Ein Kampf gegen Windmühlen: Qualitative Studie über Informatikabsolvent_innen und ihre Datenprivatheit

Gina Maria Schmidbauer-Wolf
Technische Universität Darmstadt – Wissenschaft und Technik für Frieden und Sicherheit (PEASEC)
Darmstadt, Germany
{lastname}@peasec.tu-darmstadt.de

Franziska Herbert
Technische Universität Darmstadt – Wissenschaft und Technik für Frieden und Sicherheit (PEASEC)
Darmstadt, Germany
{lastname}@peasec.tu-darmstadt.de

Christian Reuter
Technische Universität Darmstadt – Wissenschaft und Technik für Frieden und Sicherheit (PEASEC)
Darmstadt, Germany
{lastname}@peasec.tu-darmstadt.de

ZUSAMMENFASSUNG

Wie werden eigene private Daten geschützt? Um dieser Frage nachzugehen, wurde in einer qualitativen Studie mit sechs Informatikabsolvent_innen erfragt, wie diese die Privatheit ihrer Daten schützen. Das Ziel der teilstrukturierten Interviews war es einen möglichst breiten Überblick über tatsächlich verwendete Techniken und Technologien zum Schutz der privaten Daten zu gewinnen. Während sich die Vermutung bestätigte, dass alle Teilnehmer_innen ein Bewusstsein für die Brisanz ihrer privaten Daten hatten, unterschieden sich die Definitionen ebendieser privaten Daten sowie das Verhalten, um diese zu schützen. Es konnte beobachtet werden, dass viel Wissen in diesem Bereich nicht zwangsläufig zu einem vorsichtigeren Handeln führt. Mögliche genannte Strategien zum Schutz der eigenen Daten sind: Informiert bleiben, Datensparsamkeit, Vermeidung der Produkte bestimmter Konzerne sowie Resignation. Als Motivation für das jeweilige Verhalten wurden sowohl politische, philosophische, utilitaristische, als auch angstgetriebene Gründe genannt. Letztere können in Angst vor Diebstahl und Angst vor Andersbehandlung unterschieden werden.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; • **Social and professional topics** → *Informal education*; *Computing / technology policy*; *Cultural characteristics.*

MuC'19 Workshops, Hamburg, Deutschland

https://doi.org/10.18420/muc2019-ws-302-06

KEYWORDS

privacy, personal data, privacy literacy, online behaviour, privacy enhancing technologies

1 EINLEITUNG

In Zeiten fortschreitender Digitalisierung und damit einhergehender möglicher unbeabsichtigter Preisgabe von persönlichen Daten oder gar Überwachung ist ein besonderer Schutz der persönlich Daten notwendig. Hierbei muss auch unterschieden werden zwischen der unfreiwilligen Weitergabe von Daten und der beabsichtigten Freigabe von Daten, beispielsweise im Krisenkontext (vgl. [1]). Technologien, die die Privatheit persönlicher Daten unterstützen und schützen, existieren bereits unter dem Begriff "Privacy Enhancing Technologies" (vgl. [5]). Doch wie finden solche Technologien oder Techniken zur Wahrung der eigenen Privatheit Anwendung?[1] Im Folgenden wird dieser Frage in Form einer qualitativen Studie nachgegangen. In der Absicht eine möglichst breite Übersicht über die Verwendungen dieser Technologien und Techniken zu erlangen, wurden sechs Absolvent_innen der Informatik in teilstrukturierten Interviews befragt. Es wurden keine Studienanfänger_innen befragt, um die Wahrscheinlichkeit einer höheren Datenprivatheits-Sensibilisierung oder Datenprivatheits-Alphabetisierung zu erhöhen, da die befragten Personen durch mindestens einen Studienabschluss in der Informatik diesen Themen länger exponiert sein könnten. Es wird erwartet, dass dieser Zielgruppe ihre Privatheit und die Gefährdung dieser bewusst ist.

Auf der Grundlage dieser gesammelten Informationen können Studien durchgeführt werden, die sich beispielsweise mit dem Sicherheitsverhalten von Informatiker_innen bezüglich ihrer Privatdaten im Allgemeinen beschäftigen. Hierbei sollten jedoch auch Informatiker_innen befragt werden, die keine akademische Ausbildung im Bereich der Informatik

[1] Weiterführende Informationen zu Anwendungsgebieten, Usability, UX und dem Engineering sicherheitskritischer Anwendungen finden sich in "Sicherheitskritische Mensch-Computer-Interaktion" (Reuter, 2018) [13]

absolviert haben. Auch ist es denkbar das Verhalten von Informatiker_innen bezüglich des Stands der Forschung, des Stands der Technik, des Aufwands und der Sinnhaftigkeit und der Machbarkeit für Nicht-Informatiker_innen zu bewerten. Hierzu wären auch Studien nötig, die das Verhalten bezüglich der Datenprivatheit von Nicht-Informatiker_innen im Allgemeinen und Speziellen untersuchen.

Interessant ist hierbei die Frage, ob es praktische und einfach zu erlernende oder anzuwendende Techniken und Technologien gibt, um die eigene Datenprivatheit zu wahren, die manchen Teilen der Bevölkerung bewusster sind als anderen. Wäre dem so, so sollten Schritte ergriffen werden, um die Privatheits-Alphabetisierung zu erhöhen.

Verwandte Arbeiten

Es gibt bereits Studien, die das Privatheitsverhalten von Studierenden (bspw. [3, 7, 10, 11, 16, 18, 26]) untersuchen. Diese verfolgen jedoch nicht das Ziel dieser Studie, Anregungen und Wissen zu sammeln. Die meisten Studien wollen das Verhalten einzelner Gruppen, eben beispielsweise Studierender, beschreiben, bewerten oder Instrumente entwickeln, mit denen sich dieses Privatheitsverhalten messen lässt. Auf der anderen Seite gibt es auch bereits praktische Studien, die die Anwendbarkeit einzelner Privatheits- und Sicherheitsmaßnahmen untersuchen.

Lawler und Molluzzo [10] untersuchen das Wissen von Studierenden im ersten Jahr bezüglich ihres Umgangs mit Privatheit und Sicherheit anhand ihres Verhaltens auf Seiten sozialer Netzwerke (Social Network Sites – SNS) und ihrem Verhalten gegenüber Privacy-Settings und -Vereinbarungen. Die Daten wurden mithilfe eines Fragebogens, bei dem nur diskrete Werte als Antworten zulässig waren, erhoben. Diese Studie hat somit einen Fokus auf Studienbeginner_innen und ist deskriptiver Natur, indem sie versucht deren Verhalten zu beschreiben. In einem ebenfalls auf dieser Studie aufbauenden Paper [11], bei dem auch Studierende aus höheren Semestern berücksichtigt werden, kommen Lawler, Molluzzo und Doshi zu dem Schluss, dass die erfragten Daten die Konklusion zulassen, dass Studierende mehr in Sicherheits- und Privatheitsfragen geschult werden müssten. Da die Studie vor acht Jahren durchgeführt wurde und es seitdem sowohl beträchtliche Entwicklungen bei Technologien als auch der Nutzung des Internets gab, sind Verhaltensänderungen, gerade jüngerer Menschen, zu erwarten. Es könnte auch ein anderes Bewusstsein bezüglich Privatheitsproblemen geben, wenn Personen mit Technologien aufwachsen oder deren Nachteile in den Medien oder ihrem Umfeld diskutiert werden. Deshalb ist eine Wiederholung der Studie mit einem Vergleich zu den damaligen Ergebnissen durchaus interessant. Bornoe und Barkhuus [3] betrachten ebenfalls das Privatheitsverhalten Studierender in sozialen Netzwerken. Das Ergebnis dieser Studie zeigte auch, wie die vorhergehend erwähnten Arbeiten, dass die befragten Studierenden wenig bis keine Ressourcen oder Energie in die Privaterhaltung ihrer Daten steckten und kein ausgeprägtes Bewusstsein hierfür hatten. Auch diese Studie liegt acht Jahre zurück und es ist zu untersuchen, ob die Entwicklungen der seitdem vergangenen Zeit einen Einfluss auf das allgemeine Privatheitsverhalten Studierender in sozialen Netzwerken hatten. Die Daten wurden in teilstrukturierten Interviews erhoben und die Teilnehmer_innen waren vornehmlich Bacheloranden ("undergraduates"). Yang und Wang [26] untersuchten die Privatheitswahrnehmung der eigenen Daten von asiatischen Studierenden. Zusätzlich zu dem Zeitfaktor (Studie von 2014), kann es sein, dass es eventuell kulturelle Unterschiede zu Deutschland oder westlichen Ländern gibt, die die Ergebnisse beeinflusst haben. Diese bis hier erwähnten Arbeiten fokussieren die Deskription des Verhaltens Studierender.

Das Privatheitsverhalten von Studierenden und wissenschaftlichen Mitarbeiter_innen bezüglich beider zuvor genannten Bereiche, SNS und E-Learning, untersuchen Ball, Ramim und Lewy [2]. In dieser Studie stellen sie fest, dass auch die Nutzer_innen, die behaupten sich der potenziellen Sicherheitsrisiken bewusst zu sein, sich nicht dementsprechend verhalten. Daraus folgern sie, dass Gewohnheitstheorie ("habit theory" [sic]) in der Informatik angewandt werden müsste, was sie im Rahmen dieses Papers auch durchführen. Es handelte sich um eine quantitative empirische Studie, die ein Fragebogeninstrument entwickelt, um die Wahrnehmung und das Verhalten von Nutzer_innen bezüglich der Privatheit ihrer Daten zu messen. Alle hier genannten Studien [2, 3, 10, 11, 26] sind auf bestimmte Plattformen oder Zwecke – Social Media und E-Learning – limitiert.

Rowan et al. [16] sowie Braghin et al. [4] untersuchen das Privatheitsverhalten von Nutzer_innen bezüglich ihres Umgangs mit Smartphones und Anwendungen auf Smartphones. Rowan et al. [16] erhoben hierfür Daten von Studierenden aus Informatik-Kursen mithilfe eines Fragebogens mit geschlossenen Fragen. Sie kommen zu dem Schluss, dass die Sensibilisierung der Studierenden bezüglicher ihrer Privatdaten sowie deren Umgang mit diesen nicht ausreichend seien und hier Maßnahmen ergriffen werden müssten. Braghin et al. [4] untersuchen den Umgang mit Datenschutzerklärungen für mobile Anwendungen und kommen dabei zu dem Schluss, dass die befragten Personen dieser wenig Beachtung schenken.

Haltinner, Sarathchandra und Lichtenberg [7] untersuchten in qualitativen Interviews die Wahrnehmung von Risiken, Sicherheit und Privatheit im Onlinekontext. Hierbei wurden 21 Studierende nach ihren persönlichen Erfahrungen und Wahrnehmungen in Interviews befragt. Haltinner et al. postulieren, dass sich das Verhalten der Studierenden bildet

anhand von Routinen, Ritualisierung von Risiken, einer optimistischen Voreingenommenheit sowie ihrer Selbstwirksamkeitserwartung. Als Strategien zum eigenen Schutz wurden das zurate ziehen von glaubwürdigen Quellen, eingeschränkte Informationsweitergabe sowie eine vorgetäuschte aber angenommene – erlernte – Hilflosigkeit genannt. In dieser Studie wurden Studierende unterschiedlicher Fachrichtungen befragt, weswegen eine Studie mit Informatiker_innen ein anderes Ergebnis liefern könnte. In jedem Fall ist es interessant die Resultate dieser Studie mit denen der vorliegenden Studie zu vergleichen. Sarathchandra, Haltinner und Lichtenberg [18] beschäftigen sich in einer späteren Studie kausalanalytisch mit der Frage des Privatheitsempfindens Studierender, wobei die Daten mithilfe eines Onlinefragebogens erhoben wurden. Es sollen Implikationen für Cybersecurity-Erlernende sowie -Praktiker abgeleitet werden können. Die größte Angst der Studierenden ist Identitätsdiebstahl, gefolgt von Angst vor Computerviren. Da es sich jedoch um geschlossene Fragen in einem Onlinefragebogen handelt, ist nicht ersichtlich, ob es nicht auch noch andere große Sorgen gibt. Sie urteilen außerdem, dass es sich hierbei um falsche Ängste handle, da die Wahrscheinlichkeit des Eintretens dieser Fälle sehr gering sei. Aus ihrer Argumentation heraus würden sie von informierteren Menschen erwarten, dass diese mehr Angst vor Wahrscheinlicherem hätten und implizieren hiermit eine Bildungslücke bzgl. Cyber-Security bei den befragten Studierenden.

Auch existiert Forschung hinsichtlich praktischer privatheits- und sicherheitsfördernder Einzelaspekte. Beispielsweise gibt es Studien und Überlegungen hinsichtlich sicherer und benutzbarer Passwörter (vgl. [6, 15, 23, 24]), sicherer und benutzbarer Betriebssysteme (vgl. [9, 22]) oder sicherer und benutzbarer E-Mail-Verschlüsselung (vgl. [17, 21, 25]). Reuter, Häusser et al. ([14]) fanden in einer repräsentativen Befragung, dass die Befragten ihre Daten in verschiedenen App-Kategorien unterschiedlich schützenswert einschätzten. So schätzen die Proband_innen ihre Daten beim mobilen Banking als am schützenswertesten ein. Ihre Daten beim online Dating empfanden die Proband_innen als am wenigsten schützenswert. Diese Studie konnte zeigen, dass Personen ihr Daten je nach Kontext (App) unterschiedlich schützenswert einschätzen. Die Maßnahme, die die Personen als am häufigsten angemessen für den Schutz ihrer Daten nannten, war die Verwendung von Passwörtern. Weitere praktische, da anwendbare oder aus der Anwendung heraus entstandene, Veröffentlichungen bezüglich benutzbarer Sicherheit und Privatheit sind die Ergebnisse von Hatscher et al. [8]. Diese führen UX und Privacy in einem praktischen Projekt zusammen, teilen ihre Lessons Learned mit, sowie Schmitt et al. [19, 20], die im Rahmen von Workshops zu „Usable Security & Privacy“ für alle Nutzer_innen-Gruppen anwendbare Methoden, Konzepte, Tools und Verfahren, die die Sicherheit und Privatheit der Anwender_innen fördern, sammeln.

Denkbar wäre es die bisher erhobenen Daten über das Verhalten, Wünsche etc. zu konsolidieren und eigene Daten zum Vergleich zu erheben, wobei auch die in letzter Zeit entwickelten Werkzeuge zum Einsatz kommen sollten. Viele Studien, alle genannten, kommen zu dem Schluss, dass das Privatheitsverhalten Studierender mangelhaft ist. Doch wie verhält es sich mit dem Privatheitsverhalten von Spezialist_innen in diesem Gebiet, der Ottonormalperson oder anderer Gruppen? Gibt es praktische Tipps, die jeder Person an die Hand gegeben werden können, nicht nur um ein Bewusstsein zu schaffen – das oftmals vorhanden zu sein scheint – sondern das Verbessern der eigenen Privatheit greifbar und einfach anwendbar zu machen? Um dieser Frage nachzugehen, muss zunächst erforscht werden was diese einfachen und anwendbaren Techniken und Technologien sind.

Forschungsfragen

Aus dieser Forschung und den noch bestehenden Lücken darin entstand die Motivation über das Erfragen des tatsächlichen Verhaltens von Informatiker_innen als Referenzgruppe im Vergleich zu den allgemeineren Gruppen (bspw. Studierende oder Studienanfänger).

- F1: Haben Informatikabsolvent_innen eine Sensibilisierung bezüglich ihres Umgangs mit ihren eigenen Privatdaten?
- F2: Gehen Informatikabsolvent_innen ähnlich mit ihren eigenen Privatdaten um?
- F3: Wie gehen Informatikabsolvent_innen mit ihren Privatdaten um?

2 METHODE

Um die Forschungsfragen zu beantworten, wurde eine explorative Studie durchgeführt. Durch die Studie entstanden keine irgendwie gearteten Gefahrensituationen für die teilnehmenden Personen. Den Teilnehmer_innen war bewusst, wofür ihre Aussagen verwendet werden sowie, dass ihre Angaben in nicht-anonymisierter Form gespeichert werden aber nur in anonymisierter Form veröffentlicht. Jeder teilnehmenden Person stand zu jedem Zeitpunkt die Freiheit zu nicht an der Studie teilzunehmen, ohne dadurch negative Konsequenzen zu erleiden.

Studiendesign

Es wurden teilstrukturierte Interviews jeweils in schriftlicher oder mündlicher Form durchgeführt. Diese Wahl wurde den Teilnehmer_innen gelassen, da sich deren Wünsche diesbezüglich unterschieden. Der Begriff der “teilstrukturierten

Interviews" wurde gewählt, da alle Teilnehmer_innen gebeten wurden alles zu erzählen, was ihnen zu den jeweiligen Fragen einfällt, auch wenn es sich um benachbarte Bereiche handelt. Die Fragen des Interviewleitfadens wurden hierbei jeweils in zwei Blöcke aufgeteilt präsentiert. Zunächst bekamen die Teilnehmer_innen den folgenden Fragenblock, anhand dessen sie sich entscheiden konnten, ob sie die Fragen schriftlich oder mündlich beantworten wollten:

- Schützt du deine privaten Daten?
  - wenn ja oder nein, wieso?
  - wenn ja, seit wann?
- Wie schützt du deine privaten Daten?
- Hast du das Gefühl, dass dich das Schützen deiner privaten Daten einschränkt?
- Was sind private Daten für dich?

Nachdem diese Fragen in der gewählten Form beantwortet wurden, folgte ein zweiter Fragenblock. Diese Reihenfolge wurde gewählt, damit die folgenden Fragen nicht die Antworten des ersten Blocks beeinflussen, da sie potenzielle Antworten auf die vorherigen Fragen darstellen. Der zweite Fragenblock beinhaltete folgende Fragen:

- Benutzt du Browser-Add-Ins, die deiner Privatheit dienen sollen?
- Benutzt du VPNs? Wenn ja, wozu?
- Fallen dir weitere implementierte PETs ein?

Rekrutierung und Sampling

Die interviewten Personen stammen aus dem Bekanntenkreis der Autor_innen, da eine motivierte Teilnahme an der Studie gewährleistet werden musste, um Studienabbrüche möglichst zu vermeiden und ausführliche Antworten auf alle Fragen zu erhalten. Auch die Bereitschaft persönlichere Informationen preiszugeben, sollte hierdurch gesteigert werden. Es wurde darauf geachtet möglichst unterschiedliche Informatikstudiengänge, -abschlüsse und ein ausgewogenes Geschlechterverhältnis zu erhalten. Hierbei handelt es sich somit um eine selbstselektierte Stichprobe durch die Autor_innen, die nicht als repräsentativ für die Grundgesamtheit angesehen werden kann, wobei eine heterogene gezielte Stichprobe angestrebt wurde. Innerhalb dieser heterogenen gezielten Stichprobe – die Personen wurden über unterschiedliche Messenger, Telefonate oder über eine Anfrage an eine Fachschaft – in dem Sinne des Prinzips der maximalen Ähnlichkeit ausgewählt, da es sich um Personen handeln musste, die mindestens einen Abschluss in Informatik besitzen. Dies geschah mit dem Ziel diese Personen, die Informatikabsolvent_innen, als Expert_innen zu interviewen. Die befragten Teilnehmer_innen sind in Tabelle 1 aufgeführt.

Tabelle 1: Teilnehmer_innen der qualitativen Studie

ID	Abschluss	Alter	Gender	Interviewform
P1	B.Sc., Dipl.Inf.	25	w	schriftlich
P2	B.A., M.Sc.	32	m	schriftlich
P3	B.Sc.	29	m	in persona
P4	B.A., M.Sc.	27	w	telefonisch
P5	Dipl.Inf., M.Sc.	24	m	in persona
P6	B.Sc.	26	w	telefonisch

Datenerhebung

Die Teilnehmer_innen der Studie durften individuell entscheiden, ob sie die Fragen schriftlich oder in einem Gespräch beantworten. Es entschieden sich jeweils zwei Personen für eine Beantwortung der Fragen in persona, zwei für eine schriftliche Beantwortung und zwei für ein telefonisches Interview. Bei den Personen, die die mündliche – telefonisch oder in persona – Variante bevorzugten, wurden Aufnahmen der Gespräche gemacht, welche sinngemäß transkribiert wurden. Die Gespräche dauerten alle zwischen 25 und 30 Minuten.

Datenanalyse

Um die Antworten der Befragten auszuwerten, wurde, wie im Folgenden beschrieben, vorgegangen. Die Aussagen jeder Person wurden zunächst schriftlich paraphrasiert und anschließend codiert. Codieren ist eine Methode zur Analyse von qualitativen Daten, die in der vorliegenden Studie datenreduzierend und induktiv, also aus dem bestehenden Datenmaterial heraus, verwendet wurde. Beim Codieren werden einer Aussage Bedeutungen zugewiesen. Die Codierung erfolgte ausschließlich auf inhaltlicher Basis und wurde aus ökonomischen Gründen nur von einer Person induktiv durchgeführt. Deshalb können keine Angaben zur Reliabilität der Codierung gemacht werden. Anschließend wurden die reduzierten Codes aller sechs Interviews vereinigt, um die Gesamthäufigkeit von Bedeutungsaussagen zu erkennen. In den Originalaussagen wurden außerdem Schlagworte identifiziert, die mit besonders starken Konnotationen verbunden sind (bspw. Angst, Hoffnung, Motivation).

3 RESULTATE

Im Folgenden werden die Ergebnisse der Interviews, gruppiert nach Fragestellung, vorgestellt. Allgemein war bei keiner Person das Sicherheitsverhalten von einem konkreten Ereignis geprägt. Bei zwei Personen nahm der Schutz der eigenen Daten über die Zeit ab: sie gaben aus Bequemlichkeitsgründen mehr Daten leichtsinniger [sic] online an.

Was sind private Daten

Ein Ansatz zur Definition privater Daten, der beobachtet werden konnte, ist insofern holistisch, dass alle von der Person produzierten und messbaren Daten privater Natur sind: "Für mich persönlich sind Daten alles was erfassbar und messbar ist. Alles was ich tue, lässt sich auf irgendeine Weise quantifizieren und auswerten." (P2). Auch P3 hat eine sehr weit gefasste Definition zu privaten Daten: "Alle Daten, die es erlauben Rückschlüsse auf mich, mein Verhalten, mein zukünftiges Verhalten zu erlangen". Dahingegen vertreten P1, P4 und P5 die Meinung, dass ihre Privatdaten lediglich die Daten sind, die auch auf ihren Personalausweisen zu finden sind, sowie ihre Kontodaten. P6 hat eine Mischform der Definition, bei der private Daten aus den persönlichen Daten und den verschickten Nachrichten bestehen.

Empfundener Schutz privater Daten

Auch wenn jede der befragten Personen den Schutz ihrer privaten Daten anders umsetzt, was nicht zuletzt auch den individuellen Definitionen privater Daten geschuldet ist, sind sich alle Befragten einig: ihre Daten sind nicht sicher. Eines der bezeichnenden Zitate stammt von P1: "Ich würde behaupten, ich bin eher vorsichtig als *geschützt*". Daneben gibt es jedoch auch deutlich fatalistischere Deutungen dieser Unsicherheit der Daten:

> "All diese Bemühungen sind wahrscheinlich letztendlich ein Kampf gegen Windmühlen. Nachdem sich ein gewisses Bewusstsein [...] bei mir erst nach einigen Jahren der Nutzung gebildet hat, sind bereits genügend Unternehmen/Personen/etc. im Besitz vieler privater Daten meinerseits. Das lässt sich bis zu einem gewissen Grad leider nicht rückgängig machen. Und auch jetzt passieren mir bei Nutzung gewisser Dienste immer noch "Fehler" aus Perspektive des Datenschutzes. Ebenso gibt es viele Widersprüche in dem, was ich möchte und was ich tue. "– P2

Praktischer Schutz der privaten Daten

Die Taktiken zum Schutz der eigenen Daten unterscheiden sich zwischen den Teilnehmer_innen. Alle sechs verwendeten Passwörter, die sie selbst als sicher ansahen. Zusätzlich berichtete P4 seine Passwörter regelmäßig zu ändern und P2 und P4 davon für jede Seite ein anderes Passwort zu benutzen. P2 nutzt einen Passwortmanager, um sehr komplexe Passwörter verwenden zu können. Hierbei sieht er Passwortmanager sowie andere Werkzeuge, die die Privatheit steigern nicht als nachteilslos, sondern denkt, dass für jede verwendete Technologie Vor- und Nachteile gegeneinander abgewogen werden müssen. P1, P3 und P5 geben bei Onlinediensten ihre Klarnamen nicht an. P3 nennt hierzu den Begriff der "Datensparsamkeit", bei der nur die jeweils für den jeweiligen Dienst nötigen Daten ein- und somit preisgegeben werden. Auch P2 macht in einem Zitat deutlich, dass er versucht nach dieser Devise zu handeln: "Ich versuche also immer möglichst bewusst zu entscheiden, wer von mir welche Daten wann und zu welchem Zweck erhält, sei es online oder offline. Das klappt nicht immer, aber allein das aktive darüber Nachdenken hat mich wahrscheinlich vor manch einer Dummheit bewahrt." P6 verwendet als einzige der befragten Personen VPNs, um in öffentlichen Netzwerken die Privatheit ihrer Daten zu wahren. Die anderen befragten Personen sahen keinen Privatheitsgewinn durch die Verwendung von VPNs. Vier der sechs befragten Personen gaben an Browser-Add-Ins zu verwenden: alle zum Blockieren von Trackern, insbesondere Cookies. Diesen Plug-ins wurde keine große Aufmerksamkeit gewidmet, wie folgendes Zitat von P3 zeigt: "Ich glaube irgendwo läuft auch noch ein Trackblocker". Die anderen beiden Personen gaben an Cookies in regelmäßigen Abständen selbst zu löschen. Der Verzicht auf soziale Medien wurde nur von zwei Personen ausgeübt, während alle Personen äußerten, dass sie soziale Medien als Schwachstelle für ihre privaten Daten sähen. Drei Personen äußerten hierbei, dass sie aus Bequemlichkeitsgründen in sozialen Medien oder unsicheren Messengern bleiben, obwohl sie wissen, dass ihre Daten so gefährdet werden. Die Möglichkeit E-Mails zu verschlüsseln, wurde von allen Teilnehmer_innen genannt, jedoch nur von P3 angewandt. Der Inkognito-Modus in Browsern war allen Teilnehmer_innen bekannt und wird von diesen in unterschiedlichem Ausmaß angewandt. Zwei der Personen nutzen vornehmlich Apple-Betriebssysteme, um ihre Daten geschützter zu wissen. P3 verwendet möglichst Linux-Derivate.

Komfort des Datenschutzes

Alle befragten Personen gaben an, dass ein umfassender Schutz ihrer Daten mit Komforteinbußen verbunden wäre, bspw. P3 in folgenden Worten: "Wenn ich meine Daten wirklich konsequent schützen würde, würde es mich einschränken". Ob sich dieser Aufwand lohnt, differierte jedoch zwischen den Teilnehmer_innen. So gab P2 an: "Mag sein, dass sich meine Einstellung dazu irgendwann ändert, aber im Moment bin ich sehr gewillt, zumindest zu versuchen meine privaten Daten weitestgehend zu schützen, auch wenn das mit gewissen Nachteilen und einem gewissen Aufwand verbunden ist". Andere Personen, bspw. P6, gaben an, dass die Nachteile zu sehr überwiegen würden, da ein gelebter Datenschutz "sozial isolierend und unpraktisch" sei. Hiermit ist bspw. der Verzicht auf als nicht sicher empfundene Messengerdienste oder soziale Netzwerke gemeint. Der Verzicht auf diese Dienste und Netzwerke hätte empfunden für manche befragten Personen zur Folge, dass sie nicht mit den dort vertretenen Personen in Kontakt bleiben könnten.

Motivation zum Schutz der privaten Daten

Als Motivation wurden neben Wünschen und Ängsten von zwei Personen der Grund genannt, dass sie aus einer Philosophie (P2) oder ihrer politischen Einstellung (P3) heraus die Motivation finden ihre privaten Daten zu schützen. P3 sah es außerdem als Teil seiner Kompetenz an seine Daten zu schützen, wenn er beruflich als Datenschutzexperte ernstgenommen werden wolle.

Nur eine Person, P2, hegte Wünsche und positive Erwartungen an das Sammeln und Verwenden seiner privaten Daten:

> "Möchte ich, dass andere diese Daten einsehen können[?] Ja und Nein [...] Ein Arzt oder Fitness Trainer kann mir [...] Anpassungen vorschlagen, die mir letztendlich zur Verbesserung dienen können. Meine Krankenversicherung sollte hingegen nicht unbedingt wissen, dass ich gestern fünf Schokoriegel verdrückt habe, weil [...] sich dann womöglich mein Tarif erhöht." – P2

Sorgen und Ängste wurden jedoch von allen Teilnehmer_innen beschrieben: Es konnten zwei unterschiedliche Ängste beobachtet werden. Eine Gruppe der Teilnehmer_innen äußerte die Angst, dass ihre Daten und dadurch auch Teile ihres Eigentums gestohlen werden können. Die Ängste der anderen Gruppen sind auf Benachteiligung durch Organisationen oder Systeme fokussiert. Konkret wurde die Angst vor dem Umgang mit ihren privaten Daten durch Facebook, Google, Krankenkassen, Arbeitgeber, den Staat, die Polizei und weitere genannt. Während die erstgenannte Gruppe Angst vor dem Verlust von Eigentum hat, hat die zweite Gruppe Angst davor, dass ihr Verhalten und das Wissen von Organisationen ihnen in ihrem Leben weniger Chancen offenlässt oder sie offen benachteiligen werden (vgl. auch Zitat P2).

4 DISKUSSION

Die erhobenen Informationen können als Vorbereitung für deskriptive, komparative oder explikative Studien dienen, da sie Anreize bezüglich sowohl praktischem Privatheitsverhalten, als auch Indizien bezüglich des Privatheitsverhaltens von Informatiker_innen liefern.

Diskussion der Resultate

Im Folgenden werden die Forschungsfragen, die zu Beginn gestellt wurden diskutiert. Es ist hierbei zu beachten, dass den Autor_innen bewusst ist, dass die beobachteten Ergebnisse nur Indizien sind und nicht als repräsentativ angesehen werden können.

F1: *Haben Informatikabsolvent_innen eine Sensibilisierung bezüglich ihres Umgangs mit ihren eigenen Privatdaten?* Eine bei Studierenden im Allgemeinen fehlende Sensibilisierung hinsichtlich des eigenen Umgangs mit eigenen privaten Daten – wie bei [3, 4, 11, 16] – konnte bei den befragten Personen nicht festgestellt werden: Allen befragten Informatiker_innen ist gemein, dass diese bewusst mit ihren Daten umgehen und besorgt bezüglich dieser sind. Dieses Bewusstsein scheint auch dazu zu führen, dass alle befragten Personen Maßnahmen ergriffen, um ihre privaten Daten zu schützen. Jedoch handelt es sich nicht um eine gleichförmige Sensibilisierung, da die Definition von "Privatdaten" unterschiedliche Ausprägungen annahm: von Personendaten bis hin zu allen messbaren Daten einer Person.

F2: *Gehen Informatikabsolvent_innen ähnlich mit ihren eigenen Privatdaten um?* Der Umgang der Befragten mit ihren Privatdaten war unterschiedlich. Während manche Personen viel Wert darauf legten, dass ihre Personendaten nicht für andere verfügbar seien, legten andere gerade auf diese Daten keinen Wert. Einzig die Geheimhaltung von Passwörtern und Bankdaten war allen Teilnehmer_innen gemein. Auch die Maßnahmen, die die Personen ergriffen, um ihre privaten Daten zu schützen, waren sehr unterschiedlich. Eine mangelhafte Maßnahmenergreifung beobachteten bereits Bornoe et al. [3], Ball et al. [2], sowie Molluzzo et al. [11]. Es bleibt zu untersuchen, welche Faktoren über die Maßnahmenergreifung entscheiden oder eine Rolle spielen.

F3: *Wie gehen Informatikabsolvent_innen mit ihren Privatdaten um?* Diese Maßnahmen, deren Ausmaß und Menge, unterschieden sich jedoch zu großen Teilen zwischen den befragten Personen – und das bei nur sechs befragten Personen. Auffällig hierbei war, dass alle Teilnehmer_innen Passwörter benutzten, eine Technik, die auch, wie eingangs erwähnt, bei Reuter et al. [14], in einer repräsentativen Studie die am weitesten verbreitete und anerkannte Methode ist, Daten zu schützen. Es ist denkbar, dass es weitere tieferliegende Verhaltensmuster zum Schutz der eigenen Daten – insbesondere auch innerhalb der Gruppe der Informatiker_innen – gibt, die jedoch im Rahmen dieser Studie nicht erfasst werden konnten. Haltinner et al. [7] nannten drei dominante Strategien zum Schutz der eigenen Daten: das zu Rate ziehen von glaubwürdigen Quellen, eine eingeschränkte Informationsweitergabe, sowie eine erlernte Hilflosigkeit. Eine weitere Strategie, die mehrere befragte Personen nannten und die sich nicht explizit in dieser Klassifizierung von Haltinner et al. [7] findet, ist die Vermeidung bestimmter Dienste, Software oder Produkte bestimmter Hersteller oder Konzerne. Während die eingeschränkte Informationsweitergabe von allen befragten Personen in unterschiedlichen Ausprägungen erwähnt wurde, wurde das zu Rate ziehen glaubwürdiger Quellen nur von manchen Personen genannt. Die Personen, die andauernd verschiedene und aktuelle Quellen zu Rate ziehen, um auf dem neuesten Stand hinsichtlich Cybersecurity zu bleiben, waren jedoch nicht zwangsläufig die Personen, die den Eindruck erweckten ihre privaten Daten am wirkungsvollsten zu schützen. Dieses in sich scheinbar

widersprüchliche Verhalten konnten auch bspw. Ball et al. [2] sowie Norberg, Horne et al. [12] beobachten. Haltinner et al. [7] bezeichnen dieses bewusste Ignorieren von Wissen beim eigenen Handeln als Strategie der erlernten Hilflosigkeit. Ein Grund hierfür könnte eine Art Resignation aufgrund der Ausweglosigkeit – keine praktikablen Alternativen zu aktuell benutzten Diensten – oder Bequemlichkeit – Alternativen wären zu aufwendig zu nutzen, hätten spürbare negative Auswirkungen auf die Lebensqualität – sein. Die Gründe für dieses widersprüchliche Verhalten könnten jedoch weiter erforscht werden, um die ausschlaggebenden Gründe für dieses oder die anderen Verhaltensweisen zu finden. Haltinner et al. [7] nennen als ausschlaggebende Gründe Routinen, Ritualisierung von Risiken, eine optimistische Voreingenommenheit sowie die Selbstwirksamkeitserwartung der einzelnen Personen.

Sarathchandra et al. [18] sehen ein Problem darin, dass die Personen sich vor den falschen, da unwahrscheinlichen, Dingen – bspw. Identitätsdiebstahl – fürchten. Es stellt sich die Frage, ob es sich hierbei wirklich um "falsche" Ängste handelt und wenn ja, wie man die "richtigen" Ängste weiter ins Bewusstsein der Menschen bringen könnte. Es ist jedoch möglich, dass nur Gefahren mit gravierenden Folgen so starke Emotionen auslösen, dass sie das tägliche Verhalten einer Person beeinflussen und dass somit die "richtigen" Ängste und somit wahrscheinlichen Risiken nicht genug motivierende Kraft innehaben. Während die Angst vor dem Identitätsdiebstahl von manchen befragten Personen benannt wurde, wurde in der vorliegenden Studie jedoch eine weitere gravierende Angst ausfindig gemacht: die Angst vor Benachteiligung durch passiv erzeugte Daten. Diese zwei Kategorien der Ängste erschienen den Autor_innen äußerst interessant: Es stellt sich die Frage, ob Personen, die eine der beiden Sorgen haben auch die andere wahrnehmen und ihr lediglich weniger Beachtung schenken, oder ob es sich um unterschiedliche Personengruppen mit unterschiedlichen Ängsten handelt. Eine weitere Klassifizierung dieser Ängste und Sorgen erscheint somit sinnvoll.

Limitationen

Die angewandten Methoden, teilstrukturierte Interviews, sind für eine explorative Studie als angemessen zu bewerten, da sie den Proband_innen einen Rahmen Bieten. Die Fragen vereinfachen den Einstieg in ein Gespräch, die Offenheit und Struktur des Interviews erlauben es den Proband_innen aber auch, ihre Gedanken frei zu äußern und auf diese einzugehen. Weitere qualitative Methoden, die ebenfalls einen offenen und einladenden Charakter haben, wie beispielsweise die Fokusgruppe, sind ebenfalls denkbar. Jedoch wäre bei Fokusgruppen zu bedenken, dass die Teilnehmer_innen aus Angst vor der Verurteilung durch die anderen Teilnehmer_innen in ihren Wortbeiträgen nicht ihr tatsächliches Verhalten preisgeben.

Die gewählte Reihenfolge der Fragen schien nicht optimal zu sein. Bei den mündlichen Interviewformen wurde nach dem Beantworten der letzten Frage des ersten Blocks (Definition private Daten) in allen vier Fällen Ergänzungen zu den vorherigen Fragen gemacht wurden. Bei der schriftlichen Bearbeitung dieser Fragen konnte ein solches Verhalten naturgemäß nicht beobachtet werden. Die Frage nach der Definition sollte also bei einer Replikation oder Fortführung dieser Studie an den Anfang gestellt werden oder die zuvor gestellten Fragen nach dieser Frage wiederholt werden.

Zwischen den Antworten der drei Interviewformen – in persona, telefonisch oder im Schriftverkehr – konnten keine Unterschiede festgestellt werden. Die Form beeinflusste weder die Länge noch die Ausführlichkeit der Antworten. Diese Werte unterschieden sich stark und unabhängig von der Interviewform.

Es handelt sich nicht um eine deskriptive Studie, die den Anspruch erhebt allgemeingültige Aussagen aus den erhobenen Daten ableiten zu können Es findet auch keine explikative Auswertung statt, da das Verhalten der Teilnehmer_innen weder bewertet wird, noch versucht wird herauszufinden, wieso ihr Verhalten derart ist. Es handelt sich außerdem um eine Momentaufnahme mit einer sehr kleinen Stichprobe. Wiederholungen der Studie im größeren Rahmen oder in zeitlichen Abständen erscheinen sinnvoll.

5 FAZIT UND AUSBLICK

Bei der Durchführung der qualitativen Studie in Form von teilstrukturierten Interviews mit sechs Informatikabsolvent_innen konnten diverse Eindrücke über das Verhalten von Informatiker_innen hinsichtlich ihres Umgangs mit ihren privaten Daten gewonnen werden. Die anfänglich angenommene Vermutung, dass Informatikabsolvent_innen eine Sensibilität bezüglich ihrer privaten Daten haben, konnte bestätigt werden: Alle befragten Personen hatten eine eigene Definition von privaten Daten und jeder Person war bewusst, dass sie diese Daten nicht leichtfertig angeben oder teilen sollte. Die zum Schutz der privaten Daten verwendeten Techniken und Technologien unterschieden sich ebenfalls zwischen den Teilnehmer_innen und korrelierten nicht zwangsläufig mit dem Detailwissen über die Gefährdung privater Daten. Als tatsächlich angewandte Strategien konnten Informiertbleiben, Datensparsamkeit, Verzicht auf die Produkte bestimmter Konzerne sowie Resignation festgestellt werden. Als angewandte Technologien zum Schutz privater Daten wurden Browser-Add-ons, die Verwendung von VPN-Netzwerken zum Schutz in öffentlichen W-LAN-Netzen, sowie die Verwendung des Inkognitomodus in Browsern genannt. Als Motivatoren zum Schutz der eigenen privaten Daten wurden

sowohl politische wie philosophische Motivationen, aber auch Ängste genannt.

Offen bleiben die Fragen nach der Ursache für die unterschiedlichen (dominanten) Ängste bezüglich des Datenmissbrauchs: Angst vor Diebstahl und Angst vor zukünftiger Benachteiligung. Welche Ängste in welcher Ausprägung bei welcher Person zu welchem Verhalten führen, blieb offen. Auch, ob die selbst wahrgenommene Kompetenz hinsichtlich des Schutzes der privaten Daten zutrifft, wird in dieser Studie nicht untersucht. Interessant wäre es auch diese Studie mit einer anderen Informatiker_innen-Vergleichsgruppe durchzuführen (bspw. Menschen, deren Abschluss über 10 Jahre zurückliegt, Fachinformatiker_innen, andere Studierende, etc.).

6 DANKSAGUNG

Diese Arbeit wurde gefördert durch das Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit sowie durch die Deutsche Forschungsgemeinschaft DFG innerhalb des SFB 1119 CROSSING. Wir möchten uns herzlich für die Zeit und Mühen der Teilnehmer_innen und Gutachter_innen bedanken. Ein besonderer Dank gilt auch Herrn Felix Kalley, der durch sein Fachwissen und seine Kommunikationsbereitschaft half die Basis dieses Papers zu gestalten sowie der Fachschaft Informatik der TU Darmstadt für die Vermittlung eines Studierenden.

LITERATUR

[1] Larissa Aldehoff, Meri Dankenbring, and Christian Reuter. 2019. Renouncing Privacy in Crisis Management? People's View on Social Media Monitoring and Surveillance. In *Proceedings of the Information Systems for Crisis Response and Management (ISCRAM)*, José H. Canós Zeno Franco, José J. González (Ed.). València, Spain.

[2] Albert L Ball, Michelle M Ramim, and Yair Levy. 2015. Examining users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems. *Online Journal of Applied Knowledge Management* 3, 1 (2015), 180–207.

[3] Nis Bornoe and Louise Barkhuus. 2011. Privacy management in a connected world: Students' perception of Facebook privacy settings. In *ACM conference on Computer Supported Cooperative Work*. 19–23.

[4] Chiara Braghin and Marilisa Del Vecchio. 2017. Is Pokémon GO watching you? A survey on the Privacy-awareness of Location-based Apps' users. In *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 2. IEEE, 164–169.

[5] Ian Goldberg, David Wagner, and Eric Brewer. 1997. Privacy-enhancing technologies for the Internet. In *Proceedings IEEE COMPCON 97. Digest of Papers*. IEEE, 103–109.

[6] Onur Hakbilen, Piraveen Perinparajan, Michael Eikeland, and Nils Ulltveit-Moe. 2018. Presenting a Convenient, Portable and Secure Password Manager. (2018).

[7] Kristin Haltinner, Dilshani Sarathchandra, and Nicole Lichtenberg. 2015. Can I Live? College Student Perceptions of Risks, Security, and Privacy in Online Spaces. In *Cyber Security Symposium*. Springer, 69–81.

[8] Michael Hatscher, Sebastian Schnorf, Martin Ortlieb, and Kalle Kormann-Philipson. 2012. Privacy UX – Was ist datenschutzbezogene User Experience?. In *Tagungsband UP12*, Henning Brau, Andreas Lehmann, Kostanija Petrovic, and Matthias C. Schroeder (Eds.). German UPA e.V., Stuttgart, 258–263.

[9] Franziska Hertlein, Tim Schneidermeier, and Christian Wolff. 2014. Praktisch oder innovativ – effizient oder neuartig? Welches Betriebssystem passt zu Ihnen?. In *UP14 - Vorträge*. German UPA, Stuttgart.

[10] James P Lawler and John C Molluzzo. 2011. A survey of first-year college student perceptions of privacy in social networking. *Journal of Computing Sciences in Colleges* 26, 3 (2011), 36–41.

[11] John C Molluzzo, James Lawler, and Vijal Doshi. 2012. An expanded study of net generation perceptions on privacy and security on social networking sites (SNS). *Information Systems Education Journal* 10, 1 (2012), 21.

[12] Patricia A Norberg, Daniel R Horne, and David A Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs* 41, 1 (2007), 100–126.

[13] Christian Reuter (Ed.). 2018. *Sicherheitskritische Mensch-Computer-Interaktion - Interaktive Technologien und Soziale Medien im Krisen- und Sicherheitsmanagement*. Springer Vieweg, Wiesbaden.

[14] Christian Reuter, Katja Häusser, Mona Bien, and Franziska Herbert. 2019. Between Effort and Security: User Assessment of the Adequacy of Security Mechanisms for App Categories. In *Mensch und Computer 2019*. Hamburg, Germany.

[15] Christian Reuter, Marc-André Kaufhold, and Jonas Klös. 2017. Benutzbare Sicherheit: Usability, Safety und Security bei Passwörtern. In *Mensch und Computer 2017 - Workshopband*, Manuel Burghardt, Raphael Wimmer, Christian Wolff, and Christa Womser-Hacker (Eds.). Gesellschaft für Informatik e.V., Regensburg.

[16] Mark Rowan and Josh Dehlinger. 2014. Privacy incongruity: An analysis of a survey of mobile end-users. In *Proceedings of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science, Computer …, 1.

[17] Scott Ruoti, Jeff Andersen, Daniel Zappala, and Kent Seamons. 2015. Why Johnny still, still can't encrypt: Evaluating the usability of a modern PGP client. *arXiv preprint arXiv:1510.08555* (2015).

[18] Dilshani Sarathchandra, Kristin Haltinner, and Nicole Lichtenberg. 2016. College Students' Cybersecurity Risk Perceptions, Awareness, and Practices. In *2016 Cybersecurity Symposium (CYBERSEC)*. IEEE, 68–73.

[19] Hartmut Schmitt and Edna Kropp. 2017. Benutzerfreundliche IT-Sicherheit: Prozessintegration und Werkzeuge (UPA-Arbeitskreis Usable Security & Privacy). In *Mensch und Computer 2017 - Usability Professionals*, Steffen Hess and Holger Fischer (Eds.). Gesellschaft für Informatik e.V., Regensburg.

[20] Hartmut Schmitt, Luigi Lo Iacono, and Sascha Wagner. 2016. Workshop des Arbeitskreises „Usable Security & Privacy" – Ziele, Themen, Ausblick. In *UP 2016*, Stefan Hess and Holger Fischer (Eds.). Gesellschaft für Informatik e.V. und die German UPA e.V, Aachen.

[21] Steve Sheng, Levi Broderick, Colleen Alison Koranda, and Jeremy J Hyland. 2006. Why johnny still can't encrypt: evaluating the usability of email encryption software. In *Symposium On Usable Privacy and Security*. 3–4.

[22] Seungwon Shin, Yongjoo Song, Taekyung Lee, Sangho Lee, Jaewoong Chung, Phillip Porras, Vinod Yegneswaran, Jiseong Noh, and Brent Byunghoon Kang. 2014. Rosemary: A robust, secure, and high-performance network operating system. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*.

ACM, 78–89.

[23] Blase Ur, Jonathan Bees, Sean M Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Do Users' Perceptions of Password Security Match Reality?. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 3748–3760.

[24] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2015. Ï Added'!'at the End to Make It Secure": Observing Password Creation in the Lab. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*. 123–140.

[25] Alma Whitten and J Doug Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.. In *USENIX Security Symposium*, Vol. 348.

[26] Fang Yang and Shudong Wang. 2014. Students' Perception toward Personal Information and Privacy Disclosure in E-Learning. *Turkish Online Journal of Educational Technology-TOJET* 13, 1 (2014), 207–216.