .....	12
1.3.4	Alter, Bildung, Internet-Erfahrung .....	12
1.3.5	Einfluss von Datenschutzrichtlinien auf Besorgnis .	13
1.4	Der Einfluss von Sorgen um die Privatsphäre auf das Online-Verhalten .....	13
1.5	Wahrnehmung institutioneller Datenspeicherung .....	14
1.5.1	Sorgen um institutionelle Datenspeicherung .....	14
1.5.2	Institutionen - Beschützer oder Angreifer der Privatsphäre? .....	15
1.5.3	Kosten-Nutzen-Abwägung: Privatsphäre vs. Nationale Sicherheit .....	16
1.5.4	Einstellungen zur institutionellen Datenspeicherung im kulturellen Vergleich .....	18
1.6	Protektive Strategien zum Schutz der Online Privatsphäre .....	19
1.6.1	Proaktive Strategien .....	19
1.6.2	Protektive Strategien in Sozialen Netzwerken .....	22
1.6.3	Weitere Strategien .....	22

1.7 Die Datenschutzrichtlinien der EU .....	23
1.7.1 Innereuropäischer Datenverkehr .....	23
1.7.2 Grenzüberschreitender Datenverkehr .....	24
1.7.3 Elektronische Kommunikation .....	25
1.8 Wissen um rechtliche Grundlagen der Datenspeicherung ..	25
1.9 Der Einfluss von Persönlichkeitsfaktoren auf das Online- Verhalten .....	27
1.10 Forschungshypothese und weitere Fragestellungen .....	28
2. Methode .....	31
2.1 Design .....	31
2.2 Untersuchungsteilnehmer .....	32
2.3 Messinstrument .....	33
2.3.1 Demographische Daten .....	33
2.3.2 Medienkonsum .....	33
2.3.3 Big 5 .....	34
2.3.4 Besorgnis .....	34
2.3.5 Wissen .....	35
2.3.6 Protektive Strategien .....	35
2.3.7 „Knew-it-all-along“-Effekt .....	36
2.3.8 Lebenszufriedenheit - SWL .....	36
2.4 Untersuchungsdurchführung .....	37
2.5 Statistische Hypothesen .....	37
3. Ergebnisse .....	39
3.1 Deskriptive Ergebnisse .....	40
3.1.1 Demographische Daten .....	40
3.1.2 Internetzugang und Nutzung .....	41
3.1.3 Protektive Strategien .....	43

3.1.4 „Knew-it-all-along“-Effekt .....	44
3.1.5 Lebenszufriedenheit der Teilnehmer .....	44
3.1.6 Medienkonsum .....	45
3.1.7 Wissen .....	46
3.1.8 Persönlichkeitsfaktoren .....	47
3.1.9 Einstellung zum Erhebungskontext .....	47
3.1.10 Besorgnis - Deskriptive Statistik auf Item-Ebene .	49
3.2 Interferenzstatistische Ergebnisse .....	51
3.2.1 Faktorenanalyse zur Skala „Einstellungen zur flächendeckenden Datenspeicherung“ .....	51
3.2.2 Prädiktor-Modelle .....	53
3.2.2.1 Prädiktor-Modell der Online Stichprobe.....	53
3.2.2.2 Prädiktor-Modell der Paper-Pencil-Stichprobe...	54
3.2.2.3 Modell Vergleich.....	55
3.2.3 Lebenszufriedenheit, Medienkonsum und Einstellungen zur flächendeckenden Datenspeicherung .....	56
3.2.4 Stichprobenvergleich .....	56
3.3 Hypothesenprüfung .....	58
4. Diskussion.....	60
4.1 Interpretation .....	60
4.2 Limitationen der Studie .....	65
5. Zusammenfassung und Abstract.....	66
5.1 Abstract .....	66
5.2 Zusammenfassung .....	67
6. Literaturverzeichnis.....	68
7. Tabellen- und Abbildungsverzeichnis.....	81
7.1 Tabellenverzeichnis .....	81
7.2 Abbildungsverzeichnis .....	82

8. Anhang.....	83
8.1 Korrekte Items der Skala Wissen (Turow et al., 2005) ..	83
8.2 Deutsche Übersetzung der Skala Wissen .....	83
8.3 Messinstrument .....	84
9. Lebenslauf.....	95

## 1. Einleitung und Problemstellung

Als Edward Snowden, ehemaliger US-Geheimdienstmitarbeiter, auf der Plattform WikiLeaks im Jahr 2013 erstmals geheime Dokumente zum Ausmaß der staatlichen Überwachung, Speicherung und Analyse von persönlichen Daten durch das Abhörprogramm *Prism* im Internet veröffentlichte, war die Medienresonanz groß. Beginnend mit *The Guardian* berichteten alle großen Zeitungen im In- und Ausland sukzessive von den Enthüllungen. Kaum ein europäischer IT-Nutzer hätte gedacht, dass die NSA ohne gerichtliche Anordnung Zugriff auf Echtzeitdaten aller online- (und Mobilfunk-) Kommunikation sowie direkten Zugriff auf die Server von Microsoft, Google, Facebook und anderer großer IT-Dienstleistungsunternehmen hat, unter der einzigen Bedingung, dass einer der beiden Teilnehmer sich in diesem Moment außerhalb der USA befindet (*The Guardian*, 2013). Zudem geht es hierbei nicht lediglich um Rohdaten oder Verbindungsnachweise, sondern um Inhalte von E-Mails, Ton- und Videospuren aus Chats, Fotos, Videos, Dokumenten, Details aus sozialen Netzwerken oder GPS Daten - also um die Privatsphäre. (Greenwald & McAskill, 2013)

Diese sensiblen Daten von Bürgern und Bewohnern der Europäischen Union scheinen seit 2007 von der US-amerikanischen Regierung überwacht worden zu sein. Ziel dieser Überwachung war nicht nur der Kampf gegen Terrorismus, sondern politische Spionage (Bigo et al., 2013).

Durch das Bekanntwerden dieser geheimdienstlichen Praktiken wurde eine Diskussion über Online Privatsphäre, soziale Netzwerke und Datenschutzrichtlinien in Medien und der breiten Öffentlichkeit angestoßen, der man sich kaum entziehen konnte. Während bis dahin häufig Soziale Netzwerke an den Pranger gestellt wurden, war nun klar, dass auch Regierungen und (ausländische) Regierungsorgane Privatbürger umfassend ausspionieren können.

Edward Snowden äußerte in einem Interview die Befürchtung, dass sich durch die Enthüllungen weder unser Verhalten online noch die institutionellen Überwachungsmethoden ändern werden (*The Guardian*, 2013). Die vorliegende Diplomarbeit beschäftigt sich genau mit diesem Thema: dem Einfluss der medialen Berichterstattung über Datenspeicherung und dem Einfluss von Persönlichkeitsfaktoren, Wissen über Praktiken und Rechtslage und das Ausmaß der Sorgen um die eigene Privatsphäre auf das protektive Verhalten von Internet-Nutzern.

## *1.1 Online Privatsphäre*

### *1.1.1 Definition von Online Privatsphäre*

Um über den Schutz und den Status quo der Privatsphäre in der heutigen Gesellschaft sprechen zu können, muss der Begriff zuerst definiert werden. Privatsphäre und die Privatheit persönlicher Daten (= information privacy) klar abzugrenzen ist schwierig, da das Konstrukt stark situationsabhängig ist und sich zudem mit dem gesellschaftlichen Wandel verändert (Sheehan, 2002). Alan Westin, eine der Schlüsselfiguren in der Privatsphären-Forschung, definiert sie wie folgt:

"[Privacy is] the claim of individuals, groups, or institutions to determine for themselves, when, how, and to what extent information about them is communicated to others." (Westin, 1970, Section One, zitiert nach Moloney & Bannister, 2008)

Wenn hier von Privatsphäre gesprochen wird, geht es also darum, dass ein Individuum (oder eine Gruppe, Institution, etc.) selbst entscheiden kann, wann welche Informationen über sie an wen herausgegeben werden. Im Einklang mit dieser Definition ist es das erklärte Ziel des Datenschutzrechts die informationelle Selbstbestimmung von Internet-Nutzern zu gewährleisten (Deutscher Bundestag, 2012).

Hoffman definierte Information Privacy zehn Jahre später auf der Basis von drei distinkten Rechten: das Recht eines

Individuums selbst zu entscheiden, welche Informationen es mit anderen teilen will, das Recht darauf zu wissen, welche Daten über ein Individuum gesammelt werden und schließlich das Recht darauf, auf die Daten zugreifen zu können, um die gesellschaftliche Ordnung aufrechtzuerhalten und den Staat zu regulieren (Hoffman, 1980, zitiert nach Sheehan, 2002). Auch in Hoffmanns Verständnis von Privatsphäre spielen somit Kontrollmöglichkeit sowie situative Bedingungen eine Rolle.

Regan (1995) postulierte Mitte der 70er Jahre, dass Privatsphäre das Recht darauf bedeuten solle, Informationen und den Grad der Zugänglichkeit zum Selbst durch Dritte kontrollieren zu können. Diese Definition impliziert, dass Privatsphäre eine Funktion aus individuellen Interessen und Wahlmöglichkeiten darstellt (Sheehan, 2002): der Wert von Privatheit wird gegen andere Werte, wie Pressefreiheit, Recht und Ordnung, oder nationale Sicherheit abgewogen (Regan, 1995). Und genau dies geschieht im online Kontext- persönliche Daten werden im Tauschhandel gegen Vorteile als Konsument (Wirtz, Lwin & Williams, 2007), den Zugang zu Kommunikationsmedien (Viseu, Clement & Aspirnall, 2004), oder als potenzieller Schutz vor Terroranschlägen (The Harris Poll, 2013) preisgegeben.

Der Schutz von Privatsphäre fordert also einerseits einen bewussten, aktiven Umgang mit den eigenen Daten von Online-Konsumenten und Internetnutzern, andererseits transparentes Vorgehen von Webseiten, um Nutzern alle relevanten Informationen über die potenziellen Risiken und Praktiken zu liefern.

### *1.2 Sorgen um die Privatsphäre*

Besorgnis von Internetnutzern um ihre Privatsphäre ist ein elementarer Bestandteil des Forschungsfeldes, und Faktoren die diese beeinflussen wurden zahlreich untersucht (e.g. Schwaig, Segars, Grover & Fiedler, 2013; Wu, Huang, Yen & Popova, 2012; Preisbusch, 2013; Yao & Linz, 2008; Zukowski & Brown, 2007).

*Website Privacy Concern*, also Misstrauen einer spezifischen Webseite gegenüber, ist zum Beispiel der stärkste Prädiktor des Willens von Konsumenten private Daten im Internet preiszugeben (Li, 2014). Generell machen sich Internetnutzer starke Sorgen darum, was mit ihren im Internet freiwillig oder unfreiwillig erhobenen Daten geschieht (e.g. Zukowski & Brown, 2007). Potenzielle Sicherheitsrisiken, die Nutzer nennen, sind Identitätsdiebstahl, Missbrauch von Kreditdaten (Buchanan, Paine, Joinson & Reips, 2007), die Nutzung persönlicher Informationen in falschem Kontext (e.g. Preibusch, 2013), aber auch die Angst vor staatlicher Überwachung (e.g. Siegel, 2013). Online-Shopper äußerten darüber hinaus sehr starke Sorgen (mit durchschnittlich 5.26 Punkten auf einer 7 pt.-Likert Skala) darüber, wie Unternehmen Konsumentendaten sammeln und untereinander austauschen (Yao & Linz, 2008).

### *1.3 Individuelle Differenzen in der Besorgnis*

Die Sorgen, die sich Internet-Nutzer um ihre persönlichen Daten machen, variieren über individuelle, kulturelle und demographische Unterschiede (e.g. Westin, 2003; Li, 2014; Zukowski & Brown, 2007). Der folgende Abschnitt gibt eine Übersicht über diese Differenzen.

#### *1.3.1 Fundamentalisten, Pragmatiker und Unbesorgte*

Westin fand heraus, dass sich Internet-Nutzer anhand ihrer Sorgen in drei distinkte Gruppen unterteilen lassen: die Privatsphäre-Fundamentalisten, die Unbesorgten und die Pragmatischen, deren Einstellung dazu, was privat ist, stärker situativ (abhängig von Trade-Offs) variiert (Westin, 2003). In der ursprünglichen Studie von 1995 ließen sich die Hälfte der Teilnehmer den Pragmatischen zuordnen, jeweils 25% des Samples den beiden anderen Gruppen (Westin, 2003). In darauf folgenden Studien wuchs der Anteil der Pragmatischen stetig, mit bereits 81% und nur drei Prozent Fundamentalisten im Jahr 2001 (Sheehan, 2002). Zahlreiche Studien nehmen seither diese oder eine

ähnliche Einteilung der Probanden zur weiteren Analyse der Daten vor. In einer aktuellen Studie fanden Smit, Noort und Voorveld (2014) eine Verteilung der Probanden mit 47% sehr Besorgten, 43% mittelmäßig Besorgten und nur 10% in der Gruppe der unbesorgten Versuchsteilnehmer vor. Dies lässt darauf schließen, dass sich die grundsätzliche Einstellung zum Thema Online-Privatsphäre tatsächlich im Laufe der Jahre verändert hat.

### *1.3.2 Kulturelle Unterschiede in Sorgen um die Privatsphäre*

Selbstverständlich besteht eine individuelle Tendenz, mehr, oder weniger besorgt um die eigenen Online-Daten zu sein, analog zu realen Bedingungen (Li, 2014; Yao, Rice & Wallis, 2007). Diese Prädispositionen sind zum Teil kulturell geprägt: Akzeptanz für staatliche Überwachung vor dem Hintergrund von Terrorbekämpfung ist beispielsweise in den USA weitaus höher als in Europa, obwohl sich die Unterschiede angleichen (vgl. The Harris Poll, 2013 und Hallinan, Friedewald & McCarthy, 2012). Das persönliche Bedürfnis nach sowie der Glaube an ein Recht auf Privatsphäre üben ebenso einen signifikanten Einfluss auf das Ausmaß der Sorgen um die eigene Online-Privatsphäre aus (Yao et al., 2007).

### *1.3.3 Der Einfluss von Persönlichkeit auf Besorgnis*

Auch Persönlichkeitsfaktoren haben einen signifikanten Einfluss auf unsere Wahrnehmung dessen, was privat bleiben sollte (e.g. Bansal, Zahedi & Gefen, 2010; Korzaan & Boswell, 2008; Junglas, Johnson & Spitzmüller, 2008). So führen höhere emotionale Instabilität und Verträglichkeit zu erhöhter Sensitivität die Privatsphäre betreffend und damit auch, ebenso wie eine stark ausgeprägte Gewissenhaftigkeit, zu mehr Sorgen (Bansal et al., 2010).

### *1.3.4 Alter, Bildung, Internet-Erfahrung*

Ältere Internet-Nutzer machen sich stärker Sorgen, während das Bildungsniveau einen negativen Zusammenhang mit dem Konstrukt *Privacy Concern* aufzeigt (Zukowski & Brown, 2007). Im Gegensatz

dazu scheint Internet-Erfahrung Besorgnis stärker zu schüren (Yao & Linz, 2008).

#### *1.3.5 Einfluss von Datenschutzrichtlinien auf Besorgnis*

Die Datenschutzrichtlinien einer Website haben ebenso Einfluss auf Besorgnis: Wird den Nutzern hier in Etwa die Möglichkeit gegeben, Daten, die über sie gesammelt wurden, einzusehen und gegebenenfalls zu korrigieren, schwächt dies ihre Sorgen; wird weiter angegeben, dass die Website Daten nicht weitergibt und Schritte einleitet, falls dies geschieht, hat das ebenso einen negativen, signifikanten Einfluss auf die Sorgen der Nutzer (Wu Huang & Popova, 2012).

#### *1.4 Der Einfluss von Sorgen um die Privatsphäre auf das Online-Verhalten*

Die Stärke der individuellen Besorgnis um *Information privacy* beeinflusst das Verhalten von Internetnutzern (e.g. Schwaig et al., 2012; Young & Quan-Haase, 2013). Individuen mit einem stärkeren Wunsch nach Privatsphäre weigern sich zum Beispiel häufiger persönliche Daten preiszugeben, lassen ihren Namen öfter von E-Mail-Verteilern löschen und beschweren sich bei Schwierigkeiten schneller bei Unternehmen, bzw. Regierungsabteilungen (Schwaig et al., 2013).

Individuen, die beginnen sich Sorgen um staatliche Überwachung zu machen, entwickeln wahrscheinlicher Sorgen um ihre Privatsphäre (Dinev, Hart & Mullen, 2008). Bei wahrgenommener Intrusion verstärken sich nicht nur die Sorgen, die Internetnutzer modifizieren auch ihr online Verhalten (Kateb, Rosen & Schauer, 2001). Rosen (2000) postulierte, dass sich diese Sorgen bei Betroffenen aus Angst davor entwickeln, dass Organe der Exekutive die gesammelten Daten außerhalb ihres ursprünglichen Kontextes bewerten und dadurch falsche Schlussfolgerungen ziehen könnten.

Sorgen treiben Internet-Nutzer auch dazu protektive Verhaltensmaßnahmen zu adaptieren (Buchanan et al., 2007). Fühlt man sich allerdings durch diese Vorkehrungen besser geschützt, sinken die Sorgen wiederum (Paine et al., 2007).

Es sei hier darauf hingewiesen, dass der Effekt zwischen Sorgen und Sicherheitsmaßnahmen über das Wissen um effektive Möglichkeiten mediiert wird: Studenten aus technischen Studiengängen weisen nicht nur mehr generelle Vorsicht im online-Kontext auf, sie schützen sich auch signifikant häufiger durch spezifische Software (Buchanan et al., 2007). Hui und Kollegen konnten aber keinen signifikanten Effekt der Sorgen von Internet-Nutzern auf die Menge von preisgegebenen persönlichen Daten finden (Hui, Teo & Lee, 2007).

Zudem ist die Verbindung zwischen Sorgen und Verhalten kontextabhängig und es ist kaum möglich ein allgemeingültiges Konzept überzustülpen (e.g. Smith, Dinev & Xu, 2011). Li (2014) postulierte, dass *website privacy concern* erhoben werden sollte, wenn das Verhalten auf einer spezifische Webseite von Online-Shops von Interesse ist, aber *online privacy concern*, wenn das Augenmerk auf der generellen Einstellung dem Internet gegenüber liegt. Die gewissenhafte Differenzierung von Konzeptionen und Quantifizierungen ist hier sehr wichtig.

### *1.5 Wahrnehmung institutioneller Datenspeicherung*

Ein Themenbereich, der gerade durch Whistleblower wie Edward Snowden vermehrt in den Fokus getreten ist, ist die institutionelle Datenspeicherung, sei es durch Regierungsorgane, Versicherungen oder zu ökonomischen Zwecken. Der bisherige Stand des Wissens hierbei wird im folgenden Kapitel dargestellt.

#### *1.5.1 Sorgen um institutionelle Datenspeicherung*

*Privacy Concerns* spielen eine wichtige Rolle dabei zu erklären, wie der Zusammenhang zwischen staatlichen Initiativen zur

Datenspeicherung und Internet-Nutzung bewertet wird (Dinev et al., 2008). Angst vor staatlicher Intrusion steht in statistisch signifikantem Zusammenhang mit Sorgen um die eigene Privatsphäre, was wiederum negativ mit dem Willen, Daten online preiszugeben, korreliert (Dinev et al., 2008). Trotzdem steht die Angst vor staatlicher Überwachung nicht in direktem Zusammenhang mit protektiven Handlungen (Dinev, Bellotto, Hart, Colautti, Russo & Serra, 2005).

Zudem entwickeln Personen, die ein stärker ausgeprägtes Bedürfnis nach staatlicher Kontrolle haben, weniger stark ausgeprägte Sorgen um ihre Privatsphäre (Dinev et al., 2008). Dieselben Individuen, die ein Überwachungsprogramm zum Schutz der nationalen Sicherheit unterstützen, sind dennoch gleichzeitig stark gegen ein solches Programm, wenn es an nicht-kriminelle US-Bürger gerichtet wird (Dinev et al., 2008). Allerdings werden solche Technologien schneller weiter entwickelt und in Gebrauch genommen, als das öffentliche Bewusstsein dafür wachsen kann, und die (US-amerikanische) Bevölkerung scheint bereit zu sein viele Aspekte ihrer Privatsphäre aufzugeben (Gelbord & Roelofsen, 2002).

### *1.5.2 Institutionen - Beschützer oder Angreifer der Privatsphäre?*

Unabhängig von persönlichem Hintergrund und Einstellungen die Privatsphäre betreffend besitzen Internet-Nutzer gleichzeitig zwei einander widersprechende Einstellungen: dass dieselben großen Institutionen einerseits dabei helfen ihre Online Privatsphäre zu schützen, aber andererseits Informationen an Dritte weitergeben ohne das Wissen oder die Zustimmung der Internet-Nutzer (Turow & Hennessy, 2007). Microsoft, der US-amerikanischen Regierung, Banken und Kreditinstitutionen sowie Internet-Providern wurde gleichzeitig zugetraut die Privatsphäre zu schützen und private Daten preiszugeben, obwohl (mit weniger als einem halben Skalenpunkt) signifikant häufiger der Schutz im

Vordergrund stehe (Turow & Hennessy, 2007). Doch es gibt Ausnahmen: Den Großen der Werbebranche wurde kaum eine Rolle im Schutz der Daten zugesprochen, während Entwickler von Software zum Schutz der Privatsphäre am wenigsten wahrscheinlich als Herausgeber von Daten eingeschätzt wurden (Turow & Hennessy, 2007). Diese Ergebnisse stimmen auch mit der Flash Eurobarometer Studie von 2008 überein, die unterschiedliche Levels von Vertrauen in verschiedene Institutionen aufdeckten. Medizinische Services wurden von 82% der Probanden als vertrauenswürdig eingestuft, was das Handling persönlicher Daten betraf, im Gegensatz zu nur 67% bei lokalen Autoritäten (The Gallup Organization, 2008).

### *1.5.3 Kosten-Nutzen-Abwägung: Privatsphäre vs. Nationale Sicherheit*

Nach den Terroranschlägen von 9/11 haben zahlreiche westliche Regierungen, die EU eingeschlossen, neue Maßnahmen im Kampf gegen Terror und Verbrechen eingeführt, die sich zum Großteil auf *surveillance-oriented security enhancing technologies*, kurz SOTS (überwachungsorientierte Technologien zur Verbesserung der Sicherheit) stützen (Rasmussen, 2006). Während von diesen Technologien nur erwartet wird, dass sie die nationale Sicherheit schützen, werden gewöhnliche Bürger mit einem zunehmenden Maß an Überwachung konfrontiert, das die Privatsphäre beeinträchtigen und Bürgerrechte verletzen kann (Levi & Wall, 2004).

Oft wird dieses Phänomen von einem Kosten-Nutzen-Standpunkt aus analysiert, der Privatsphäre und nationale Sicherheit gegenüberstellt, was durchaus kritisch gesehen werden kann (Pavone & Esposti, 2012). So fanden Pavone und Esposti (2012) an einer Diskussionsgruppe spanischer Probanden heraus, dass viele Internet-Nutzer es inakzeptabel finden, SOTS für staatliche oder kommerzielle Zwecke zu nutzen und dass ihnen bewusst ist, wie der Faktor Angst in der öffentlichen Diskussion zur Manipulation

genutzt wird; darüber hinaus waren den Teilnehmern klare Richtlinien zum Einsatz der Technologien wichtig.

Die Stichprobe war zudem in zwei distinkte Gruppen geteilt: Internet-Nutzer, die sich Sorgen um ihre Privatsphäre machen und daher staatliche Überwachung ablehnen, und vertrauensvolle Personen, die SOTS als effektive Maßnahmen zu ihrem eigenen Schutz bewerteten und sie schlussendlich auch nicht als Bedrohung ihrer Privatsphäre wahrnehmen (Pavone & Esposti, 2012).

An einem Sample von gut gebildeten College Studenten zeigten Hayes und Kollegen (2014), dass 78% dieser Gruppe die aktuell praktizierten Gesetze zum Schutz der individuellen Privatsphäre im Internet nicht nur zu schwach finden, sondern dass 62% der Probanden auch die Macht, die der US-amerikanischen Regierung im Zuge der Terrorbekämpfung in Bezug auf die Speicherung und Analyse privater Daten zur Verfügung steht, als zu stark empfinden (Hayes, Kesan, Bashir, Hoff & Joen, 2014).

Siegel (2013) untersuchte in einer quasi-experimentellen Studie die Wahrnehmung von institutioneller Datenspeicherung auf sozialen Netzwerken im Rahmen der Terrorbekämpfung; während Probanden in der Untersuchungsgruppe gefragt wurden „Stimmen Sie der Überwachung der Internet-Nutzung durch die Regierung vor dem Hintergrund der Terrorbekämpfung zu?“, beantworteten die Teilnehmer der Kontrollgruppe die Frage „Stimmen Sie der Überwachung von Internet-Nutzung durch die Regierung zu?“. Obwohl der Widerstand über beide Gruppen hinweg groß war, war er in der Kontrollgruppe signifikant höher (Siegel, 2013). Der Effekt wurde allerdings durch häufige Nutzung der Sozialen Netzwerke abgeschwächt (Siegel, 2013).

Ein interessanter Befund der Flash Eurobarometer Studie von 2008 ist, dass auch europäische Internet-Nutzer damit einverstanden seien, wenn geltende Datenschutzrichtlinien im

Kampf gegen internationalen Terrorismus gebogen oder ausgehebelt würden. 82% der Teilnehmer stimmten zu, dass es in diesem Fall möglich sein sollte Flug-Details zu überwachen, ebenso wie Telefongespräche (72%), Kreditkarteninformationen (69%) und Internetaktivitäten (75%) (The Gallup Organization, 2008). Allerdings betonte etwa ein Drittel der Stichprobe, dass dies nur bei ausreichendem Anfangsverdacht gelten sollte, und ca. 20% würden noch striktere Richtlinien anlegen (The Gallup Organization, 2008). Dabei war die Unterstützung für „uneingeschränkte Überwachung von persönlichen Daten“ bei Probanden aus Großbritannien und Ungarn mit 53% der Befragten am höchsten (The Gallup Organization, 2008).

#### *1.5.4 Einstellungen zur institutionellen Datenspeicherung im kulturellen Vergleich*

Lim, Cho und Sanchez stellten 2009 einen kulturellen Vergleich zur Akzeptanz von Regierungs-Überwachung (und der Einführung von Personalausweisen) in Bangalore, New York, Seoul, Singapur und Sydney an. Internet-Nutzer aus Seoul wiesen hierbei die am negativsten geprägte Einstellung auf, die indischen Teilnehmer aus Bangalor die positivste (Lim et al., 2009).

Auch Dinev und Kollegen (2005) bestätigten kulturelle Unterschiede in der Wahrnehmung von Überwachung. Kroatische Internet-Nutzer etwa zeigen sich kritisch, was die Effektivität von Überwachung angeht, sind aber nicht besorgt darüber (Budak, Anic & Rajh, 2013). Darüber hinaus differieren Überzeugungen über Datenspeicherungsaktivitäten im Zusammenhang mit Privatsphäre zwischen Subgruppen von Internet-Nutzern (Wirtz, Lwin & Williams, 2007). So sind auch in der kroatischen Bevölkerung Gegner von staatlicher Überwachung zu finden, die sich signifikant durch ihr Alter und Bildungsniveau von unbesorgten Nutzern unterscheiden; jüngere und gebildetere Personen weisen hier größeren Widerstand auf (Budak et al., 2013).

## *1.6 Protektive Strategien zum Schutz der Online Privatsphäre*

Häufig beschäftigen sich Studien lediglich mit einer oder wenigen Strategien zum Schutz der Privatsphäre und generalisieren ihre Ergebnisse dann auf „Protektive Verhaltensweisen“ im Allgemeinen (Phillips, 2004). Dies bildet zum einen nur einen kleinen Teil der tatsächlichen Verhaltensweisen ab, ist zum anderen problematisch, da es eine breite Varianz an schützenden Strategien für spezifische Probleme bzw. Ängste gibt, die auch selektiv genutzt werden könnten (Buchanan et al., 2006). Allgemein lässt sich sagen, dass die Nutzung von Schutzmaßnahmen trotz des Bewusstseins für die Problematiken des Datenschutzes im Internet relativ selten bleibt (Dommeyer & Gross, 2003).

Der folgende Abschnitt gibt einen Überblick über die technischen sowie andere Möglichkeiten zum Schutz der Online Privatsphäre, deren Nutzung in der Literatur bereits untersucht wurde.

### *1.6.1 Proaktive Strategien*

Technische Möglichkeiten, die zum Schutz der Privatsphäre genutzt werden können, wie etwa spezifische Software, die ein aktives Handeln (Einholen von Informationen, Installation, eventuell finanzieller Aufwand) vom Nutzer fordern, werden als Proaktive Strategien bezeichnet (Cho Rivera-Sánchez & Lim, 2009).

Die Adaption protektiver Strategien, wie z.B. Verschlüsselung von Daten oder Verwendung von Anti-Phishing-Programmen, wird zu einem guten Viertel durch die Intention sich zu schützen determiniert; die Intention ist abhängig von drei Hauptfaktoren: einer wohlwollenden Sichtweise der möglichen Sicherheitsstrategien (abhängig vom Bedürfnis nach Privatheit,

Selbstwirksamkeitserwartung und persönlichen Werten), wahrgenommener Kontrollierbarkeit (in diesem Fall gleichzusetzen mit der Annahme, die Strategien wirksam ausführen zu können) und einer hohen Selbstwirksamkeitserwartung (Yao & Linz, 2008). Personen die bereits eine schlechte Erfahrung mit z.B. Computer-Viren gemacht haben, sind besonders motiviert ihren Computer nach außen hin zu schützen, ebenso wie Individuen, die riskantes Internet-Verhalten, wie z.B. illegale Downloads, betreiben (Bubaš, Orehovacki & Konecki, 2008). Zudem besteht ein signifikanter Unterschied in der Häufigkeit der Nutzung zwischen jungen Erwachsenen und älteren Internet Nutzern, hier wird vom *Age Divide* gesprochen (e.g. Litt, 2013).

Paine und Kollegen (2007) fanden heraus, dass 73% der Internet-Nutzer ihre Privatsphäre online aktiv schützen und zwar die Individuen, die mehr Zeit im Internet verbringen. In dieser Studie waren die zwei am häufigsten berichteten protektiven Strategien die Nutzung von Firewalls und Anti-Virus-Programmen (Paine, Reips, Stieger, Joinson & Buchanan, 2007).

Smit, Van Noort und Voorveld untersuchten 2014 in einer großangelegten Studie mit über 2000 Teilnehmern, welche protektiven Maßnahmen Internetnutzer zum Schutz der Online-Privatsphäre nutzen. Die Probanden wurden nach der Häufigkeit gefragt, mit der sie gewisse Strategien anwenden. Die Stichprobe versuchte sich am häufigsten durch die folgenden Methoden zu schützen: Überprüfen, ob Spyware installiert wurde, das Blockieren von Pop-Ups, das Löschen der Browser History oder von Cookies (Smit et al., 2014). Die am seltensten angewandte Schutzmaßnahme war in Smits Studie das tatsächliche Lesen von Datenschutzrichtlinien einer Webseite (obwohl dies oft Bedingung für eine Registrierung ist). Das zeigte sich auch in anderen Studien, e.g. bei Custers, Hof, Schermer, Appelby-Arnold und Brockdorf (2013), wobei 54% der Probanden die *Privacy Policies* einer Webseite „selten“ bis „nie“ lasen und 73% die Allgemeinen

Geschäftsbedingungen „manchmal“ bis „nie“. Haynes und Kollegen erfragten die Gründe hierfür: 81% der Probanden gaben an die *Privacy Policies* deshalb nicht zu lesen, weil sie ihnen zu lang waren (Hayes et al., 2014).

Park (2011) beforschte Online-Privatsphäre dahingehend, wie Internet-Nutzer die Veröffentlichung eigener Daten kontrollieren. Hierfür teilte er protektive Verhaltensweisen in eine soziale und eine technische Dimension, wobei erstere nochmals in aktive und passive Kontrolle unterteilt wurde, erhoben in Häufigkeiten und Intensität der Nutzung (Park, 2011). Die Skala zur technischen Dimension der Informationsfluss-Kontrolle beinhaltete Fragen nach ähnlichen Verhaltensweisen wie bei Smit und Kollegen (2014): Löschen der Browser History, Management von unerwünschten E-Mails oder aber die Nutzung von Verschlüsselungs-Software. Die Skala zur sozialen Dimension der Informationsflusskontrolle enthielt wie bereits erwähnt aktive und passive Subskalen; zur passiven, sozialen Informationsflusskontrolle gehören Rückzug, Vermeidung und Identitätsverschleierung, zur aktiven Beschwerden, Richtigstellung und Nutzung mehrerer Accounts (Park, 2011).

Die meisten Probanden griffen nur selten auf Schutzmaßnahmen der technischen Dimension (über Browser-Applikationen, bzw. *Privacy Enhancing Technologies*) zurück, die Kontrolle des Informationsflusses stellte sich also in dieser Dimension gering dar. Gleiches gilt für die aktive soziale Informationsflusskontrolle. Praktiken der passiven sozialen Kontrolle wurden aber moderat bis häufig genutzt. (Park, 2011)

Die Rolle von technischer Vertrautheit, Bewusstheit von Überwachungspraktiken und des Verstehens von Datenschutzrichtlinien auf das Kontrollverhalten wurden bestätigt (Park, 2011). Allerdings wurden die Effekte dieser wissensbezogenen Kategorien auf das Verhalten durch das Alter mediiert: Alter war die Variable, die das Kontroll-Verhalten am

konsistentesten erklären konnte, mit weniger adaptierten protektiven Strategien, je älter ein Proband ist.

### *1.6.2 Protektive Strategien in Sozialen Netzwerken*

Im Bereich der Sozialen Netzwerke lassen sich weitere Strategien zum Schutz der Privatsphäre erkennen. Stutzman, Capra und Thompson (2011) ermittelten an einer relativ kleinen (N = 122), hauptsächlich weiblichen Stichprobe von Collegestudenten, dass 77% des Samples ihre Einstellungen zum Schutz der Privatsphäre auf Facebook (Privacy Settings) an ihre Bedürfnisse angepasst haben und weitere 15% zusätzlich festlegten, welchen Personen ihrer Kontaktliste bestimmte Beiträge zugänglich sind. Weiter restringieren knapp 80% der Facebook-Nutzer den Zugang zu ihrem Profil und Fotos (Young & Quan-Haase, 2013). Die Nutzung falscher Informationen, wie eines Alias statt des richtigen Namens, wird im Rahmen sozialer Netzwerke ebenso als häufige Schutzstrategie genutzt (Lenhart & Madden, 2007; Hoy & Milne, 2010).

### *1.6.3 Weitere Strategien*

Weitere, nicht proaktive Strategien lassen sich unter den Kategorien Vermeidungsstrategien (z.B. kein online-Banking zu benutzen), bzw. „Opt-out“-Strategien (in etwa ablehnende, verweigernde Strategien) zusammenfassen (Cho et al., 2009). Dabei gehört *Opt-out* über Kulturkreise hinweg zu den am häufigsten genutzten Maßnahmen (gefolgt von Proaktiven)-vermutlich da sie wenig technisches Verständnis und kaum Zeitaufwand erfordern (Cho et al., 2009).

Die wohl effektivste protektive Maßnahme ist dabei Selbstzensur, die bisher aber nur in einer Studie von 18 Kunststudenten eingehend untersucht wurde; Selbstzensur wurde in diesem Sample bei einer Varianz an Themen genutzt, allerdings hauptsächlich mit dem Ziel dem erwünschten transportierten Selbstbild auf Facebook gerecht zu werden (Sleeper, Balebako, Das, McConahy, Wiese & Cranor, 2013).

Auch außerhalb von Sozialen Netzwerken versuchen Internet-Nutzer ihre Privatsphäre zu schützen. Die am häufigsten angewandten Strategien von Teenagern sind das Angeben unwahrer Informationen und die Bemühung, ihre Namen aus E-Mail Verteilern löschen zu lassen (Moscardelli & Divine, 2007).

In der Eurobarometer-Erhebung 359 (2010) gaben nur 15% der Internet-Nutzer an, gar nichts zu tun, um ihre Privatsphäre zu schützen. Auch Strategien, die hier noch nicht erwähnt wurden, wie das Bereitstellen inkorrektter Informationen, die Weigerung Daten herauszugeben oder das Vermeiden von Situationen, in denen es erforderlich wäre Daten preiszugeben, wurden betont (TNS Opinion & Social, 2010).

## *1.7 Die Datenschutzrichtlinien der EU*

### *1.7.1 Innereuropäischer Datenverkehr*

Um fundiert über Online-Privatsphäre sprechen zu können, soll hier ein kurzer Abriss der relevanten rechtlichen Grundlagen auf EU-Ebene gegeben werden.

Gemäß Artikel 8 der Europäischen Menschenrechtskonvention ist das Recht auf Schutz vor der Erhebung und Verwendung personenbezogener Daten Teil des Rechts auf Achtung des Privat- und Familienlebens, der Wohnung und der Korrespondenz und ist als das Recht auf Datenschutz im europäischen Grundrecht verankert (Agentur der Europäischen Union für Grundrechte, 2014). Hierbei werden personenbezogene Daten nach dem (deutschen) Datenschutzgesetz als un-anonymisierte Einzelangaben über persönliche, oder sachliche Verhältnisse einer bestimmten, oder bestimmbaren natürlichen Person definiert; mit Einzelangaben kann eine breite Varianz an Informationen gemeint sein, von äußeren Erscheinungsmerkmalen bis hin zu politischen Meinungen oder Beziehungen zu Dritten (Betz und Kübler, 2013). Die Regulierung betrifft die Erhebung, Speicherung, Sperrung und Löschung (=automatisierte und manuelle

Verarbeitung) dieser Daten (Betz und Kübler, 2013, p. 162). Es handelt sich hierbei allerdings nicht um ein absolutes Recht, sondern um eines, das gesamtgesellschaftlichen Interessen wie dem Schutz von Rechten und Freiheit gegenübergestellt werden muss (Agentur der Europäischen Union für Grundrechte, 2014).

Für die Verarbeitung personenbezogener Daten muss eine Einwilligung in voller Sachkenntnis und im konkreten Fall vom Betroffenen vorliegen, die nicht unter Druck erlangt wurde (AUEG, 2014, S. 61); die Betroffenen müssen angemessen über Zweck und Konsequenzen der Verarbeitung informiert worden sein (AEUG, 2014, S. 50). Dabei muss gewährleistet sein, dass die Daten auf dem neuesten Stand und sachlich richtig verarbeitet werden; es besteht ein Recht darauf bei Antrag zu erfahren, welche Daten gesammelt und verarbeitet wurden. Werden Verarbeitungsvorgänge hinzugefügt oder unabsehbar verändert, muss eine erneute Einwilligung eingeholt werden, die auch jederzeit zurückgenommen werden kann; dies gilt auch für die Weitergabe der Daten an Dritte (AUEG, 2014, S. 65). Zusätzlich müssen Daten wieder gelöscht werden, sobald sie verarbeitet wurden (AEUG, 2014, S. 119).

### *1.7.2 Grenzüberschreitender Datenverkehr*

Im Rahmen der vorliegenden Arbeit ist auch grenzüberschreitender Datenverkehr von Relevanz. Beim freien Datenverkehr mit Drittländern (also Nicht-EU-Staaten) muss kein gleichwertiger, sondern nur ein angemessener Maßstab an den Datenschutz gelegt werden (AUEG, 2014, S. 149).

Mit den USA gemeinsam wurden die „Grundsätze des sicheren Hafens“ (*Safe Harbour Privacy Principles*) erarbeitet, ein für US-Unternehmen geltender Verhaltenskodex. Auch ohne angemessenes Datenschutzniveau können dadurch Daten an Drittländer weitergegeben werden, wenn die betroffene Person ohne jeden Zweifel in den Datenexport eingewilligt hat. (AUEG, 2014)

### *1.7.3 Elektronische Kommunikation*

In der „Datenschutzrichtlinie für elektronische Kommunikation von 2009“ wird zwischen drei Kategorien von Daten differenziert. Die Daten, die den Inhalt der Kommunikation ausmachen, unterliegen absoluter Vertraulichkeit. Sogenannte Verkehrsdaten (z.B. Partner und Dauer einer Kommunikation) dürfen, abgesehen von Abrechnungszwecken oder dem Bereitstellen von Diensten, nur mit Einwilligung verarbeitet werden; dasselbe gilt für jene Verkehrsdaten, die über den Standort eines Nutzers informieren. Die Verwendung von Cookies ist nur dann zulässig, wenn die ausdrückliche Erlaubnis von Internet-Nutzern eingeholt wurden; außerdem stellt die Vorratsdatenspeicherung von Telekommunikationsdaten ausdrücklich eine Verletzung des Rechtes auf Datenschutz dar, was nur durch den Schutz höherer Güter gerechtfertigt werden kann. (AUEG, 2014)

### *1.8 Wissen um rechtliche Grundlagen der Datenspeicherung*

In einer breit aufgestellten, telefonisch administrierten Studie des Annenberg Public Policy Centers mit 1500 Teilnehmern untersuchte Turow unter anderem das vorhandene Wissen US-amerikanischer, erwachsener Internet-Nutzer über rechtliche Grundlagen, die den Datenschutz und Konsum im Internet betreffen (Turow, Feldman & Meltzer, 2005). Hierfür entwickelten Turow und Kollegen eine Skala, die mit 17 True/False-Items die rechtlichen Bestimmungen alltäglich relevanter Datensammelungs-Praktiken von z.B. Banken und kommerziellen Webseiten abfragt. 80% des Samples war bewusst, dass Firmen ihr Verhalten online verfolgen können, und 62% wussten ebenso, dass Firmen einsehen können, ob eine E-Mail von ihnen geöffnet wurde, auch wenn der Konsument nicht darauf reagiert (Turow & Hennesy, 2007). Etwa der Hälfte der Teilnehmer war darüber hinaus bekannt, dass Firmen Konsumenten-Daten mit ihren Tochtergesellschaften ohne Erlaubnis teilen dürfen, dass Zeitschriften-Verlage Daten ohne Erlaubnis

verkaufen können und dass Konsumenten die Daten, die über sie gesammelt wurden, nicht zur Einsicht bereitgestellt geschweige denn gelöscht werden müssen (Turow et al., 2005). Dies bedeutet aber auch, dass die andere Hälfte der Nutzer in dieser Studie kein Wissen darüber besitzt. Ein weiteres alarmierendes Ergebnis der Befragung war, dass 75% der Internet-Nutzer nicht klar ist, dass die bloße Existenz einer Datenschutzrichtlinien nicht damit gleichzusetzen ist, dass die Website keine Daten weitergibt (Turow et al., 2005).

Park (2011) nutzte dieselben Skalen wie Turow und Kollegen (2005), um das Wissen der Probanden über Überwachungspraktiken und Datenschutzgesetze zu erfassen. Zwar haben Internet-Nutzer ein basales Verständnis davon, wie Daten online erhoben und genutzt werden, allerdings missverstanden mehr als 40% der Probanden die grundlegendsten Datensammlungs-Praktiken von Institutionen (Park, Campbell & Kwak, 2012). Darüber hinaus konnten lediglich 8 der insgesamt 419 Teilnehmer alle Fragen zu den Datenschutzgesetzen richtig beantworten; hier sei darauf hingewiesen, dass es sich bei dem Panel um eine leicht überdurchschnittlich gebildete Gruppe handelte (Park et al., 2012).

Hayes und Kollegen (2014), ein Team aus Juristen sowie Psychologen, erfassten das Wissen der Probanden über unterschiedlich Kategorien: *Cloud Computing*, *Online Security*, *Economics*, *Educational Records* und *Legal Aspects*. Während die Teilnehmer mit durchschnittlich 75-78% richtiger Antworten relativ gut über die ersten Kategorien Bescheid wussten (am höchsten war das Niveau bei Fragen zu wirtschaftlichen Praktiken), kannten sie durchschnittlich nur 49% der korrekten Antworten zur rechtlichen Lage des Datenschutzes (Hayes et al., 2014).

Der Zusammenhang zwischen dem Wissen um rechtliche Grundlagen beim Datenschutz im Internet und dem online Verhalten

ist bisher noch nicht erschöpfend untersucht; Smit und Kollegen (2014) konnten bei europäischen Internet-Nutzern allerdings keinen signifikanten Zusammenhang zwischen Wissen (erhoben mit Turows Items) und dem Aufnehmen protektiver Verhaltensweisen beobachten.

### *1.9 Der Einfluss von Persönlichkeitsfaktoren auf das Online-Verhalten*

Die Rolle von Persönlichkeitsfaktoren, also über Situationen und Zeit stabile individuelle Dispositionen, die das Auftreten einer Verhaltensweise mehr oder weniger wahrscheinlich machen (e.g. Ajzen, 1988, zit. nach Junglas, Johnson & Spitzmüller, 2008), wurde im Zusammenhang mit der Informationsflusskontrolle von Internet-Nutzern untersucht (e.g. Bansal et al., 2010).

Unsere Persönlichkeit beeinflusst zum Beispiel, als wie sensibel wir Daten über uns wahrnehmen. Bansal und Kollegen (2010) ermittelten einen starken signifikanten Einfluss von Neurotizismus und einen schwachen für Verträglichkeit darauf, wie sehr Individuen gesundheitsbezogene Daten als privat wahrnehmen, was wiederum signifikant mit dem Ausmaß der Besorgnis um diese Daten korreliert. Der Einfluss von Extraversion und Gewissenhaftigkeit erreichte hingegen nicht das Signifikanzniveau. (Bansal et al., 2010)

Junglas et al. (2008) untersuchten an Universitätsstudenten den Einfluss der Big 5 Persönlichkeitsfaktoren (Neurotizismus, Gewissenhaftigkeit, Verträglichkeit, Extrovertiertheit und Offenheit für neue Erfahrungen) auf *Privacy Concerns* bezüglich *Location based services* (LBS). LBS sind in das Mobiltelefon integrierte GPS Sender, die den Standort einer Person genau bestimmen können (Junglas et al., 2008). Die Faktoren Verträglichkeit, Gewissenhaftigkeit und Offenheit für neue Erfahrungen wiesen einen signifikanten Einfluss auf die Privacy Concerns der Studienteilnehmer in Bezug auf LBS auf (Junglas et

al., 2008). Je verträglicher (harmoniebedürftiger) eine Person ist, desto schwächer fallen die Sorgen um die eigene Privatsphäre aus; je gewissenhafter (organisierter, strukturierter) ein Smart-Phone-Nutzer ist und je offener er für neue Erfahrungen ist, desto stärker sorgt er sich um seine privaten Daten (Junglas et al., 2008). Obwohl das Modell von Junglas und Kollegen nur eine Erklärungsmacht von  $R\text{-quadrat}=11\%$  besitzt, trägt dies statistisch signifikant zur Erklärung des Ausmaßes der Sorgen um Privatsphäre bei. In dieser Studie wurden die Persönlichkeitsfaktoren als Intrapersonelle Informationsquelle im Rahmen der Theorie der Schutzmotivation untersucht (Junglas et al., 2008).

In einer ebenfalls 2008 erhobenen Untersuchung ermittelten Korzaan und Boswell nur für den Faktor Verträglichkeit einen signifikanten Einfluss auf die Sorgen um Informationsprivatheit, im Gegensatz zu Junglas und Kollegen (2008) allerdings einen gegenteiligen, nämlich positiven Einfluss (Korzaan & Boswell, 2008). Dies könnte mitunter den unterschiedlichen Instrumenten zur Erhebung der Persönlichkeitsfaktoren („A very brief measure of the Big-5 personality domains“, Gosling, Rentfrow & Swann, 2003, vs. Items aus „The International Personality Item Pool“, Goldberg, Johnson, Hogan, Eber, Cloninger & Gough, 2006), aber auch den situativen Bedingungen (Smart-Phone vs. Internet-Nutzung vom Heimgerät) geschuldet sein.

### *1.10 Forschungshypothese und weitere Fragestellungen*

Nachdem Edward Snowden im Sommer 2013 geheime Dokumente der NSA auf WikiLeaks veröffentlicht hatte, entstand in Fernsehen, Radio, Zeitungen sowie in der breiten Öffentlichkeit eine Diskussion über Online-Privatsphäre und die Gefahren von flächendeckender Datenspeicherung, bzw. von Überwachung aller Bürger durch in- und ausländische Geheimdienste (e.g. Gidda, 2013). Obwohl die Einstellung von Internet-Nutzern zur Privatsphäre (e.g. Buchanan et al., 2006; Hallinan et al., 2012;

Li, 2014; Smit, 2014) und ihrer Möglichkeiten diese zu schützen (e.g. Paine et al., 2008; Park, 2011; Sleeper et al., 2013; Yao & Linz, 2008) in der Literatur bereits erörtert wurden, steht die europäische Gesellschaft nun an einem ganz besonderen Punkt in der Geschichte: In der gesamten europäischen Bevölkerung wurde ein Bewusstsein für die Gefahren des Internets, abseits von rein kommerziellen Interessen der Datensammlung, geschaffen. Die vorliegende Arbeit versucht daher aufzuklären, inwieweit die Furcht-Appelle von Politik, Experten und Medien tatsächlich zu einer Verhaltensänderung der Bürger geführt haben. Daraus ergibt sich folgende Forschungsfrage:

*Hat sich das Ausmaß der Anwendung protektiver Verhaltensweisen von Internet-Nutzern zum Schutz der Online-Privatsphäre durch die mediale Berichterstattung über potenziell flächendeckende Datenspeicherung verändert?*

Intrapersonelle Informationsquellen, wie etwa Persönlichkeitsfaktoren, haben einen Einfluss darauf wie wahrscheinlich ein gewisses Verhalten adaptiert wird (Ajzen, 1988, zit. nach Junglas et al., 2008). Diese Faktoren beeinflussen das Maß, in dem Internet-Nutzer Daten als sensibel wahrnehmen (Bansal et al., 2010) und wie stark sich Sorgen um die Privatsphäre ausprägen (Junglas et al., 2008). Dies führt zur Hypothese:

*Persönlichkeitsfaktoren sind ein Prädiktor für das Ausmaß der Änderung in der Nutzung protektiver Verhaltensweisen zum Schutz der Online-Privatsphäre.*

Der Wissensstand um aktuell praktizierten Datenschutz in der allgemeinen Bevölkerung ist alarmierend gering (Turow et al., 2005). Die Ergebnisse zum Einfluss dieses Wissens auf protektive Verhaltensweisen stellen sich in der Literatur als ambivalent dar. Technisch versierte Studenten schützen sich zum Beispiel signifikant häufiger durch spezifische Software

(Buchanan et al., 2007), während an anderen Stichproben kein signifikanter Zusammenhang zwischen Wissen und protektiven Verhaltensweisen ermittelt werden konnte (Smit et al., 2014). Die Analyse der nachfolgenden Hypothese kann also einen weiteren Beitrag zur Klärung dieses Phänomens beitragen:

*Das Wissen um Datenschutz ist ein Prädiktor für das Ausmaß der Veränderung in der Nutzung protektiver Verhaltensweisen zum Schutz der Online-Privatsphäre.*

Diverse Studien (e.g. Schwaig et al., 2012; Young & Quan-Haase, 2013) ermittelten einen Einfluss von Sorgen auf das Online-Verhalten bzw. den Schutz der Privatsphäre. Dies führt zu folgender Annahme:

*Besorgnis ist ein Prädiktor für das Ausmaß der Änderung in der Nutzung protektiver Verhaltensweisen zum Schutz der Online-Privatsphäre.*

Unser Erinnerungsvermögen ist Verzerrungseffekten, wie dem „Knew-it-all-along“-Effekt unterworfen (Hasher, Attig & Alba, 1981). Da in der folgenden Untersuchung zum einen nach bereits vergangenen Verhaltensweisen gefragt wird und zum anderen viele Personen im Zuge der medialen Berichterstattung über bis dahin nicht offiziell bestätigte Datensammelpraktiken behaupteten, dass ihnen diese Informationen sowieso „schon immer klar gewesen“ wären, ergibt sich die nächste Hypothese:

*Der „Knew-it-all-along“-Effekt ist ein Prädiktor für das Ausmaß der Änderung in der Nutzung protektiver Verhaltensweisen zum Schutz der Online-Privatsphäre.*

Da sich die vorliegende Studie mit protektivem Verhalten im Internet beschäftigt stellt sich die Frage, ob besonders vorsichtige Internet-Nutzer überhaupt gewillt sind solch sensible Informationen in einem online-Kontext preiszugeben. Dies ist besonders in Hinblick auf zukünftige Untersuchungen von

großer Bedeutung, aber ebenso für die adäquate Interpretation der Ergebnisse wichtig. Um dies zu ermitteln wurde zusätzlich zum Online-Fragebogen auch im Paper-Pencil Format erhoben, was zu zwei unabhängigen Stichproben führt. Die nächste Forschungshypothese ist demnach folgende:

*Die Antworten der Untersuchungsteilnehmer der beiden Stichproben unterscheiden sich.*

Des Weiteren wird unsere Lebenszufriedenheit unter anderem durch das Ausmaß beeinflusst, in dem wir uns als „freie Menschen“ fühlen; es wäre also möglich, dass die mediale Berichterstattung und die daraus resultierenden Sorgen von Internet-Nutzern diese beeinflussen, was uns zur letzten Forschungshypothese führt:

*Die Lebenszufriedenheit von Internet-Nutzern steht im Zusammenhang mit der medialen Berichterstattung über potenziell flächendeckende Datenspeicherung und den damit zusammenhängenden Befürchtungen um die Online-Privatsphäre.*

## 2. Methode

### 2.1 Design

Bei der vorliegenden Untersuchung handelt es sich um einen quasiexperimentellen Zwei-Gruppen-Versuchsplan mit einer abhängigen Variable und 13 unabhängigen Variablen. Diese sind:

#### 1. Abhängige Variable:

- Ausmaß der Änderung in der Nutzung protektiver Verhaltensweisen:  $M_{Nachher} - M_{Vorher}$

#### 2. Unabhängige Variablen/Prädiktoren:

- Intensität der Beschäftigung mit der medialen Berichterstattung: *Medienkonsum*
- Wissen um Risiken der Datensammelpraktiken und deren rechtliche Grundlagen: *Wissen*

- Einstellung in Bezug auf die Überwachung von Internet-Aktivitäten: *Besorgnis, Kognitive Bewertung, Politische Bedenken.*
- Die Big 5: *Neurotizismus, Extraversion, Offenheit für neue Erfahrungen, Gewissenhaftigkeit* und *Verträglichkeit.*
- Protektives Verhalten vor der Berichterstattung: *M\_Vorher*
- Protektives Verhalten nach der Berichterstattung: *M\_Nachher*
- „Knew-it-all-along“-Effekt: Knew-it-all-along
- Lebenszufriedenheit: *SWL* (=Satisfaction with life)

Da sich der Einfluss der unabhängigen Variablen den Kontrollmöglichkeiten der Studienleiterin entzieht, handelt es sich um eine Felduntersuchung. Die Zuteilung der Untersuchungsteilnehmer zur Online- bzw. Paper-Pencil Stichprobe geschah im Sinne einer anfallenden Stichprobe.

## 2.2 Untersuchungsteilnehmer

Die Stichprobe umfasst 755 Versuchsteilnehmer, wobei 83% online (627 Personen) und 128 Personen (17%) über das Paper-Pencil-Format erhoben wurden.

Es handelt sich um eine eher weibliche (56.8%) gut gebildete (90% mit Matura bzw. Hochschulabschluss) Stichprobe aus überwiegend deutschen (64.1%) und österreichischen (27%) Probanden. Der Mittelwert des Alters beträgt 32.41, der Median 26. Knapp 65% der Befragten befanden sich zum Zeitpunkt der Erhebung in einer festen Beziehung, knapp mehr als die Hälfte lebt in einer Großstadt oder Metropole. Generalisierungen auf die Gesamtbevölkerung sollten daher kritisch geprüft werden (für eine ausführliche Darstellung siehe Kapitel 3.1.1).

## *2.3 Messinstrument*

Da im Anhang nur der selbstentworfen Teil des Instrumentes enthalten ist soll hier darauf hingewiesen werden, dass die Teile sich wie folgt nacheinander reihen: Demographische Daten, Wissen, Internetnutzung, Medienkonsum, „Knew-it-all-along“-Effekt, Protektive Strategien, Big 5, Besorgnis, SWL.

### *2.3.1 Demographische Daten*

Zur Untersuchung der interessierenden Kriterien wurde ein online und offline administrierter Fragebogen entwickelt. Der Fragebogen (siehe Anhang, S. 84) erhebt anfangs demographische Daten (Alter, Geschlecht, Bildungsgrad, Englisch-Kenntnisse, Staatsbürgerschaft, Familienstand, Wohnort), sowie deskriptive Daten das Internet-Verhalten betreffend (Zugang, typisches Verhalten, Nutzung von Online Social Networks).

Die weiteren Skalen des Fragebogens werden im Folgenden genauer beschrieben.

### *2.3.2 Medienkonsum*

Um den Einfluss der medialen Berichterstattung auf die Verhaltensänderung untersuchen zu können enthält der FB die Skala „Medienkonsum“, welche mit 7 Items erhoben wird. Ausgehend von der Frage, ob die mediale Berichterstattung über die Möglichkeiten der Überwachung, Speicherung und Analyse von Internet-Aktivitäten mit Interesse wahrgenommenen wurde (auf einer 5-stufigen Likert-Skala (von „nein“ über „eher nein/ja“ bis „ja“), wird erfragt, welche Medien in welcher Intensität (5-stufige Likert-Skala von „gar nicht“ über „kaum“, „etwas“, „überwiegend“ bis „sehr“) aktiv genutzt wurden, um weitere Informationen zu erhalten. Zur Verrechnung wurde die Summe der Werte der einzelnen Items gebildet, wodurch sich ein Bereich zwischen 7 (geringe Beschäftigung mit der medialen Darstellung) und 35 (sehr intensive Beschäftigung) ergibt.

### 2.3.3 Big 5

Um den prädiktorischen Wert von Persönlichkeitsfaktoren erheben zu können wurde ein Kurz-Fragebogen zur Erfassung von Persönlichkeitsfaktoren, der Big Five Inventory-SEOP (BFI-S), in der deutschen Übersetzung von Gerlitz und Schupp (2005) herangezogen. Das Modell der Big 5 ist ein weithin akzeptiertes Rahmenmodell zur Beschreibung von Persönlichkeit (John, Naumann, & Soto, 2008).

Der Fragebogen erhebt die Persönlichkeitsdimensionen Neurotizismus, Extraversion, Offenheit für neue Erfahrungen, Verträglichkeit und Gewissenhaftigkeit in 7-stufigem Antwortformat von (1) trifft überhaupt nicht zu bis (7) trifft voll zu (Schupp und Gerlitz, 2008). Die Auswertung erfolgt gemäß Dehne und Schupp (2007).

Die Reliabilitäten der Items variieren mit Cronbachs Alpha zwischen 0.53 und 0.7; die Skalen Verträglichkeit, Neurotizismus und Extraversion sind nicht hinreichend konsistent, was laut Autoren allerdings an der geringen Item-Anzahl liegt (Schupp und Gerlitz, 2008). Diskriminante Validität und konvergente Validität im Verhältnis zum (gut etablierten) NEO-PI-R sind jedoch trotzdem gegeben (Hahn, Gottschling & Spinath, 2012). Der BFI-S wurde als über Erhebungskontexte robust bestätigt, sowohl computer-unterstützt als auch selbst-administriert (Lang, John, Lüdtke, Schupp & Wagner, 2011).

### 2.3.4 Besorgnis

Die Besorgnis der Studienteilnehmer um ihre Online Privatsphäre und damit zusammenhängende Themen wird mit 12 Items erhoben, die teilweise affektive, teilweise kognitive Aspekte berücksichtigen. Da die Skala keinem vorherigen Fragebogen folgt, wurde eine Faktorenanalyse durchgeführt. Die Ergebnisse hierzu und die resultierenden Faktoren werden im Abschnitt 3.2.1 genau dargestellt.

Beispiel-Items für die Skala sind „Ich mache mir Sorgen um die Macht, die die Regierung hat um online Aktivitäten aufzuzeichnen.“, oder „Die Möglichkeit der flächendeckenden Datenspeicherung aller Online-Aktivitäten durch Regierungen finde ich angemessen.“

Alle Items sind auf einer 5-pt.-Likert Skala von (1) *starke Ablehnung* bis (5) *starke Zustimmung*, bzw. von „stimme nicht zu“ über „stimme eher nicht zu“, „teils teils“, bis „stimme eher zu“ und „stimme zu“ einzuschätzen.

#### 3.4.5 Wissen

Um das Wissen im Bereich des Online-Datenschutzes abzufragen wird hier die Knowledge-Skala von Turow und Kollegen (2005) herangezogen. Sie erfasst in 15 Items relevantes Wissen über Risiken der Datensammlung (8 Items) und deren rechtliche Grundlagen (7 Items) in einem dichotomen Ja/Nein-Antwortformat, plus der Ausweichoption „Ich weiß es nicht“, welche in der Auswertung zur Kategorie „falsch“ gezählt wird (Turow et al., 2007). Zur Verrechnung wird eine Gesamtsumme der richtigen Antworten gebildet, womit sich ein potenzieller Wertebereich zwischen 0 und 15 ergibt. Die Skala besitzt eine gute Reliabilität mit einem Cronbachs Alpha von 0.74 (Turow et al., 2005). Die Antworten wurden für die vorliegende Arbeit im Einklang mit der europäischen Datenschutzrichtlinie statt dem US-amerikanischen Vorbild ausgewertet (korrekte Antworten siehe Anhang, S. 83).

#### 2.3.6 Protektive Strategien

Mit insgesamt 45 Items (siehe Anhang, S. 87 ff.) erfragt das Untersuchungsinstrument die Häufigkeit (bzw. Intensität, Menge, etc.) der Nutzung unterschiedlichster protektiver Verhaltensweisen zur Kontrolle der eigenen Daten im online-Kontext vor bzw. nach dem Bekanntwerden der Möglichkeiten der flächendeckenden Datenspeicherung und -analyse durch Regierungen. Einige Beispiele für erfragte Strategien sind die

Nutzung von Verschlüsselungsprogrammen und sicheren Suchmaschinen, das Löschen der Browser-History oder die Verwendung sicherer Passwörter. Zur Verrechnung wurden zunächst alle Items so gepolt, dass größere Werte einem sicherheitsbewussteren Verhalten zugeschrieben werden können. Um das Ausmaß der Verhaltensänderung zu bestimmen wurde die Differenz der Mittelwerte aus den Items nach und vor der Berichterstattung gebildet.

#### *2.3.7 „Knew-it-all-along“-Effekt*

Da der Bericht eigener Verhaltensweisen aus der Vergangenheit häufig Verzerrungseffekten bzw. Gedächtnisfehlern unterworfen ist, wurden drei Items zum „Knew it all along“-Effekt vorgegeben, welcher beschreibt, dass Erwachsene sich nicht an ihren vorherigen Wissensstand erinnern können, nachdem sie neuere Informationen gesammelt haben (Hasher, Attig & Alba, 1981).

Auf einer 4-stufigen Likert-Skala von „trifft nicht zu“ über „trifft eher nicht zu“ und „trifft eher zu“ bis „trifft zu“ soll eingeschätzt werden, inwieweit den Teilnehmern schon vor der medialen Berichterstattung klar war, dass Daten so weitreichend gespeichert und analysiert werden können und werden (Items siehe Anhang, S. 87). Auch hier wurde die Summe über alle Item-Antworten gebildet, wodurch sich ein Wertebereich von minimal 4 bis maximal 12 Punkte ergibt.

#### *2.3.8 Lebenszufriedenheit - SWL*

Um die Lebenszufriedenheit der Studienteilnehmer zu erfassen wurde zudem die deutsche Version der Satisfaction with Life Scale (Glaesmer, Grande, Braehler und Roth, 2011) eingesetzt. Hier werden 5 Aussagen über die Zufriedenheit in einzelnen Lebensbereichen über eine 7-stufige Antwortskala eingeschätzt.

Die englische Version des Instrumentes weist eine Test-Retest-Relibiliät von 0.82, bzw. 0,9 auf, wenn situative

Faktoren mit einbezogen werden (Eid & Diener, 2004). Zur weiteren Verrechnung wird ein Summenwert über alle 5 Items gebildet.

#### 2.4 Untersuchungsdurchführung

Die Stichprobe wurde zunächst in einem dreimonatigen Erhebungszeitraum (1.7.2014-30.9.2014) online akquiriert. Erreicht wurden die Studienteilnehmer über das Schneeballprinzip sozialer Netzwerke und studienbezogener Gruppen (aus den Institutionen Uni Wien, Technische Universität Wien und Wirtschaftsuniversität Wien) auf Facebook (e.g. *Pöbelpsychologen Uni Wien*, *Gegen die Vernachlässigung des Diplomstudiums*, etc.) sowie Aussendungen von Studienprogrammleitungen der Universität Wien (Studienvertretung Japanologie sowie Theologie), und über die Hochschulgruppe von *Digital Courage*, eine gemeinnützige Organisation, die es sich zur Aufgabe gemacht hat, Bürgerrechte vor allem im Bereich des Datenschutzes zu vertreten. Außerdem konnte der Link zum online-Fragebogen über die Webseite der Zeitschrift *Psychologie Heute* aufgerufen werden.

Im Anschluss an die online Erhebung wurden weitere Daten im Zeitraum zwischen dem 1.10.2014 - 10.02.2015 durch die Paper-Pencil Version des Untersuchungsinstruments im erweiterten Freundes- und Bekanntenkreis der Studienleiterin sowie in einem Psychologie-Seminar an der Universität Wien erhoben, um systematische Unterschiede zwischen den Erhebungskontexten analysieren zu können.

#### 2.5 Statistische Hypothesen

- H0/1: Medienkonsum ist kein Prädiktor für  
 $M_{Nachher} - M_{Vorher}$ .
- H1/1: Medienkonsum ist ein Prädiktor für  
 $M_{Nachher} - M_{Vorher}$ .
- H0/2: Die *Big 5* sind keine Prädiktoren für  
 $M_{Nachher} - M_{Vorher}$ .

- H1/2.1: *Neurotizismus* ist ein Prädiktor für  
*M\_Nachher - M\_Vorher*.
- H1/2.2: *Extraversion* ist ein Prädiktor für  
*M\_Nachher - M\_Vorher*.
- H1/2.3: *Verträglichkeit* ist ein Prädiktor für  
*M\_Nachher - M\_Vorher*.
- H1/2.4: *Gewissenhaftigkeit* ist ein Prädiktor für  
*M\_Nachher - M\_Vorher*.
- H1/2.5: *Offenheit für neue Erfahrungen* ist ein Prädiktor  
für *M\_Nachher - M\_Vorher*.
- H0/3: Die Einstellung ist kein Prädiktor für  
*M\_Nachher - M\_Vorher*.
  - H1/3.1: *Besorgnis* ist ein Prädiktor für  
*M\_Nachher - M\_Vorher*.
  - H1/3.2: *Kognitive Bewertung* ist ein Prädiktor für  
*M\_Nachher - M\_Vorher*.
  - H1/3.3: *Politische Bedenken* ist ein Prädiktor für  
*M\_Nachher - M\_Vorher*.
- H0/4: *Wissen* ist kein Prädiktor für *M\_Nachher - M\_Vorher*.
  - H1/4: *Wissen* ist ein Prädiktor für *M\_Nachher - M\_Vorher*.
- H0/5: *M\_Vorher* ist kein Prädiktor für *M\_Nachher - M\_Vorher*.
  - H1/5: *M\_Vorher* ist ein Prädiktor für *M\_Nachher - M\_Vorher*.
- H0/6: *Knew-it-all-along* ist kein Prädiktor für  
*M\_Nachher - M\_Vorher*.
  - H1/6: *Knew-it-all-along* ist ein Prädiktor für  
*M\_Nachher - M\_Vorher*.

Die Hypothesen H0/1 bis H0/6 werden durch eine rückwärts-  
gewandte Multiple Regression für zwei unabhängige Stichproben  
mit 13 Prädiktoren geprüft.

- H0/7.1: *SWL* steht nicht in statistisch signifikantem Zusammenhang mit *Medienkonsum*.

H1/7.1: *SWL* steht in statistisch signifikantem Zusammenhang mit *Medienkonsum*.

H1/7.2: *SWL* steht in statistisch signifikantem Zusammenhang mit *Besorgnis, Kognitive Bewertung* und *Politische Bedenken*.

Die Hypothese H0/7 wird mit Spearman-Korrelationen geprüft.

- H0/8: Die Stichproben unterscheiden sich nicht signifikant in ihren Antworten.

H1/8.1: Die Stichproben unterscheiden sich signifikant in *M\_vorher*.

H1/8.2: Die Stichproben unterscheiden sich signifikant in *M\_nachher*.

H1/8.3: Die Stichproben unterscheiden sich signifikant in *Wissen*.

H1/8.4: Die Stichproben unterscheiden sich signifikant in *Besorgnis*.

H1/8.5: Die Stichproben unterscheiden sich signifikant in *Kognitiver Bewertung*.

H1/8.6: Die Stichproben unterscheiden sich signifikant in *Politischen Bedenken*.

Die Hypothesen H0/8.1 bis H0/8.6 werden bei Normalverteilung mit T-Tests für unabhängige Stichproben geprüft; liegt keine Normalverteilung vor, werden sie mit Whitney-Mann U-Tests geprüft.

### 3. Ergebnisse

Im folgenden Kapitel werden die deskriptiven und interferenzstatistischen Ergebnisse der vorliegenden Arbeit dargestellt. Alle Ergebnisse wurden mithilfe des Programmes SPSS Statistics 22.0.0.0 berechnet.

Da sich die vorliegende Untersuchung unter anderem mit den systematischen Unterschieden zwischen den akquirierten Stichproben beschäftigt, werden auch die deskriptiven Ergebnisse nach Erhebungskontext aufgeteilt dargestellt.

### 3.1 Deskriptive Ergebnisse

#### 3.1.1 Demographische Daten

Insgesamt nahmen 755 Personen an der Untersuchung teil, wovon 627 Personen den Fragebogen online ausfüllten und 128 in der Paper-Pencil-Version.

**Tab. 1:** Demographische Daten beider Stichproben.

	N_On	N_PP	M_On	M_PP	SD_On	SD_PP
Alter	601	126	32.08	34.66	13.29	14.58
Geschlecht	605	128	1.63	1.5	0.52	0.53
Bildungsgrad	606	127	3.36	3.06	0.72	0.75
Familienstand	606	124	2.36	2.31	0.48	0.46
Englisch- Kenntnisse	606	128	4	3.78	0.84	0.81
Wohnort	606	128	3.63	3.63	1.45	1.38

*Note.* Geschlecht- (1) männlich, (2) weiblich; Bildungsgrad von (1) Pflichtschule bis (4) Hochschulabschluss; Familienstand- (2) in einer Beziehung, (3) allein stehend; Englischkenntnisse- (1) keine bis (5) sehr gute; Wohnort- (1) ländlich bis (5) Metropole, für On = Online Stichprobe, bzw. PP = Paper-Pencil-Stichprobe.

Beide Stichproben sind eher jung mit einem Mittelwert von  $M = 32$  (online) bzw. knapp  $M = 34$  (Paper-Pencil) Jahren, wobei die Spanne in der online Stichprobe zwischen 14 und 75 liegt, in der PP zwischen 17 und 68. Die 95%-Konfidenzintervalle bezüglich des Alters in der Online-Stichprobe  $KI = [6.03;58.13]$  und in der PP-Stichprobe  $KI = [6.08;63.7]$  überschneiden sich.

Die Online-Stichprobe ist eher weiblich ( $M = 1.63$ ,  $SD = 0.52$ ), im Vergleich zur PP-Stichprobe ( $M = 1.5$ ,  $SD = 0.53$ ).

Beide Stichproben weisen einen hohen Bildungsgrad und gute Englischkenntnisse auf (siehe Tabelle 1).

Ebenso leben die meisten Befragten beider Stichproben alleinstehend in Metropolregionen (siehe Tabelle 1).

Die meisten Teilnehmer beider Stichproben haben die österreichische oder deutsche Staatsbürgerschaft, wobei Personen deutscher Herkunft weit mehr als die Hälfte ausmachen (siehe Abb. 1).

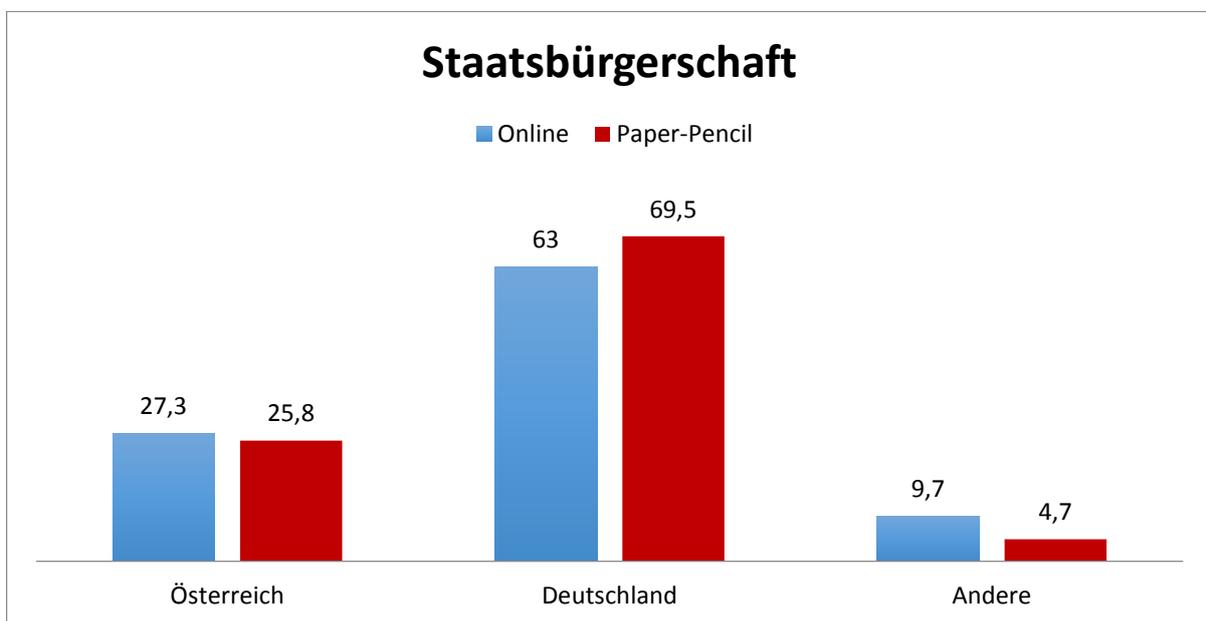


Abb.1: Staatsbürgerschaft der Teilnehmer in Prozent.

### 3.1.2 Internetzugang und Nutzung

Knapp 93% der Probanden haben einen festen Internet-Anschluss zuhause und 77,5% besitzen ein internetfähiges Smartphone; einen mobilen Internetanschluss wie in etwa Daten-Sticks nutzen nur knapp 30% der Befragten.

Um einen Einblick in die typischen Internetnutzungsgewohnheiten der Teilnehmer zu erlangen wurde über eine 5 pt.-Likert-Skala erhoben, mit welcher Häufigkeit von (1) nie bis (5) immer sie das Internet zu welchem Zweck nutzen (siehe Tabelle 2).

**Tab. 2:** Häufigkeit der Nutzung unterschiedlicher Dienste im Internet.

	<i>N_On</i>	<i>N_PP</i>	<i>M_On</i>	<i>M_PP</i>	<i>SD_On</i>	<i>SD_PP</i>
Zeitvertreib	544	125	3.44	3.23	1.01	1.00
Arbeit/Ausbildung	544	126	4.02	3.91	0.94	0.94
OSN	544	125	3.07	2.95	1.33	1.33
Unterhaltung	544	125	3.27	3.3	1.14	1.14
Nachrichten	544	124	3.53	3.58	1.03	1.03
Shoppen	544	126	2.81	2.79	0.94	0.94
Informationssuche	542	127	4.23	4.15	0.66	0.66
E-Mails	542	127	4.15	4.06	0.89	0.89

*Note:* Erhoben auf 5-pt. Likert Skala von (1) *nie* bis (5) *immer* in beiden Stichproben.

In beiden Gruppen sind Informationssuche ( $M = 4.23$ ,  $SD = 0.66$ ; bzw.  $M = 4.15$ ,  $SD = 0.55$ ) und E-Mails ( $M = 4.15$ ,  $SD = 0.89$ ; bzw.  $M = 4.06$ ,  $SD = 0.86$ ) die typisch am häufigsten ausgeführten Handlungen.

Da soziale Netzwerke einen großen Part in der öffentlichen Diskussion zum Thema Datenschutz einnehmen wurde auch die Häufigkeit der Nutzung der gängigsten OSNs erfragt (siehe Tabelle 3).

In beiden Gruppen ist Facebook das am häufigsten genutzte Online Social Network, mit einem Mittelwert von  $M = 3.15$  ( $SD = 1.54$ ), bzw.  $M = 2.8$  ( $SD = 1.55$ ).

**Tab. 3:** Häufigkeit der Nutzung von unterschiedlichen Online Social Networks.

	N_On	N_PP	M_On	M_PP	SD_On	SD_PP
Facebook	544	127	3,15	2,8	1,54	1,55
Twitter	544	126	1,30	1,23	0,81	0,66
Instagram	544	126	1,37	1,32	0,93	0,86
Vine	544	126	1,06	1,03	0,39	544
Andere	544	120	1,52	1,73	0,96	1,08

Note. Erhoben auf Likert Skala von *nie* (1), *selten* (2), *gelegentlich* (3), *oft* (4) bis *immer* (5).

### 3.1.3 Protektive Strategien

Die Deskriptiven Kennwerte für den Mittelwert der Intensität bzw. Häufigkeit in der die Teilnehmer protektive Strategien vor und nach der Medialen Berichterstattung angewendet haben, um ihre Privatsphäre im Internet zu schützen, sind in Tabelle 4 dargestellt.

**Tab. 4:** Ausmaß der Anwendung protektiver Strategien.

	M_Vorher _On	M_Vorher _PP	M_Nachher _On	M_Nachher _PP	M_Nachher- M_Vorher _On	M_Nachher- M_Vorher _PP
<i>N</i>	373	79	387	77	369	75
<i>M</i>	3.15	3.07	3.24	3.16	0.09	0.1
<i>SD</i>	.4	0.37	0.4	0.37	0.16	0.14
<i>Min</i>	2.04	2.26	2.07	2.39	-0.72	-.14
<i>Max</i>	4.5	4	4.74	4.09	1.02	0.5

Note. Ausmaß der Anwendung protektiver Strategien vor und nach der Berichterstattung sowie Ausmaß der Verhaltensänderung in beiden Stichproben.

In beiden Stichproben wurden die unterschiedlichen Strategien durchschnittlich „gelegentlich“ (siehe Tabelle 4) angewendet. Die Differenz des Verhaltens zwischen den beiden Zeitpunkten ist in beiden Stichproben sehr gering ( $M_{\text{Online}} = 0.09$ ,  $SD_{\text{Online}} = 0.16$ ;  $M_{\text{PP}} = 0.1$ ,  $SD_{\text{PP}} = 0.14$ ), mit einem Maximum von gut einem Skalen-Punkt in der Online-, und einem halben in der PP-Stichprobe. Auch ist ersichtlich, dass vereinzelte Probanden sogar einen negativen Wert erreichten, also sich nachher noch weniger schützen als vorher.

Die durchschnittlich am häufigsten angewandten Strategien vor der Berichterstattung waren das Nutzen einer Firewall ( $M_{\text{Online}} = 4.4$ ,  $SD_{\text{Online}} = 1.23$ ;  $M_{\text{PP}} = 4.32$ ,  $SD_{\text{PP}} = 1.20$ ) und eines Spam-Filters für E-Mail Accounts ( $M_{\text{Online}} = 4.3$ ,  $SD_{\text{Online}} = 1.22$ ;  $M_{\text{PP}} = 4.13$ ,  $SD_{\text{PP}} = 1.31$ ). Am seltensten wurden unabhängige Clouds zur Datenspeicherung verwendet ( $M_{\text{Online}} = 1.11$ ,  $SD_{\text{Online}} = 4.57$ ;  $M_{\text{PP}} = 1.13$ ,  $SD_{\text{PP}} = .575$ ).

#### 3.1.4 „Knew-it-all-along“-Effekt

In dieser Untersuchung wurde der „Knew-it-all-along“ Effekt mit 3 Items auf einer 4-pt. Likert Skala erhoben. Zur weiteren Verrechnung wurde ein Summenwert gebildet. Beide Gruppen erreichten hier im Durchschnitt einen Wert knapp unter 10 Punkten (siehe Tab. 5).

**Tab. 5:** Statistische Kennwerte des Summenscores des „Knew-it-all-along“-Effekts.

	<i>N</i>	<i>M</i>	<i>Mdn</i>	<i>SD</i>
Online	543	9.58	10	2.13
Paper-Pencil	127	9.72	10	2.03

*Note.* Der Summenscore kann Werte zwischen 3 und 12 annehmen.

#### 3.1.5 Lebenszufriedenheit der Teilnehmer

Mit dem SWLS (Gerlitz und Schupp, 2005) wurde die Lebenszufriedenheit der Teilnehmer erhoben (siehe Tab. 6), die

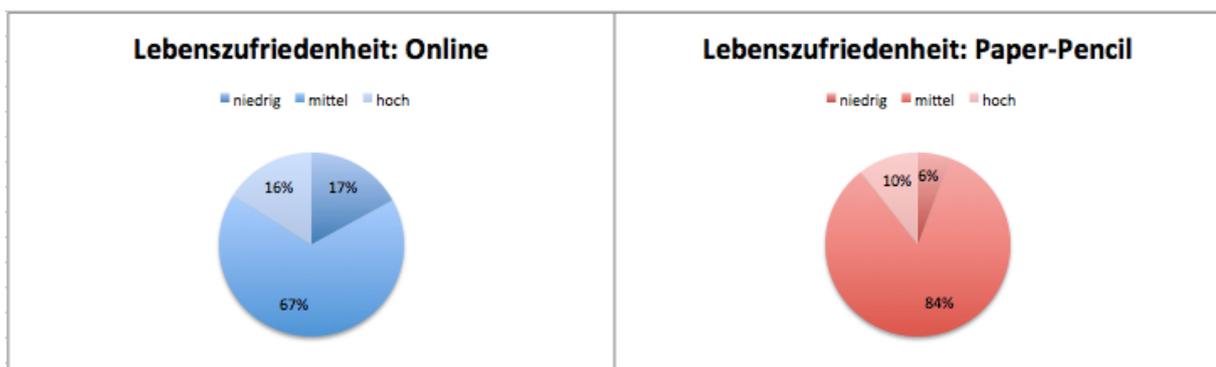
Werte können zwischen 5 und 35 variieren, wobei ein hoher Wert einer hohen Lebenszufriedenheit entspricht.

**Tab. 6:** Statistische Kennwerte des SWLS.

	<i>N</i>	<i>M</i>	<i>Mdn</i>	<i>SD</i>
Online	453	25.20	26	6.44
Paper-Pencil	123	26.55	27	4.78

*Note.* SWLS = Werte der Satisfaction with life scale.

Mittelwert und Median beider Stichproben liegen im Bereich einer mittleren Lebenszufriedenheit (Werte 19 bis 31); die Mehrheit beider Stichproben erreicht eine mittlere Lebenszufriedenheit, wobei 16% der Online-Stichprobe im Vergleich zu 10% der Paper-Pencil-Stichprobe eine hohe Lebenszufriedenheit aufweisen (siehe Abb. 2).



*Abb. 2:* Prozent der Teilnehmer mit niedriger/mittlerer/hocher Lebenszufriedenheit.

### 3.1.6 Medienkonsum

Für die Items zum Ausmaß, in dem die Probanden die Berichterstattung über die Möglichkeiten von Datenspeicherung und Analyse nahezu aller Internetaktivitäten verfolgten, kann der Summenscore Werte zwischen 7 und 35 Punkten annehmen. Die Paper-Pencil-Stichprobe liegt hier mit einem Median von  $Mdn = 18$  zwei Punkte über dem der Online Stichprobe  $Mdn = 18$  (siehe Tab. 7).

**Tab. 7:** Intensität der aktiven Beschäftigung mit der medialen Berichterstattung.

	<i>N</i>	<i>M</i>	<i>Mdn</i>	<i>SD</i>
Online	543	16.39	16	3.66
Paper-Pencil	121	17.05	18	4.83

*Note.* Erhoben auf 5-pt. Likert Skala von (1) *gar nicht*, über (2) *kaum*, (3) *etwas* (4) *überwiegend*, bis (5) *sehr*. Summenscore kann Werte zwischen 7 und 35 annehmen.

### 3.1.7 Wissen

Die Knowledge Skala von Turow und Kollegen (2005) erhebt Wissen über die Risiken der Datensammelpraktiken (acht Items), sowie deren gesetzlichen Grundlagen (sieben Items) und bildet einen Gesamt-Summenwert für alle richtig beantworteten Fragen.

In beiden Stichproben wurde durchschnittlich etwa die Hälfte der Fragen korrekt beantwortet ( $M = 8.07$ ,  $SD = 2.28$ , bzw.  $M = 7.78$ ,  $SD = 1.97$ ).

Nur eine Person der Online-Stichprobe konnte alle Fragen richtig beantworten, in der Paper-Pencil-Gruppe keine. Die weiteren statistischen Kennwerte der Skala sind in Tabelle 8 ersichtlich.

**Tab. 8:** Scores der Knowledge Skalen Risiken der Datensammelpraktiken und Gesetzliche Grundlagen, sowie Gesamtscore in beiden Stichproben.

	Risiken	Gesetze	Gesamtscore
<i>N</i> _On	546	545	545
<i>N</i> _PP	123	124	122
<i>M</i> _On	5.62	2.44	8,07
<i>M</i> _PP	5.51	2.27	7.78
<i>Mdn</i> _On	6	2	8
<i>Mdn</i> _PP	6	2	8
<i>SD</i> _On	1.42	1.39	2.28
<i>SD</i> _PP	1.16	1.21	1.97

*Note.* Score ergibt sich aus Anzahl der richtig beantworteten Items. Risiken= Risiken der Datensammelpraktiken (8 Fragen),Gesetze= gesetzliche Grundlagen der Datensammelpraktiken (7 Fragen).

### 3.1.8 Persönlichkeitsfaktoren

In beiden Stichproben wurden die Big-5 Persönlichkeitsfaktoren mithilfe des BFI-S erhoben. In der online Stichprobe entspricht der Mittelwert ( $M = 50$ ) genau dem der Normstichprobe (SOEP, 2005), in der Paper-Pencil-Stichprobe liegen sie knapp darüber bzw. darunter (siehe Tab. 6). Die Teilnehmer dieser Studie entsprechen also in etwa der der Normstichprobe (für weitere Kennwerte siehe Tab. 6).

**Tab. 9:** Big 5 Persönlichkeitsfaktoren (BFI-S).

	O	G	E	V	N
<i>N_On</i>	453	453	453	453	453
<i>N_PP</i>	122	122	122	122	122
<i>M_On</i>	50	50	50	50	50
<i>M_PP</i>	49.99	49.95	49.98	50.01	50.05
<i>Mdn_On</i>	50.79	50.23	50.44	49.75	49.85
<i>Mdn_PP</i>	49.73	51.28	49.58	49.88	49.89
<i>SD_On</i>	9.55	10.61	5.59	6.15	10.44
<i>SD_PP</i>	8.8	10.72	6.06	7.18	10.25
<i>Min_On</i>	17.56	10.15	26.96	34.94	24.65
<i>Min_PP</i>	26.42	21	34.71	27.81	29.14
<i>Max_On</i>	77.5	73.26	63.91	66.97	74.83
<i>Max_PP</i>	68.39	72.28	63.82	71.85	74.72

*Note.* Offenheit für neue Erfahrungen (O), Gewissenhaftigkeit (G), Extraversion (E), Verträglichkeit (V), Neurotizismus (N).

### 3.1.9 Einstellung zum Erhebungskontext

Da die vorliegende Untersuchung Fragen enthält, die möglicherweise in der Online-Erhebung als zu sensibel wahrgenommen und daher nicht ehrlich beantwortet werden könnten, wurde erfragt ob die Teilnehmer der Online Stichprobe den Fragebogen lieber im Papier-Format ausgefüllt hätten.

**Tab. 10.1:** *Hätten Sie diesen Fragebogen lieber im Papier Format ausgefüllt?*

	<i>M</i>	<i>Mdn</i>	<i>SD</i>
Online	2,08	1,5	1,339

*Note. (1) nein, (2) eher nein, (3) Ich weiß es nicht. (4) eher ja, (5) ja.*

In Kategorien zusammengefasst ergibt sich hier überraschenderweise ein Prozentsatz von 69% der Online Befragten, die den Fragebogen nicht lieber als Paper-Pencil Version bearbeitet hätten (siehe Abb. 3).

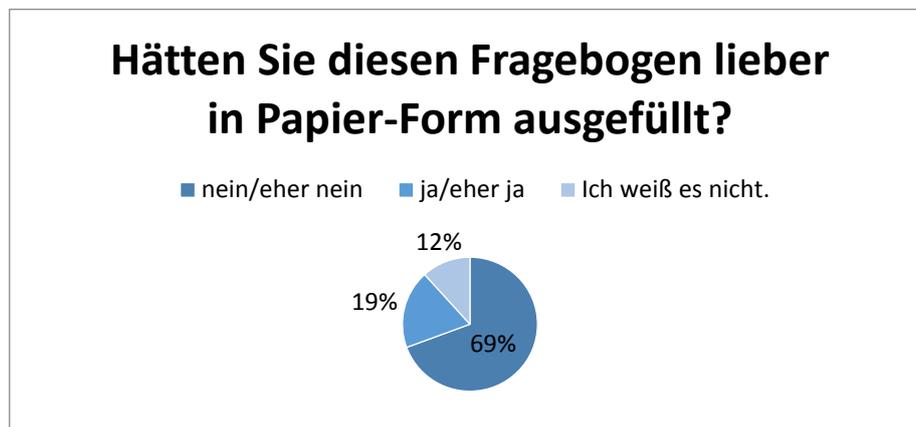


Abb. 3: Einstellung zum Erhebungskontext in der Online-Stichprobe.

Im Gegensatz dazu wurde bei der Paper-Pencil-Erhebung die Frage gestellt *Hätten Sie diesen Fragebogen auch online ausgefüllt?*. Hier liegen sowohl Mittelwert als auch Median ca. bei 3 (siehe Tab. 8), was der Antwortkategorie (3) „Ich weiß es nicht“ entspricht.



Abb. 4: Einstellung zum Erhebungskontext in der Paper-Pencil Stichprobe.

Obwohl sensible Daten erfragt wurden, hätten dennoch 45% der Paper-Pencil-Stichprobe den Fragebogen auch online bearbeitet, im Vergleich zu 45%, die dies nicht oder eher nicht getan hätten (siehe Abb. 4).

**Tab. 10.2:** Hätten Sie diesen Fragebogen auch online ausgefüllt?

	<i>M</i>	<i>Mdn</i>	<i>SD</i>
Paper-Pencil	3,03	3	1,55

Note. (1) *nein*, (2) *eher nein*, (3) *Ich weiß es nicht*, (4) *eher ja*, (5) *ja*.

### 3.1.10 Besorgnis - Deskriptive Statistik auf Item-Ebene

Um den prädiktorischen Wert der Besorgnis-Skala auf die Verhaltensänderung der Studienteilnehmer zu untersuchen wurden die Faktorwerte aus der Faktorenanalyse (siehe Abschnitt 3.2.1) verwendet.

**Tab. 11:** Statistische Kennwerte der Rohwerte zu Besorgnis, Kognitive Bewertung und Politische Bedenken auf Item-Ebene.

	<i>N</i> _On	<i>N</i> _PP	<i>M</i> _On	<i>M</i> _PP	<i>SD</i> _ON	<i>SD</i> _PP
<b>Besorgnis</b>						
Ich mache mir Sorgen um die Macht, die die Regierung hat um Online-Aktivitäten aufzuzeichnen.						
	453	122	3.66	3.61	1.15	1.04
Ich mache Mir Sorgen darüber, dass meine im Internet preisgegebenen persönlichen Informationen offener für Kontrollen von Regierung und Wirtschaft werden.						
	453	122	3.69	3.7	1.15	1,08
Ich mache mir Sorgen um die Möglichkeiten der Regierung Internet-Aktivitäten zu überwachen.						
	453	122	3.7	3.73	1.16	1.11
Die Möglichkeit der flächendeckenden Datenspeicherung aller Online-Aktivitäten durch Regierungen macht mir Angst.						
	450	123	3.14	3.26	1.22	1.18
<b>Kognitive Bewertung</b>						
Die Möglichkeit der flächendeckenden Datenspeicherung aller Online-Aktivitäten durch Regierungen empfinde ich als...						
... angemessen.						
	449	123	1.84	1.96	0.91	0.08
.... wichtig für unsere Sicherheit.						
	448	122	2.31	2.49	1.06	1.03
... ist auch nichts anderes als wir durch FB & Co tun.						
	452	119	2.69	2.82	1.23	1.28
Ich habe nichts zu verbergen.						
	447	121	3.11	3.1	1.36	1.27
Ich werde sowieso nicht überwacht.						
	451	112	1.75	1.85	0.95	1.07
<b>Politische Bedenken</b>						
... Als Eindringen in meine Privatsphäre.						
	452	120	4.04	3.93	1.07	1.10
... Verstoß gegen meine Grundrechte.						
	451	122	3.93	3.89	1.1	1.01
... Ist für mich ein Ärgernis.						
	451	122	3.64	3.59	1.19	1.141

*Note.* Auf 5-pt. Likert Skala erhoben, Rohwerte können also zwischen 1 und 5 liegen.

In Tabelle 11 sind die statistischen Kennwerte der Rohwerte auf Item-Ebene angegeben. Hier ist ersichtlich, dass die Untersuchungspersonen über beide Stichproben hinweg den Items im

Faktor Besorgnis (Mittelwerte zwischen  $M = 3.14$  und  $M = 3.73$ ) eher indifferent gegenüberstehen, obwohl die Teilnehmer der Paper-Pencil-Stichprobe tendenziell eher zustimmen.

Bei *Kognitive Bewertung* lässt sich jedoch klar erkennen, dass die Aussagen in beiden Erhebungskontexten im Durchschnitt eher abgelehnt werden (siehe Tab. 11). Deutschsprachige Internet-Nutzer geben also an, die Datensammelungspraktiken unangemessen zu finden und sehen sie eher nicht als wichtig für unsere Sicherheit an.

*Politische Bedenken* äußern beide Stichproben ebenfalls in ähnlichem Maße, sie halten die flächendeckende Datenspeicherung eher für einen Verstoß gegen ihre Grundrechte, empfinden sie als Eindringen in ihre Privatsphäre sowie als Ärgernis (siehe Tab. 11).

### 3.2 Interferenzstatistische Ergebnisse

#### 3.2.1 Faktorenanalyse zur Skala „Einstellungen zur flächendeckenden Datenspeicherung“

Um die Besorgnis der Internet Nutzer auf kognitiver und affektiver Ebene zu erheben wurden 13 Items (siehe Anhang S. 92) vorgegeben. Da die Skala „Einstellungen zur flächendeckenden Datenspeicherung“ nicht in Gänze einer bereits vorhandenen entspricht, wurde zunächst eine Hauptkomponentenanalyse mit Varimax Rotation, konvergiert in 5 Iterationen, für beide Stichproben gemeinsam, durchgeführt.

Mit einem Kaiser-Meyer-Olkin Wert von  $KMO = .87$  kann davon ausgegangen werden, dass die Stichprobe gut geeignet ist. Bartlett's Test auf Sphärizität  $\chi^2(66) = 3711.59$ ,  $p < .001$  zeigt, dass die Inter-Item-Korrelationen groß genug für eine Hauptkomponentenanalyse sind.

Nach dem Kaiserkriterium konnten drei Faktoren mit einem Eigenwert  $> 1$  identifiziert werden, die gemeinsam knapp 67% der

Varianz erklären können. Die Faktorladungen nach der Rotation sind in Tabelle 12 abgebildet.

**Tab. 12:** Rotierte Komponentenmatrix für „Einstellungen zur medialen Berichterstattung“.

Item	Faktor 1:	Faktor 2:	Faktor 3:
	Besorgnis	Kognitive Bewertung	Politische Bedenken
1	0.91		
2	0.89		
3	0.86		
4	0.71		
5		0.77	
6		0.75	
7		0.64	
8		0.56	
9		0.5	
10			0.87
11			0.84
12	0.49		0.64
12			
Eigenwert	5.35	1.56	1.11
%			
erklärter	28.26	19.76	18.81
Varianz			

*Note.* Für ausformulierte Items siehe Anhang S. 92.

Der erste Faktor enthält vier Items mit Ladungen zwischen .91 und .71, die sich alle auf Sorgen um die Datenspeicherungspraktiken beziehen, er wird daher *Besorgnis* genannt. Die Reliabilität dieses Faktors ist mit  $\alpha = .91$  exzellent. Ein Beispielitem ist: „Ich mache mir Sorgen um die Möglichkeiten der Regierung Internet-Aktivitäten zu überwachen.“. Hohe Werte in diesem Faktor zeigen ein hohes Maß an Besorgnis an. Besorgnis erklärt gut 28% der Varianz der Skala.

Der zweite Faktor enthält fünf Items und kann knapp 19% der Varianz erklären. Die Ladungen der Items liegen zwischen .5

(gerade noch annehmbar nach Field, 2009) und .77, die Reliabilität ist mit  $\alpha = .7$  annehmbar. Alle Items spiegeln kognitive Bewertungen wieder, die mit Besorgnis zusammenhängen, z.B. „Die Möglichkeit der flächendeckenden Datenspeicherung aller Online Aktivitäten finde ich angemessen.“ und wird daher *kognitive Bewertung* genannt. Alle Items des Faktors sind so ausgerichtet, dass hohe Werte implizieren, dass der Nutzer geringe Bedenken hat.

Der dritte Faktor, der extrahiert werden konnte, umfasst drei Items mit Ladungen zwischen .64 und .87, die gemeinsam knapp 20% der Varianz erklären. Ein Beispiel-Item ist: „Die Möglichkeit der flächendeckenden Datenspeicherung aller Online Aktivitäten durch Regierungen empfinde ich als Verstoß gegen meine Grundrechte.“ Am passendsten wurde die Bezeichnung *politische Bedenken* erachtet. Die Reliabilität liegt bei  $\alpha = .84$ .

Zur weiteren Verrechnung wurden die von IBM SPSS Statistics 22.0 berechneten Faktoren genutzt. In der Tabelle 12 ist die rotierte Komponentenmatrix dargestellt.

### 3.2.2 Prädiktor-Modelle

Um den Einfluss der Prädiktoren auf das Ausmaß der Verhaltensänderung zu identifizieren wurde eine rückwärts-gewandte Regression mit 13 Prädiktoren für beide Stichproben durchgeführt.

#### 3.2.2.1 Prädiktor-Modell der Online Stichprobe

In der Online Stichprobe lag für die Daten weder Multikollinearität (Toleranzwerte unauffällig nach Fields, 2009, S. 224, da alle  $VIF < 1.4$ ) vor, noch gibt es Autokorrelationen ( $d = 2.1$ ); die Voraussetzungen für eine Multiple Regression können also als gegeben angenommen werden.

Das Modell fällt mit  $F(5,334) = 11.16$  bei einem Signifikanzniveau von  $p < .001$  signifikant aus; es konnten für die Online-Stichprobe fünf Faktoren mit statistisch signifikantem Erklärungswert extrahiert werden, die gemeinsam mit  $R^2 = .143$  nur 14% der Varianz erklären. Die identifizierten Prädiktoren sind:

- *Wissen*
- *M\_vorher*
- *Medienkonsum*
- *Besorgnis*
- *Politische Bedenken*

Die standardisierten Beta-Werte und Signifikanzmaße können Tabelle 13 entnommen werden.

**Tab. 13:** Beta und Signifikanzniveaus der Prädiktoren mit signifikantem Erklärungswert.

Online-Stichpr.	B	Sig.	PP_Stichpr.	B	Sig.
<i>Wissen</i>	.10	.04	<i>Gewissenhaftigkeit</i>	.27	.03
<i>M_Vorher</i>	-.22	.00	<i>M_Vorher</i>	-.45	.00
<i>Medienkonsum</i>	.2	.00	<i>Medienkonsum</i>	.22	.07*
<i>Besorgnis</i>	.18	.00	<i>Besorgnis</i>	.23	.07*
<i>Politische Bedenken</i>	.1	.05	<i>Kognitive Bewertung</i>	.22	.66*

Note. \* Signifikant bei  $p \leq .1$  für „Multiple Regression rückwärts“ nach Bühl & Zöfel (2000).

### 3.2.2.2 Prädiktor-Modell der Paper-Pencil-Stichprobe

Auch in der Paper-Pencil Stichprobe liegen weder Multikollinearität noch Autokorrelationen ( $d = 1.78$ ) vor, die Voraussetzungen für eine Multiple Regression sind also gegeben.

Mit  $F(5,57) = 4.25$  fällt das Modell mit  $p = .002$  bei einem Signifikanzniveau von  $p = .01$  ebenfalls signifikant aus.

Ebenso wie in der Online-Stichprobe konnten 5 Prädiktoren mit Erklärungswert extrahiert werden, die gemeinsam jedoch mehr, nämlich gut 27% der Varianz, erklären können. Für die Paper-Pencil-Stichprobe sind diese:

- *Gewissenhaftigkeit*
- *M\_vorher*
- *Medienkonsum*
- *Besorgnis*
- *Kognitive Bewertungen*

Die standardisierten Beta-Werte und Signifikanzmaße können ebenfalls aus der Tabelle 13 entnommen werden.

### 3.2.2.3 Modell Vergleich

Wie bereits beschrieben konnten sowohl in der Online- als auch in der Paper-Pencil-Stichprobe signifikante Regressionsmodelle mit jeweils 5 Prädiktoren erstellt werden. In beiden Stichproben ist das Ausmaß der Anwendung protektiver Verhaltensweisen zum Schutz der Online-Privatsphäre (*M\_vorher*) der stärkste Prädiktor für die Verhaltensänderung (*M\_nachher-M\_vorher*), wenn sein Einfluss in der PP-Stichprobe auch fast doppelt so hoch ausfällt (siehe Tab. 13).

Für beide Stichproben gilt, dass Personen, die sich früher schon stark geschützt haben, wenig an ihrem Verhalten ändern, Individuen, die höhere Änderungswerte aufweisen, schützten sich früher weniger intensiv.

Des Weiteren sind *Medienkonsum* sowie *Besorgnis* für beide Stichproben Prädiktoren. *Wissen* erreicht nur in der Online Stichprobe das Signifikanzniveau, ebenso wie *Politische Bedenken*, während für *Gewissenhaftigkeit* und *Kognitive Bewertung* das Gegenteil gilt.

Der fast doppelt so hohe Erklärungswert des Paper-Pencil-Models gegenüber dem Online-Daten-basierten Modell wird in der Interpretation diskutiert.

### 3.2.3 Lebenszufriedenheit, Medienkonsum und Einstellungen zur flächendeckenden Datenspeicherung

Um zu erörtern, ob die mediale Berichterstattung und das Ausmaß der Sorgen einen Einfluss auf die Lebenszufriedenheit der Untersuchungsteilnehmer haben könnte, wurde für den Zusammenhang dieser Variablen Spearmans-Rho berechnet (siehe Tabelle 14 für alle Kennwerte). In der Online-Stichprobe gab es keine signifikanten Zusammenhänge zwischen der Lebenszufriedenheit der Teilnehmer und *Medienkonsum*, *Besorgnis*, *kognitive Bewertung* sowie *politische Bedenken*.

**Tab. 14:** Zusammenhang zwischen Lebenszufriedenheit, Medienkonsum und Einstellungen zur flächendeckenden Datenspeicherung.

	N_On	N_PP	r_On	r_PP	Sig._On	Sig._PP
<i>Besorgnis</i>	435	112	-0.03	.01	.59	.95
<i>Kognitive Bewertung</i>	435	112	0.04	.07	.46	.45
<i>Politische Bedenken</i>	435	112	-0.05	.20	.3	.03*
<i>Medienkonsum</i>	453	117	0.05	-0.10	.29	.28

Note. r = Spearman-Rho Korrelationskoeffizient.

\* signifikant bei Niveau  $p < .05$  (zweiseitig)

In der Paper-Pencil-Stichprobe erreichte der niedrige Zusammenhang zwischen Lebenszufriedenheit und *Politische Bedenken* mit  $r = .2$ ,  $p < .05$  jedoch das Signifikanzniveau. Dies bedeutet, dass Individuen mit höherer Lebenszufriedenheit mehr politische Bedenken äußerten.

### 3.2.4 Stichprobenvergleich

Um systematische Unterschiede im Antwortverhalten zu identifizieren wurden für die Variablen *M\_vorher*, *M\_nachher*,

*M\_nachher-M\_vorher*, *Wissen*, *Besorgnis*, *Kognitive Bewertung* sowie *Politische Bedenken* und *Knew-it-all-along* zunächst Tests auf NV durchgeführt und im Anschluss Mittelwerts-Vergleiche angestellt.

Sowohl in puncto Wissen als auch im Mittel des protektiven Verhaltens vor und nach der medialen Berichterstattung zeigt sich kein signifikanter Unterschied zwischen der Paper-Pencil- und der Online-Stichprobe (Ergebnisse der T-Tests für unabhängige Stichproben mit homogenen Varianzen, sowie Effektstärken siehe Tabelle 15).

**Tab. 15:** Ergebnisse der T-Tests mit Effektstärke (d) für den Stichprobenvergleich im Sicherheitsverhalten vor und nach der Berichterstattung, sowie *Wissen*.

	t	df	Sign.	d
<i>M_vorher</i>	1.50	450	0.13	0.19
<i>M_nachher</i>	1.50	462	0.14	0.19
<i>Wissen</i>	1.31	665	0.19	0.13

Dies gilt auch für das Ausmaß der Verhaltensänderung, *Knew-it-all-along*, *Besorgnis* und *Politische Bedenken*; in *Kognitiver Bewertung* zeigt sich zwar auch kein signifikanter Unterschied, mit einer Effektgröße von  $r = .07$  allerdings ein Trend: Personen der Online-Stichprobe weisen tendenziell höhere Werte auf. (Für die Testwerte und Effektstärken der Mann-Whitney U-Tests siehe Tab. 16.)

**Tab. 16:** Ergebnisse der Mann-Whitney-U Tests mit Effektstärke (r) für den Stichprobenvergleich in Verhaltensänderung und Einstellungen zur Datenspeicherung.

	U	z	Sign.	r
<i>M_Nachher-M_Vorher_On</i>	12778	-1.06	.29	0.05
<i>Besorgnis</i>	24397.5	-0.12	.90	0.00
<i>Kognitive Bewertung</i>	22222.5	-1.57	.12	0.07*
<i>Politische Bedenken</i>	22991.5	-1.058	.29	0.05
<i>Knew-it-all-along</i>	33487.5	-0.51	.61	0.02

\* tendenziell signifikant, mit höheren Werten in der Online Stichprobe.

### 3.3 Hypothesenprüfung

Eine tabellarische Übersicht der Hypothesenprüfung ist in Tabelle 17 dargestellt. Um die Übersichtlichkeit zu bewahren, werden hier nur noch einmal diejenigen Nullhypothesen ausformuliert, welche anhand der vorliegenden Daten verworfen werden konnten. Diese sind für die Online-Stichprobe:

- H0/1: *Medienkonsum* ist kein Prädiktor für *M\_Nachher* - *M\_Vorher*.
- H0/3.1: *Besorgnis* ist kein Prädiktor für *M\_Nachher* - *M\_Vorher*.
- H0/3.3: *Politische Bedenken* ist kein Prädiktor für *M\_Nachher* - *M\_Vorher*.
- H0/4: *Wissen* ist kein Prädiktor für *M\_Nachher* - *M\_Vorher*.
- H0/5: *M\_Vorher* ist kein Prädiktor für *M\_Nachher* - *M\_Vorher*.

Für die Paper-Pencil-Stichprobe konnten die folgenden Nullhypothesen verworfen werden:

- H0/1: *Medienkonsum* ist kein Prädiktor für *M\_Nachher* - *M\_Vorher*.
- H0/2.4: *Gewissenhaftigkeit* ist kein Prädiktor für *M\_Nachher* - *M\_Vorher*.
- H0/3.1: *Besorgnis* ist kein Prädiktor für *M\_Nachher* - *M\_Vorher*.
- H0/3.2: *Kognitive Bewertung* ist kein Prädiktor für *M\_Nachher* - *M\_Vorher*.
- H0/5: *M\_vorher* ist kein Prädiktor für *M\_Nachher* - *M\_Vorher*.
- H0/7.2: *SWL* steht nicht in statistisch signifikantem Zusammenhang mit *Besorgnis*, *Kognitive Bewertung* und *Politische Bedenken*.

Allerdings konnte die H0/7.2 nur für den Faktor *Kognitive Bewertung* verworfen werden, nicht aber in Bezug auf *Besorgnis* und *Kognitive Bewertung*.

**Tab. 17:** Hypothesenprüfung für beide Stichproben.

	Online		Paper-Pencil	
	beibehalten	verworfen	beibehalten	verworfen
H0/1		X		X
H0/2.1	X		X	
H0/2.2	X		X	
H0/2.3	X		X	
H0/2.4	X			X
H0/2.5	X		X	
H0/3.1		X		X
H0/3.2	X			X
H0/3.3		X	X	
H0/4		X	X	
H0/5		X		X
H0/6	X		x	
H0/7.1	X		x	
H0/7.2	x			X
	Stichprobenvergleich			
	beibehalten		verworfen	
H0/8.1	X			
H0/8.2	X			
H0/8.3	X			
H0/8.4	X			
H0/8.5	X			
H0/8.6	X			

*Note.* Für ausformulierte Hypothesen siehe Abschnitt 2.5.

Allerdings konnte die H0/7.2 nur für den Faktor *Kognitive Bewertung* verworfen werden, nicht aber in Bezug auf *Besorgnis* und *Kognitive Bewertung*.

## 4. Diskussion

### 4.1 Interpretation

Die vorliegende Studie hat sich mit dem prädiktorischen Wert von Furcht-Appellen durch die Medien, Wissen um Risiken der Datensammelpraktiken und deren gesetzlichen Grundlagen, Besorgnis, Persönlichkeitsfaktoren und dem „Knew-it-all-along“-Effekt auf das Ausmaß, in dem Internet-Nutzer versuchen ihre Privatsphäre stärker zu schützen, beschäftigt. Außerdem wurde der Zusammenhang der Lebenszufriedenheit der Teilnehmer mit dem Ausmaß an Besorgnis und der Intensität, in der die mediale Berichterstattung verfolgt wurde, betrachtet. Dies geschah in zwei unabhängigen Stichproben, die sich durch ihren Erhebungskontext (Online- bzw. Paper-Pencil) unterscheiden.

Die Intensität, mit der sich Untersuchungsteilnehmer mit der medialen Berichterstattung über die Möglichkeiten von Regierungen flächendeckend nahezu alle Internetkommunikation zu überwachen, zu speichern und zu analysieren beschäftigt haben, ist als Prädiktor für das Ausmaß der Verhaltensänderung geeignet. Die mediale Berichterstattung scheint also einen Einfluss auf unsere protektiven Verhaltensweisen auszuüben; dieses Ergebnis steht im Einklang mit Untersuchungen zum Einfluss von Furcht-Appellen auf das Sicherheitsverhalten im Netz (siehe z.B. Johnston & Warketin, 2010). Interessanterweise war in beiden Stichproben dennoch das Verhalten vor der Berichterstattung der stärkste Prädiktor für die Verhaltensänderung, und zwar so, dass Personen, die sich schon immer geschützt haben, am wenigsten veränderten, und andersherum. Auch dies deckt sich mit älteren Studien; zum Beispiel fanden Paine und Kollegen (2007) heraus, dass Sorgen um die Privatsphäre sinken, sobald wir uns besser geschützt fühlen, was ja wiederum das Verhalten beeinflusst (e.g. Young & Quan-Haase, 2013).

Das Einsetzen protektiver Maßnahmen zum Schutz der Privatsphäre im Internet ist in beiden Stichproben sowohl vor als auch nach der medialen Berichterstattung wenig ausgeprägt und unterscheidet sich auch zwischen den beiden Zeitpunkten nicht signifikant. Dommeyer und Gross (2003) kamen ebenfalls zu dem Ergebnis, dass die Nutzung von Schutzmaßnahmen trotz vorhandenen Bewusstseins für die Problematik relativ selten ist. Möglicherweise liegt hier derselbe Effekt zugrunde, der auch dazu führte, dass der „Knew-it-all-along“-Effekt in beiden Stichproben nicht zum Vorhersagen der Verhaltensänderung taugte.

Bei der Erhebung fiel auf, dass viele Teilnehmer diverse Strategien nicht kannten - es wäre also möglich, dass z.B. die Teilnahme an der Studie oder anderweitige Konfrontation mit potenziellen Möglichkeiten zum Schutz dazu führen würde, dass mehr Strategien angewendet werden.

Yao und Linz (2008) zeigten schon, dass die Adaption protektiver Strategien zu gut einem Viertel durch drei Faktoren determiniert wird: eine wohlwollende Sichtweise möglicher Sicherheitsmaßnahmen, das Vertrauen diese auch effektiv selbst anwenden zu können, sowie eine hohe Selbstwirksamkeitserwartung. Es wäre also theoretisch fundiert zu vermuten, dass die Teilnehmer der vorliegenden Stichproben nicht die Erwartung haben überhaupt in der Lage zu sein, ihre Privatsphäre zu schützen, unabhängig davon, ob sie nicht auf ihre eigenen Fähigkeiten Applikationen richtig anwenden zu können vertrauen oder nicht den Applikationen selbst.

In den Augen der Studienleiterin suggerierte die mediale Berichterstattung über Datensammlungspraktiken durch Regierungen eben auch, dass es für jede Schutzmaßnahme Schlupflöcher gibt; möglicherweise sind Internet-Nutzer (unabhängig von ihren IT-Kenntnissen) dadurch frustriert und befinden sich in einer Art Schockstarre. Dies deckt sich in etwa mit dem Fund von Buchanan und Kollegen (2007), dass der Effekt

von Sorgen um die Privatsphäre durch Wissen um mögliche Strategien mediiert wird. Hier würde also ein effektiver Ansatzpunkt für Interventionen liegen.

Das Wissen um Risiken der Datensammelpraktiken und deren gesetzliche Grundlagen war in beiden Stichproben gering; nur eine Versuchsperson der Online-Stichprobe wusste die Antworten zu allen Items, durchschnittlich wurden in etwa die Hälfte der Fragen korrekt beantwortet. Dies ist zwar kein überraschendes Ergebnis und ist zum Beispiel mit den Studien von Turow und Kollegen (2005), Park (2011) oder dem Euroflash Barometer (TNS Opinion & Social, 2010) vergleichbar, bleibt aber dennoch erschreckend. Ebenso wie bei Smit et al. (2014) zeigt sich in diesem Datenmaterial bei der Paper-Pencil-Stichprobe kein signifikanter Einfluss von Wissen auf die Adaption protektiver Verhaltensweisen, in der Online-Stichprobe hat diese Variable aber doch signifikanten Wert als Prädiktor ( $\beta = .105$ ). Wichtig hierbei ist es auch zu beachten, dass Wissen um Risiken eben wieder nicht bedeutet, dass die Teilnehmer auch ausreichende Kenntnisse darüber haben, wie sie sich vor diesen schützen können.

Auch Sorgen um die Online-Privatsphäre sind Prädiktoren für das Ausmaß der Verhaltensänderung in beiden Stichproben der vorliegenden Untersuchung. Die vorwiegend emotional besetzten Items des Faktors Besorgnis üben in beiden Stichproben einen Einfluss aus; politische Bedenken hingegen scheinen nur für die Online-Stichprobe als Prädiktor zu gelten. Überraschend ist der Zusammenhang des Faktors kognitive Bewertung: Er erreicht in der Online-Stichprobe einen signifikant positiven Zusammenhang mit der Verhaltensänderung. Dies bedeutet, dass Individuen, die höhere Werte aufweisen, mehr an ihrem protektiven Verhalten geändert haben. Auch auf Item-Ebene bleibt das Ergebnis kontraintuitiv: Wer hohe Werte in diesem Faktor aufweist hält die Möglichkeit der flächendeckenden Datenspeicherung durch

Regierungen zum Beispiel für angemessen und wichtig für unsere Sicherheit; darüber hinaus haben diese Personen das Gefühl sowieso nicht überwacht zu werden und nichts zu verbergen zu haben. Eine mögliche Erklärung scheint zu sein, dass Zustimmung zu diesen Aussagen nicht im Umkehrschluss bedeutet, dass die Sorgen geringer sind. Auch wenn die Items der Skala *Einstellungen* ursprünglich intendiert waren, um verschiedene Aspekte von Besorgnis zu erfassen, scheinen die drei Faktoren nicht drei latente Variablen eines Konstrukts zu sein, sondern im Gegenteil unabhängige Konstrukte widerzuspiegeln.

Dem Zusammenhang mit dem Ausmaß der Verhaltensänderung könnte eine differenzierte Betrachtungsweise der Items zu Grunde liegen. Analog zu den Ergebnissen aus der Studie von Dinev et al. (2008) wäre ein möglicher Erklärungsansatz, dass Internet-Nutzer die flächendeckende Datenspeicherung als angemessen empfinden, wenn sie gegen „kriminelle“ Individuen gerichtet ist. Sie lehnen diese also auf einer kognitiven Ebene nicht ab, ihnen ist allerdings durch die mediale Berichterstattung auch klar geworden, dass ihre persönliche Kommunikation, die als schützenswert betrachtet wird, damit ebenso für Regierungsorgane zugänglich wird - wogegen sie sich zu wehren versuchen.

Die Persönlichkeitsfaktoren *Neurotizismus*, *Extraversion*, *Offenheit für neue Erfahrungen* und *Verträglichkeit* erreichten in beiden Prädiktor-Modellen nicht das Signifikanzniveau. Nur Gewissenhaftigkeit kann in der Paper-Pencil-Stichprobe einen signifikanten Beitrag in der Schätzung der Verhaltensänderung leisten. Dies widerspricht zwar z.B. der Studie von Bansal und Kollegen (2010), die Forschungslage ist in diesem Bereich aber nicht eindeutig, das Ergebnis also nicht weiter überraschend und wie schon im Abschnitt 1.9 angesprochen vermutlich mitunter den unterschiedlichen Erhebungsinstrumenten für die Big 5 geschuldet. Dass gerade der Faktor Gewissenhaftigkeit als Prädiktor nützt ist intuitiv verständlich.

Das Regressionsmodell für die PP-Stichprobe ist in der Lage auffallend mehr Varianz, nämlich doppelt so viel (14% versus 27%), zu erklären. Es ist möglich, dass dies ein statistisches Artefakt durch die größere Varianz der Verhaltensänderung in der Online Stichprobe darstellt. Die Antworten der PP-Probanden sind homogener und dadurch leichter durch ein Modell erklärbar.

In der Online-Stichprobe scheint die Lebenszufriedenheit nicht durch die mediale Berichterstattung oder Sorgen um die Privatsphäre beeinflusst zu sein. In der Paper-Pencil-Stichprobe besteht allerdings ein positiv-signifikanter Zusammenhang zwischen Lebenszufriedenheit und politischen Bedenken, was bedeutet, dass Individuen mit höherer Lebenszufriedenheit die staatliche Intrusion eher als Verletzung ihrer Grundrechte und Eindringen in ihre Privatsphäre erachten. Dieser Zusammenhang scheint zunächst nicht logisch erklärbar, könnte aber mitunter durch die persönlichen Wichtigkeit von Privatheit bedingt sein, denn das persönliche Bedürfnis nach Privatsphäre übt auch einen signifikanten Einfluss auf das Ausmaß der Sorgen um die eigenen Online-Privatsphäre aus (Yao et al., 2006).

Im Vergleich der beiden Stichproben konnten keine signifikanten Unterschiede gezeigt werden. Nur Kognitive Bewertungen sind in diesen Stichproben tendenziell signifikant unterschiedlich; die Teilnehmer der PP-Stichprobe stimmten den Aussagen tendenziell mehr zu.

Die so gering ausgefallenen Unterschiede machen stutzig und werden noch dadurch gestützt, dass 70% der Online-Teilnehmer den Fragebogen nicht (oder eher nicht) lieber im Papier-Format ausgefüllt hätten. Die Sensibilität des Themas scheint also nach wie vor nicht in den Köpfen der Teilnehmer angekommen zu sein.

Zusammenfassend lässt sich also sagen, dass sowohl die mediale Berichterstattung als auch Sorgen um die Privatsphäre und die kognitive Bewertung von Datenspeicherungspraktiken,

sowie Wissen, potenziell als Prädiktoren für eine Verhaltensänderung im Bereich der protektiven Strategien zum Schutz der Online Privatsphäre herangezogen werden können, Internet-Nutzer aber immer noch wenige Strategien anwenden und sich der Tragweite des Themas nicht in vollem Ausmaße bewusst sind.

#### *4.2 Limitationen der Studie*

Die Aussagekraft der Ergebnisse wird durch die folgenden Limitationen der vorliegenden Studie beschränkt.

Zunächst kann nicht angenommen werden, dass die beiden Stichproben als repräsentativ für die Allgemeinbevölkerung gelten, da die Teilnehmer im Durchschnitt gebildeter sind, bessere Englischkenntnisse haben (ein im Online-Kontext nicht zu unterschätzender Faktor) und eher in Großstadtreionen leben als der „Durchschnittsbürger“.

Beim Vergleich der beiden Stichproben ist die starke Differenz in der Stichprobengröße zu beachten, welche durch die Limitation des Umfanges und Aufwandes einer akademischen Abschlussarbeit bedingt ist und möglicherweise Auswirkungen auf die Ergebnisse haben kann.

Der finale Fragebogen umfasste schließlich 12 Seiten und nahm je nach Teilnehmer bis zu 25 Minuten Bearbeitungszeit in Anspruch, was vor allem bei den online erhobenen Daten zu vielen Abbrüchen und generell zu geringer Motivation führte. Für zukünftige Arbeiten zu diesem Thema scheint es angebracht ein Instrument zu entwickeln, das nicht mit so vielen Items das Sicherheitsverhalten erfasst, sondern die Dimensionen auf wenige, aussagekräftige Fragen reduziert.

Auffällig war auch, dass einige Probanden selbst die gängigsten Strategien (z.B. Ad-Blocker) nicht kannten und es dadurch relativ häufig zu fehlenden Werten kam, was die

Aussagekraft der statistischen Analyse weiter einschränkt. Eine Möglichkeit wäre, die jeweiligen Maßnahmen zunächst zu erklären. Alternativ wäre es auch möglich fehlende Werte so zu interpretieren, dass der Teilnehmer die Strategie wohl nicht anwendet. Dieser Kausalzusammenhang kann aber korrekterweise nicht ohne eingängige Überprüfung geschlussfolgert werden.

Um erschöpfend zu klären, was die ausschlaggebenden Gründe für die geringe Änderung im Verhalten sind, bedarf es noch weiterer Forschung.

## 5. Zusammenfassung und Abstract

### 5.1 Abstract

Last year when institutional possibilities to monitor online behavior have been made public, controversial discussions in European media were evoked. So far research focused mainly on factors influencing privacy concerns and protective behaviors. Therefore this study tried to identify predictors for the change in behavior to protect one`s online privacy and their influence on the *satisfaction with life* in two populations. Multiple regression identified *knowledge*, *former behavior*, *media consumption*, *political concerns* and *privacy concerns* as predictors for the online acquired population. For the Paper-Pencil sample the significant predictors are *former behavior*, *media consumption* and *privacy concerns* as well, plus *cognitive appraisal* and *conscientiousness*. There were no significant differences in online behaviour and the amount of behaviour change between the two samples. Satisfaction with life was only correlated with political concerns for the Paper-Pencil sample. Both samples showed little knowledge of data gathering policies and low use of protective behaviors. The change in using those strategies after media coverage was not significant. It seems crucial to inform the public about data practices and the proper

use of protective strategies for maintaining a minimum of privacy online.

## 5.2 Zusammenfassung

Das Bekannt werden potenziell flächendeckender, institutioneller Datenspeicherung hat im letzten Jahr viel mediale Aufmerksamkeit erhalten. In der bisherigen Forschung wurden hauptsächlich Faktoren untersucht, die Besorgnis um private Daten und das Anwenden von Sicherheitsmaßnahmen beeinflussen. Die vorliegende Untersuchung hat sich daher mit Prädiktoren beschäftigt, die in einer online akquirierten, sowie einer Paper-Pencil erhobenen Stichprobe das Ausmaß der Veränderung in protektiven Verhaltensweisen und deren Einfluss auf die Lebenszufriedenheit der Teilnehmer vorhersagen können. Mithilfe einer multiplen Regression konnten in der Online-Stichprobe *Wissen*, *früheres Verhalten*, *Medienkonsum*, *politische Bedenken* und *Besorgnis* als signifikante Prädiktoren identifiziert werden. In der Paper-Pencil-Stichprobe waren es *Medienkonsum*, *Verhalten vorher* und *Besorgnis*, sowie *Gewissenhaftigkeit* und *kognitive Bewertung der Überwachungspraktiken*. Zwischen den Stichproben gab es keine signifikanten Unterschiede im Verhalten und dem Ausmaß, in dem das online Verhalten verändert wurde. Nur das Ausmaß, in dem *politische Bedenken* in der Paper-Pencil-Stichprobe geäußert wurden, stand in signifikantem Zusammenhang mit der *Lebenszufriedenheit*. Zusammenfassend lässt sich sagen, dass über beide Stichproben hinweg *Wissen* und die *Anwendung von Strategien* gering ausgeprägt sind und sich das Verhalten nicht signifikant verändert hat. Für die Zukunft sollte der Öffentlichkeit Wissen über Datensammelungspraktiken zugänglicher gemacht und die effektive Anwendung von Sicherheitsstrategien vermittelt werden, um weiterhin ein Minimum an Privatsphäre im online-Kontext gewährleisten zu können.

## 6. Literaturverzeichnis

- Agentur der Europäischen Union für Grundrechte. (2014). *Handbuch zum europäischen Datenschutzrecht*. Luxemburg: Amt für Veröffentlichungen der Europäischen Union. Retrieved from <http://fra.europa.eu/de/publication/2014/handbuch-zum-europaischen-datenschutzrecht> [04.11.2014]
- Bansal, G., Zahedi, F., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, 49(2), 138-150. doi:10.1016/j.dss.2010.01.010
- Betz, J., & Kübler, H.-D. (2013). *Internet governance*. New York: Springer.
- Bigo, D., Boulet, G., Bowden, C., Carrera, S., Guild, E., Hernanz, N., & Scherrer, A. (2013). Open Season for Data Fishing on the Web - The Challenges of the US PRISM Programme for the EU. *CEPS Policy Brief*, 18(293). Retrieved from <http://dare.uva.nl/document/2/148168> [26.08.2014]
- Bubaš, G., Orehovački, T., & Konecki, M. (2008). Factors and Predictors of Online Security and Privacy Behavior. *Journal of information and organizational sciences*, 32(2), 79-98. Retrieved from <http://jios.foi.hr/index.php/jios/index>
- Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and

protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, 58(2), 157-165. doi:10.1002/asi.20459

Budak, J., Anić, I.-D., & Rajh, E. (2013). Public attitudes towards privacy and surveillance in Croatia. *Innovation: The European Journal of Social Science Research*, 26(1-2), 100-118. doi:10.1080/13511610.2013.723404

Bühl, A., & Zöfel, P. (2000). *Eine Einführung in die moderne Datenanalyse unter Windows*. München, Deutschland: Addison-Wesley Verlag. Retrieved from <http://ebooks.pearson.de/>

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

Custers, B., van der Hof, S., Schermer, B., Appleby-Arnold, S., & Brockdorff, N. (2013). Informed Consent in Social Media Use - The Gap between User Expectations and EU Personal Data Protection Law. *SCRIPTed*, 10(4), 435-457. doi:10.2966/scrip.100413.435

Dehne, M. Schupp, J. (2007). *Persönlichkeitsmerkmale im Sozio-oekonomischen Panel (SOEP) - Konzept, Umsetzung und empirische Eigenschaften* (Report No. 26). Berlin, Deutsches Institut für Wirtschaftsforschung.

Deutscher Bundestag. (2012). *Stellungnahme des deutschen Bundetages gemäß Artikel 23 Absatz 3 Satz 1 des Grundgesetzes*.

(Drucksache 17/11352). Retrieved from  
[dipbt.bundestag.de/dip21/btd/17/113/1711325.pdf](http://dipbt.bundestag.de/dip21/btd/17/113/1711325.pdf)

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance - An empirical investigation. *The Journal of Strategic Information Systems*, 17(3), 214-233. doi:10.1016/j.jsis.2007.09.002

Dinev, T., Bellotto, M., Hart, P., Colautti, C., Russo, V., & Serra, I. (2005). *Internet Users, Privacy Concerns and Attitudes towards Government Surveillance- An Exploratory Study of Cross-Cultural Differences between Italy and the United States*. Presented at the Bled eConference eIntegration in Action, Bled. Retrieved from  
<http://aisel.aisnet.org/bled2005/30/> [28.10.2014]

Dommeyer, C. J., & Gross, B. L. (2003). What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing*, 17(2), 34-51. doi:10.1002/dir.10053

Eid, M., & Diener, E. (2004). Global judgement of subjective well-being: situational variability and long-term stability. *Social Indicators Research*, (65), 245-277. Retrieved from  
<http://link.springer.com/article/10.1023/B:SOCI.0000003801.89195.bc#page-1>

Field, A. P. (2009). *Discovering statistics using SPSS*. London, England: SAGE.

- Gelbord, B., Roelofsen, G. (2002). New Surveillance Techniques raise privacy concerns. *Communications of the ACM*, 45(11), 23-24. Retrieved from <https://clickhereforenc1101.files.wordpress.com/2011/03/option-al-ns-2.pdf>
- Gerlitz, J.-Y., & Schupp, J. (2005). *Zur Erhebung der Big-Five-basierten Persönlichkeitsmerkmale im SOEP* (Research Note). Berlin: Deutsches Institut für Wirtschaftsforschung. Retrieved from <http://www.diw-berlin.de/documents/publikationen/73/43490/rn4.pdf>
- Gidda, M. (2013, August 21). Edward Snowden and the NSA files - timeline. *The Guardian*. Retrieved from <http://www.theguardian.com> [21.08.2014]
- Glaesmer, H., Grande, G., Braehler, E., & Roth, M. (2011). The German Version of the Satisfaction With Life Scale (SWLS): Psychometric Properties, Validity, and Population-Based Norms. *European Journal of Psychological Assessment*, 27(2), 127-132. doi:10.1027/1015-5759/a000058
- Goldberg, L. R., Johnson, J. A., Eber, H. W., Hogan, R., Ashton, M. C., Cloninger, C. R., & Gough, H. G. (2006). The international personality item pool and the future of public-domain personality measures. *Journal of Research in Personality*, 40(1), 84-96. doi:10.1016/j.jrp.2005.08.007

- Gosling, S. D., Rentfrow, P. J., & Swann, W. B. (2003). A very brief measure of the Big 5 personality domains. *Journal of Research in Personality*, 37 (2003), 504-528.
- doi:10.1016/S0092-6566(03)00046-1
- Greenwald, G. & MacAskill, E. (2013). NSA Prism program taps in to user data of Apple, Google and others. *Guardian News and Media Limited*. Retrieved from <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> [05.12.2014]
- Hahn, E., Gottschling, J., & Spinath, F. M. (2012). Short measurements of personality - Validity and reliability of the GSOEP Big Five Inventory (BFI-S). *Journal of Research in Personality*, 46(3), 355-359. doi:10.1016/j.jrp.2012.03.008
- Hallinan, D., Friedewald, M., & McCarthy, P. (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer Law & Security Review*, 28(3), 263-272.
- doi:10.1016/j.clsr.2012.03.005
- Hasher, L., Attig, M., & Alba, J. W. (1981). I Knew It All Along: Or, Did I? *Journal of Verbal Learning and Verbal Behavior*, (20), 86-96. doi:10.1016/S0022-5371(81)90323-6
- Hayes, C., Kesan, J. P., Bashir, M., Hoff, K., & Jeon, G. (2014). *Knowledge, Behavior, and Opinions Regarding Online Privacy* (Report No. 14-43). Illinois: Illinois Program in Law, Behavior and Social Science. Retrieved from

[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2418830](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418830)

[29.10.2014]

Hoffman, L. (1980). *Computers and privacy in the next decade*. New York: Academic Press.

Hoy, M. G., & Milne, G. (2010). Gender Differences in Privacy-Related Measures for Young Adult Facebook Users. *Journal of Interactive Advertising*, 10(2), 28-45.

doi:10.1080/15252019.2010.10722168

Hui K-L, Teo H, Lee S-Y. The value of privacy assurance: an exploratory field experiment. *MIS Quarterly* 2007; 31:19-33.

Retrieved from [jstor.org](http://jstor.org) [24.06.2015]

IBM Corp. Released 2013. *IBM SPSS Statistics for Mac, Version 22.0*. Armonk, NY: IBM Corp.

John, O. P., Naumann, L., & Soto, C. (2008). Paradigm shift to the integrative Big-Five taxonomy: History, measurement, and conceptual issues. In John, O. P., Robins, R. W., & Pervin, L. A. (Eds.). (2008). *Handbook of personality: theory and research* (3rd ed). New York: Guilford Press. Retrieved from <https://www.ocf.berkeley.edu/~johnlab/bigfive.htm>

Johnston, A., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, 34(3), 549-566. Retrieved from [misq.org](http://misq.org)

- Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, 17(4), 387-402. doi:10.1057/ejis.2008.29
- Kateb, G., Rosen, J., Schauer, F. (2001) Invasions of privacy: Violations of Boundaries. *Social Research*, 68(1), 203-235.
- Korzaan, M., & Boswell, K. (2008). The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems*, 48(4), 15-24. Retrieved from jcis-online.org
- Lang, F. R., John, D., Lüdtke, O., Schupp, J., & Wagner, G. G. (2011). Short assessment of the Big Five: robust across survey methods except telephone interviewing. *Behavior Research Methods*, 43(2), 548-567. doi:10.3758/s13428-011-0066-z
- Lenhart, A. & Madden, M. (2007): *Teens, privacy and Online Social Networks: How Teens manage their online identities and personal information in the age of MySpace*. Washington: PEW Internet & American Life Project.
- Levi, M., & Wall, D. (2004). Technologies, Security, and Privacy in the Post-9/11 European Information Society. *Journal of Law and Society*, 31(2), 194-220. Retrieved from jstore.org
- Li, Y. (2014). A multi-level model of individual information privacy beliefs. *Electronic Commerce Research and Applications*, 13(1), 32-44. doi:10.1016/j.elerap.2013.08.002

- Lim, S. S., Cho, H., & Sanchez, M. R. (2009). Online privacy, government surveillance and national ID cards. *Communications of the ACM*, 52(12), 116. doi:10.1145/1610252.1610283
- Litt, E. (2013). Measuring users' internet skills: A review of past assessments and a look toward the future. *New Media & Society* 15(4), 612-630. . doi:10.1177/1461444813475424
- Moloney, M., & Bannister, F. (2008). Online Privacy: Measuring Individuals' Concern. In G. Psaila & R. Wagner (Eds.) *E-commerce and web technologies* (Vol. 5183, pp 22-30). Berlin Heidelberg: Springer-Verlag.
- Moscardelli, D. M., & Divine, R. (2007). Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships with Privacy-Protecting Behaviors. *Family and Consumer Sciences Research Journal*, 35(3), 232-252. doi:10.1177/1077727X06296622
- Paine, C., Reips, U.-D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of "privacy concerns" and "privacy actions." *International Journal of Human-Computer Studies*, 65(6), 526-536. doi:10.1016/j.ijhcs.2006.12.001
- Park, Y. J. (2011). Digital Literacy and Privacy Behavior Online. *Communication Research*, 40(2), 215-236. doi:10.1177/0093650211418338
- Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers*

*in Human Behavior*, 28(3), 1019-1027.

doi:10.1016/j.chb.2012.01.004

Pavone, V., & Esposti, S. D. (2012). Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science*, 21(5), 556-572. doi:10.1177/0963662510376886

Phillips, D. J. (2004). Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies. *New Media & Society*, 6(6), 691-706. doi:10.1177/146144804042523

Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies*, 71(12), 1133-1143. doi:10.1016/j.ijhcs.2013.09.002

Rasmussen, M. V. (2006). *The risk society at war: terror, technology and strategy in the twenty-first century*. Cambridge ; New York: Cambridge University Press.

Regan, P. (1995). *Legislating privacy: Technology, social values and public policy*. Chapel Hill: University of North Carolina Press.

Rosen, J. (2000). *The unwanted gaze: the destruction of privacy in America* (1st ed). New York: Random House. Retrieved from <http://books.google.at/books?hl=de&lr=&id=DUoqk0JS8fcC&oi=fnd&pg=PA3&dq=Rosen,+J.+%282000%29>

- Schwaig, K. S., Segars, A. H., Grover, V., & Fiedler, K. D. (2013). A model of consumers' perceptions of the invasion of information privacy. *Information & Management*, 50(1), 1-12. doi:10.1016/j.im.2012.11.002
- Sheehan, K. B. (2002). Toward a Typology of Internet Users and Online Privacy Concerns. *The Information Society*, 18(1), 21-32. doi:10.1080/01972240252818207
- Siegel, D. A. (2013). Will You Accept the Government's Friend Request? *Social Networks and Privacy Concerns*, 8(11), e80682. doi:10.1371/journal.pone.0080682
- Sleeper, M., Balebako, R., Das, S., McConahy, A. L., Wiese, J., & Cranor, L. F. (2013). The post that wasn't: exploring self-censorship on facebook. In *Proceedings of the 2013 conference on Computer supported cooperative work* (pp. 793-802). San Antonio, Texas: ACM.
- Smit, E. G., Van Noort, G., & Voorveld, H. A. M. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*, 32, 15-22. doi:10.1016/j.chb.2013.11.008
- Smith, H. J., Dinev, T. & H. Xu, H. 2011. Information privacy research: An interdisciplinary review. *MIS Quarterly* 35(4), 989-1015. Retrieved from <http://dl.acm.org/citation.cfm?id=2208950>

Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior*, 27(1), 590–598. doi:10.1016/j.chb.2010.10.017

The Gallup Organization. (2008). *Data Protection in the European Union. Citizens` perceptions*. Flash Eurobarometer (225).

Retrieved from

[http://ec.europa.eu/public\\_opinion/flash/fl\\_225\\_en.pdf](http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf)

[09.10.2014]

The Guardian (Producer). (2013). *NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of*

*things'*. Available from

<https://www.youtube.com/watch?v=0hLjuVyIIrs&spfreload=10>

The Harris Poll. (2013). *Less than Half of Americans trust Federal Government with Personal Info* (The Harris Poll Nr. 45). New York: Harris Interactive Inc.

TNS Opinion & Social. (2010). *Attitudes on Data Protection and Electronic Identity in the European Union*. Special

Eurobarometer (395). Retrieved from

[http://ec.europa.eu/public\\_opinion/archives/ebs/ebs\\_359\\_en.pdf](http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf)

Turow, J., Feldman, L., & Meltzer, K. (2005). *Open to*

*Exploitation: America`s Shoppers Online and Offline*.

Pennsylvania, USA: Annenberg School for Communication

Departmental Papers. Retrieved from upenn.edu

- Turow, J., & Hennessey, M. (2007). Internet privacy and institutional trust: insights from a national survey. *New Media & Society, 9*(2), 300-318. doi:10.1177/1461444807072219
- Viseu, A., Clement, A., & Aspinall, J. (2004). Situating Privacy Online: Complex perceptions and everyday practices. *Information, Communication & Society, 7*(1), 92-114. doi:10.1080/1369118042000208924
- Westin, A. F. (1970). *Privacy and Freedom*. London: The Bodley Head Ltd.
- Westin, A. F. (2003). Social and Political Dimensions of Privacy, *Journal of Social Issues, 59*(2), 431-453. Retrieved from <http://www.privacysummersymposium.com/reading/westin.pdf>
- Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management, 18*(4), 326-348. doi:10.1108/09564230710778128
- Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior, 28*(3), 889-897. doi:10.1016/j.chb.2011.12.008
- Yao, M. Z., & Linz, D. G. (2008). Predicting Self-Protections of Online Privacy. *CyberPsychology & Behavior, 11*(5), 615-617. doi:10.1089/cpb.2007.0208

- Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*, 58(5), 710-722.  
doi:10.1002/asi.20530
- Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *The Journal of Consumer Affairs*, 43(3), 389-418.  
Retrieved from orionshoulders.com
- Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, 16(4), 479-500. doi:10.1080/1369118X.2013.777757
- Zukowski, T., & Brown, I. (2007). Examining the Influence of Demographic Factors on Internet Users`Information Privacy Concern. In *Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries* (pp. 197-204). ACM New York.  
doi:10.1145/1292491.1292514

## 7. Tabellen- und Abbildungsverzeichnis

### 7.1 Tabellenverzeichnis

Tabelle 1. Demographische Daten beider Stichproben. ....	S.47
Tabelle 2. Häufigkeit der Nutzung unterschiedlicher Dienste im Internet. .....	S. 49
Tabelle 3. Häufigkeit der Nutzung von unterschiedlichen Online Social Networks. ....	S. 50
Tabelle 4. Ausmaß der Anwendung protektiver Strategien. ....	S. 51
Tabelle 5. Statistische Kennwerte des Summscores des „Knew-it-all-along“- Effekts. ....	S. 52
Tabelle 6. Statistische Kennwerte des SWLS. ....	S. 53
Tabelle 7. Intensität der aktiven Beschäftigung mit der medialen Berichterstattung. ....	S. 54
Tabelle 8. Scores der Knowledge Skalen Risiken der Datensammlungspraktiken und Gesetzliche Grundlagen, sowie Gesamtscore in beiden Stichproben.....	S. 55
Tabelle 9. Big 5 Persönlichkeitsfaktoren (BFI-S). ....	S. 56
Tabelle 10.1. Hätten Sie diesen Fragebogen lieber im Papier Format ausgefüllt? .....	S.57
Tabelle 10.2. Hätten Sie diesen Fragebogen auch online ausgefüllt? ...	S. 58
Tabelle 11. Statistische Kennwerte der Rohwerte zu Besorgnis, Kognitive Bewertung und Politische Bedenken auf Item-Ebene. ....	S. 59
Tabelle 12. Rotierte Komponentenmatrix für „Einstellungen zur medialen Berichterstattung“. ....	S. 61
Tabelle 13. Beta und Signifikanzniveaus der Prädiktoren mit signifikantem Erklärungswert. ....	S. 64
Tabelle 14. Zusammenhang zwischen Lebenszufriedenheit, Medienkonsum und Einstellungen zur flächendeckenden Datenspeicherung. ....	S.67
Tabelle 15. Ergebnisse der T-Tests mit Effektstärke (d) für den Stichprobenvergleich im Sicherheitsverhalten vor und nach der Berichterstattung, sowie Wissen. ....	S.68

Tabelle 16. Ergebnisse der Mann-Whitney-U Tests mit Effektstärke ( $r$ ) für den Stichprobenvergleich in Verhaltensänderung und Einstellungen zur Datenspeicherung. .... S. 68

Tabelle 17. Hypothesenprüfung für beide Stichproben. .... S. 70

## *7.2 Abbildungsverzeichnis*

Abbildung 1. Staatsbürgerschaft der Teilnehmer in Prozent. .... S. 48

Abbildung 2. Prozent der Teilnehmer mit niedriger/mittlerer/hoher Lebenszufriedenheit. .... S. 53

Abbildung 3. Einstellung zum Erhebungskontext in der Online-Stichprobe. S.57

Abbildung 4. Einstellung zum Erhebungskontext in der Paper-Pencil Stichprobe. .... S. 58

## 8. Anhang

## 8.1 Korrekte Items der Skala Wissen (Turow et al., 2005)

Tab. 18: Korrekte Items der Skala Wissen nach EU Datenschutzrecht

Risiken der Datensammelungspraktiken	richtig	Gesetzliche Grundlagen	richtig
Item 1	x	Item 1	x
Item 2	x	Item 2	x
Item 3	x	Item 3	
Item 4	x	Item 4	x
Item 5		Item 5	
Item 6	x	Item 6	x
Item 7	x	Item 7	
Item 8			

## 8.2 Deutsche Übersetzung der Skala Wissen (Turow et al., 2005)

	ja	nein	Ich weiß es nicht.
Von Ihrem Surf-Verhalten ausgehend können Firmen heutzutage zielgenaue Werbebotschaften einblenden.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Auch wenn Sie nicht auf eine E-Mail reagieren, können Firmen wissen, dass Sie diese geöffnet haben.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Eine Website kann Informationen über Sie sammeln, auch wenn Sie sich dort nicht registrieren.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Beliebte Suchmaschinen wie z.B. Google erfassen die Seiten von denen sie kommen und auf die Sie als nächstes zugreifen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
E-commerce-Unternehmen wie Amazon, oder Video-on-Demand-Services (maxdome, Sky, etc.) dürfen Ihre persönlichen Daten an Behörden und Kreditauskunfteien (Schufa, Kreditschutzverband) weitergeben.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Alles was Sie während des Online-Surfens anklicken kann als Datenspur gespeichert werden.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Was Sie auf der Seite eines Online-Shops ansehen wird fast immer überwacht und gespeichert.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hat eine Website eine Datenschutzrichtlinie, dann werden Ihre Daten nicht an andere Webseiten oder Firmen weitergegeben.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

	ja	nein	Ich weiß es nicht.
Gesetzliche Bestimmungen schränken ein, wie lange der Betreiber einer Webseite Daten über Sie aufheben darf.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Es ist legal, dass Online-Shops zur gleichen Uhrzeit für ein und dieselbe Sache verschiedene Preise von verschiedenen Kunden verlangen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Es ist vom Gesetz her möglich, dass eine Website Ihre Daten an Geschäftspartner weitergibt ohne dass Sie wissen, an wen diese Daten gegeben werden.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vom Gesetz her sind E-Commerce-Betreiber wie Amazon dazu verpflichtet, Ihnen Einblick in die Daten zu gewähren, die über Sie gesammelt werden.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Nach dem Datenschutzgesetz müssen die Nutzungsbedingungen einer Website leicht verständlich formuliert sein und ein einheitliches Format haben.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ausländische Behörden können auch ohne Ihre Zustimmung und Ihr Wissen online Daten über Sie sammeln.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Nach dem Datenschutzgesetz dürfen von einer Online-Banking-Seite keine persönlichen Daten weitergegeben werden, auch nicht an Tochtergesellschaften.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

### 8.3 Messinstrument

Die selbst entworfenen Teile des Fragebogens folgen auf den nächsten Seiten.

Sehr geehrte Teilnehmer,

die folgende Studie beschäftigt sich mit Ihrer Auffassung zur möglichen Datenspeicherung von Internet-Aktivitäten. Das Ausfüllen wird ca. 15 Minuten Ihrer Zeit in Anspruch nehmen. Bitte lesen Sie alle Fragen genau und antworten Sie ehrlich.

Alle Angaben werden anonymisiert verarbeitet.

**Vielen Dank für Ihre Teilnahme!**

**1. Alter**

Alter  Jahre

**2. Geschlecht**

- männlich
- weiblich
- keine Angabe

**3. Bildungsgrad**

- Pflichtschule
- Lehre
- Matura/Abitur
- Hochschulabschluss

Beruf

Studiengang

- |                    | keine                 | wenig                 | mittelmäßig           | ziemlich gut          | sehr gut              |
|--------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Englischkenntnisse | <input type="radio"/> |

**4. Staatsbürgerschaft**

Staatsbürgerschaft

**5. Familienstand**

- in einer Beziehung
- alleinstehend

**6. Der Ort, in dem ich momentan wohne, ist...**

- ländlich (bis zu als 5000 Einwohner).
- eine Kleinstadt (bis zu 20.000 Einwohner).
- eine Stadt (bis zu 100.000 Einwohner).
- eine Großstadt (mehr als 100.000 Einwohner).
- eine Metropole (mehr als 1 Mio. Einwohner).

### Ich nutze das Internet...

	nie	selten	gelegentlich	oft	immer
zum Zeitvertreib	<input type="radio"/>				
für die Arbeit/Ausbildung	<input type="radio"/>				
zum Online Social Networking	<input type="radio"/>				
zur Unterhaltung (z.B. Musik, Filme, etc.)	<input type="radio"/>				
um Nachrichten zu verfolgen	<input type="radio"/>				
zum Shoppen	<input type="radio"/>				
um Informationen zu suchen	<input type="radio"/>				
um E-Mails zu schreiben	<input type="radio"/>				

### Ich nutze folgende Online Social Networks:

	nie	selten	gelegentlich	oft	immer
Facebook	<input type="radio"/>				
Twitter	<input type="radio"/>				
Myspace	<input type="radio"/>				
Instagram	<input type="radio"/>				
Vine	<input type="radio"/>				
andere	<input type="radio"/>				

### 9. Mediale Berichterstattung:

Ich habe mit Interesse die Berichterstattung über die Möglichkeit der Überwachung, Speicherung und Analyse nahezu aller Internet-Aktivitäten wahrgenommen.

nein
  eher nein
  teils teils
  eher ja
  ja

### Ich habe mich aktiv über folgende Medien über die Berichterstattung im Bezug auf potenzielle Datenspeicherung informiert:

	gar nicht	kaum	etwas	überwiegend	sehr
Radio	<input type="radio"/>				
Zeitung	<input type="radio"/>				
Fernsehen	<input type="radio"/>				
Illustrierte/Magazine	<input type="radio"/>				
Online-Zeitung	<input type="radio"/>				
Internetforen	<input type="radio"/>				

## 10. Bitte bewerten Sie folgende Aussagen:

	trifft nicht zu	trifft eher nicht zu	trifft eher zu	trifft zu
Mir war bereits vor der Berichterstattung klar, dass nahezu alle Daten von Institutionen überwacht, gespeichert und analysiert werden können.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mir war bereits vor der Berichterstattung klar, dass Daten tatsächlich überwacht, gespeichert und analysiert werden.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mir war bereits vor der Berichterstattung klar, dass es möglich ist flächendeckend alle Anrufe eines Landes aufzuzeichnen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## 11. Bitte bewerten Sie, inwieweit Sie folgende Verhaltensweisen VOR, bzw. NACH dem Bekanntwerden des Ausmaßes der möglichen Datenspeicherung gezeigt haben.

	vorher					nachher				
	nie	selten	gelegentlich	oft	immer	nie	selten	gelegentlich	oft	immer
Ich mache die neusten Updates meines Betriebssystems.	<input type="checkbox"/>									
Ich mache die neuesten Updates meiner benutzten Programme.	<input type="checkbox"/>									
	gar nicht	fast nicht	teilweise	fast ganz	ganz	gar nicht	fast nicht	teilweise	fast ganz	ganz
Ich habe vor dem letzten Update die Lizenzvereinbarungen gelesen.	<input type="checkbox"/>									

	vorher					nachher				
	nein	eher nicht	teils-teils	eher ja	ja	nein	eher nicht	teils-teils	eher ja	ja
Ich habe mich vor dem letzten Update über dessen Inhalte informiert.										
Meine Passwörter gelten als sicher (Groß-, und Kleinbuchstaben mit Zahlenkombinationen, mind. 20 Zeichen).										
	eines für alle	wenige	mehrere	immer ein	eigenes	eines für alle	wenige	mehrere	immer ein	eigenes
Ich nutze ... Passwörter für unterschiedliche Dienste.										
	nie	selten	gelegentlich	oft	immer	nie	selten	gelegentlich	oft	immer
Ich nutze eine Firewall.										
Ich nutze eine Firewall, die verhindert, dass automatisch Daten an den Betreiber gesendet werden (z.B. Zone-Alarm).										
Ich nutze einen Ad-Blocker.										
Ich nutze Anti-Virus Programme.										
Ich habe die WebCam an meinem Computer abgeklebt.										
Ich säubere meine Internet-History.										
Ich entferne Cookies, deinstalliere Toolbars u.ä.										
Ich verschlüssele meine IP-Adresse durch Tor, VPN-Dienste, oder andere Möglichkeiten bei der Internetnutzung.										
Ich verschlüssele meine IP-Adresse durch Tor, VPN-Dienste, oder andere Möglichkeiten anlassbezogen.										
Ich nutze Google als Suchmaschine.										
Ich nutze Startpage/Duck.duck.go, oder andere sichere Suchmaschinen.										

	vorher					nachher				
	nie	selten	gelegentlich	oft	immer	nie	selten	gelegentlich	oft	immer
Ich nutze Startpage/Duck.duck.go, oder andere sichere Suchmaschinen anlassbezogen.										
Ich nutze Microsoft Outlook.										
Ich nutze G-Mail.										
Ich nutze Klienten, oder Provider, die E-Mails verschlüsselt senden.										
Ich nutze Clouds (z.B. Dropbox) zur Datenspeicherung.										
Ich nutze Doodle.										
Ich nutze den Adobe Flash Player.										
Ich nutze Spam Filter für meinen E-Mail Account.										
Ich säubere meine W-Lan History.										
Ich nutze Google Chrome.										

	keine	eine	bis zu 5	>5	bis zu 15	bis zu 20	>20
Ich habe ... Apps auf meinem Smartphone installiert.							

Ich habe bei der Installation einer App schon Mal den Zugriff auf ... erlaubt (Merfnennungen möglich):

	nie	selten	gelegentlich	oft	immer
Eigene Telefonnummer					
E-Mail Adressen					
Gespeicherte Telefonnummern					
Anruflisten					
Bilder					
Videos					
Standort					



nachher	1-3	4-6	7-8	9-12	13-19	20-30	30-60	>60
Wie viele Zeichen haben Sie durchschnittlich bei Ihren Passwörtern?								

	vorher					nachher				
	nie	selten	gelegentlich	oft	immer	nie	selten	gelegentlich	oft	immer
Wenn mir Inhalte auf Webseiten gefallen drücke ich auf „Gefällt mir“.										
Ich buche Flüge online.										
Ich habe meine Kreditkarten-Details schon Mal online angegeben.										
Ich habe meine Passnummer schon Mal online angegeben.										

14. Wie sehr stimmen Sie folgenden Aussagen zur Überwachung von Internet Aktivitäten zu?

	starke Ablehnung			starke Zustimmung		
Ich mache mir Sorgen um die Macht, die die Regierung hat um Online-Aktivitäten aufzuzeichnen.	<input type="radio"/>					
Ich mache mir Sorgen darüber, dass meine im Internet preisgegebenen persönlichen Informationen (z.B. E-Mails, online Shopping, Surf-Aktivitäten, etc.) offener für Kontrollen von Regierung und Wirtschaft sein werden.	<input type="radio"/>					
Ich mache mir Sorgen um die Möglichkeiten der Regierung Internet Aktivitäten zu überwachen.	<input type="radio"/>					

15. Im Folgenden geht es um Ihre persönliche Meinung zum Thema Datenspeicherung.

Die Möglichkeit der flächendeckenden Datenspeicherung aller Online Aktivitäten durch Regierungen finde ich/macht mich:

	stimme nicht zu	stimme eher nicht zu	teils teils	stimme eher zu	stimme voll zu
angemessen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Wichtig für unsere Sicherheit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
auch nichts anderes, als wir freiwillig durch die Nutzung von Facebook&Co tun.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ich habe nichts zu verbergen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ich werde sowieso nicht überwacht	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
eindringen in meine Privatsphäre	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Verstoß gegen meine Grundrechte	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ist für mich ein Ärgernis	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
macht mir Angst	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

17. Hätten Sie diesen Fragebogen auch online ausgefüllt?

Nein	eher nein	Ich weiß es nicht.	eher ja	ja
<input type="checkbox"/>				

Vielen Dank für Ihre Teilnahme! Sollten Sie noch Fragen zur Studie haben, oder sich für die Forschungsergebnisse interessieren wenden Sie sich gerne unter [t.sittauer@gmx.net](mailto:t.sittauer@gmx.net) an die Studienleiterin!

## 9. Lebenslauf

**Persönliche Angaben**

---

Name	Teresa Amelie Sittauer
Staatsangehörigkeit	Deutsch
Geburtsdatum	21.06.1989

**Schul- und Berufsbildung**

---

Mai – August 2013	Praktikum in der <i>Lehr- und Forschungspraxis</i> der Klinischen-Psychologie, Universität Wien.
März 2011	Workshop im Bereich Sexualaufklärung und Präventionsarbeit.
2010-2011	Mitarbeit im Präventionsprojekt <i>Achtung Liebe</i> der AMSA.
2010	1. Diplomprüfungszeugnis
Juli 2009	Praktikum in der Tagesklinik der <i>Kinder- und Jugendpsychiatrie Nürnberg</i> .
Seit WS 2008	Diplomstudium der Psychologie an der <i>Universität Wien</i> .
2008	Abitur
2006/2007	5-monatiger Auslands-aufenthalt an der <i>Oliver Springs High School</i> , Tennessee, USA
1999 - 2002	Tutorentätigkeit.
ab 1999	Adam-Kraft-Gymnasium Schwabach, <i>mit bilingualem Unterricht in Geographie</i> .
1995-1999	<i>Johannes-Helm-Schule</i> , Schwabach

## **Persönliche Fähigkeiten und Kompetenzen**

---

### *Sprachen*

Muttersprache

Deutsch

Fremdsprachen

1. Englisch (fließend)
1. Latein (großes Latinum)
2. Italienisch (Grundkenntnisse)
3. Dänisch (5-monatiger Sprachkurs)

### *Führerschein*

2007, Klasse B