

Abschlussbericht

Graduiertenkolleg



Privacy and Trust
for Mobile Users

Öffentlicher Teil

Sprecherhochschule
Technische Universität Darmstadt

Sprecher
Prof. Dr. Max Mühlhäuser

Förderzeitraum
01.10.2015 – 30.09.2024



TECHNISCHE
UNIVERSITÄT
DARMSTADT

U N I K A S S E L
V E R S I T Ä T

GOETHE 
UNIVERSITÄT
FRANKFURT AM MAIN

Inhaltsverzeichnis

1. Allgemeine Angaben	1
1.1. Allgemeine Informationen	1
1.2. Beteiligte (antragstellende) Wissenschaftlerinnen und Wissenschaftler (blau: nur eine Phase)	1
1.3. Zahl der Doktorandinnen und Doktoranden, Postdocs sowie studentischen Hilfskräfte	2
2. Zusammenfassung	2
3. Wissenschaftlicher Arbeits- und Ergebnisbericht	3
3.1. Ausgangsfragen und Zielsetzung des Graduiertenkollegs	3
3.2. Beschreibung der projektspezifischen Ergebnisse und Erkenntnisse der neunjährigen Förderperiode	4
3.2.1. Forschungsbereich A	4
3.2.2. Forschungsbereich B	5
3.2.3. Forschungsbereich C	6
3.2.4. Forschungsbereich D	6
3.2.5. Qualitätssicherung, Forschungsdaten-Handhabung, Kommunikation	7
4. Bilanz zu Qualifizierung, Betreuung und Kooperationen des Kollegs	9
5. Projektergebnisse	11
5.1. Projektergebnisse der Doktorandinnen und Doktoranden sowie ggf. der Postdotorandinnen und Postdoktoranden	11
5.1.1. Projektergebnisse der Doktorandinnen und Doktoranden sowie ggf. der Postdotorandinnen und Postdoktoranden (finanziert aus Mitteln des Graduiertenkollegs)	11
5.1.2. Projektergebnisse der Doktorandinnen und Doktoranden sowie ggf. der Postdotorandinnen und Postdoktoranden (anderweitig finanziert)	30
5.2. Projektergebnisse des Graduiertenkollegs	53
6. Weitere Informationen	

Der nichtöffentliche Teil des Berichts (Seiten 56-278) ist hier nicht enthalten

1. Allgemeine Angaben

1.1. Allgemeine Informationen

DFG-Geschäftszeichen: GRK 2050/2

Projektnummer: 251805230

Titel des Graduiertenkollegs in deutscher und englischer Sprache:

Privatheit und Vertrauen für mobile Nutzende (Englisch: Privacy and Trust for Mobile Users)

Namen der das Graduiertenkolleg tragenden Hochschulen:

Technische Universität Darmstadt (TUDA)

Universität Kassel (UKS)

Goethe-Universität Frankfurt (GU)

Sprecher: Prof. Dr. Max Mühlhäuser

Dienstanschrift:

Technische Universität Darmstadt

Fachbereich Informatik

Hochschulstr. 10

64289 Darmstadt

Berichtszeitraum: 01.10.2015 – 30.09.2024

1.2. Beteiligte (antragstellende) Wissenschaftlerinnen und Wissenschaftler (blau: nur eine Phase)

Name, Vorname, akademischer Titel	Zeitraum der Beteiligung	Fachgebiet
Buxmann, Peter, Prof. Dr.	01.10.2015 – 30.09.2024	Wirtschaftswissenschaften
Fischlin, Marc, Prof. Dr.	01.10.2015 – 30.09.2024	Informatik
Hinz, Oliver, Prof. Dr.	01.10.2015 – 30.09.2024	Wirtschaftswissenschaften
Hollick, Matthias, Prof. Dr.	01.10.2015 – 30.09.2024	Informatik
Hornung, Gerrit, Prof. Dr.	01.04.2020 – 30.09.2024	Rechtswissenschaften
Katzenbeisser, Stefan, Prof. Dr.	01.10.2015 – 31.03.2020	Informatik
Lamla, Jörn, Prof. Dr.	01.10.2015 – 30.09.2024	Soziologie
Mühlhäuser, Max, Prof. Dr.	01.10.2015 – 30.09.2024	Informatik
Pieschl, Stephanie, Prof. Dr.	01.04.2020 – 30.09.2024	Psychologie
Reuter, Christian, Prof. Dr. Dr.	01.04.2020 – 30.09.2024	Informatik (Usability)
Roßnagel, Alexander, Prof. Dr.	01.10.2015 – 31.03.2020	Rechtswissenschaften
Schneider, Thomas, Prof. Dr.	01.04.2020 – 30.09.2024	Informatik
Spiecker gen. Döhmman, Indra, Prof. Dr.	01.04.2020 – 30.09.2024	Rechtswissenschaften
Vogt, Joachim, Prof. Dr.	01.10.2015 – 30.09.2024	Psychologie (Usability)
Volkamer, Melanie, Prof. Dr.	01.10.2015 – 31.03.2020	Informatik (Usability)
Waidner, Michael, Prof. Dr.	01.10.2015 – 30.09.2024	Informatik

Weitere beteiligte Wissenschaftlerinnen und Wissenschaftler (*: zuvor als Postdoc beteiligt)

Name, Vorname, akademischer Titel	Zeitraum der Beteiligung	Fachgebiet
* Bretthauer, Sebastian, Dr.	01.05.2022 – 30.09.2024	Rechtswissenschaften
* Daubert, Jörg, Prof. Dr.	01.01.2019 – 31.03.2022	Informatik
* Geminn Christian, Priv.-Doz. Dr. habil.	01.09.2023 – 30.09.2024	Rechtswissenschaften
* Gerber, Nina, Dr.	01.04.2022 – 30.09.2024	Psychologie
* Hauke, Sascha, Prof. Dr.	01.04.2017 – 31.03.2024	Informatik
* Heimbach, Irina, Jun. Prof. Dr.	01.09.2017 – 31.08.2021	Wirtschaftswissenschaften

* Jandt, Silke, Dr. habil.	01.04.2016 – 31.03.2022	Rechtswissenschaften
Katzenbeisser, Stefan, Prof. Dr.	01.04.2020 – 30.09.2024	Informatik
Kersting, Kristian, Prof. Dr.	01.04.2020 – 30.09.2024	Informatik
* Kulyk, Oksana, Ass. Prof. Dr.	01.04.2018 – 30.09.2024	Informatik
* Marky, Karola, Prof. Dr.	01.04.2021 – 30.09.2024	Informatik
* Ochs, Carsten, PD Dr. habil.	01.03.2022 – 30.09.2024	Soziologie
* Schulmann, Haya, Prof. Dr.	01.04.2020 – 30.09.2024	Informatik
* Vasilomanolakis, Emmanouil, Ass. Prof. Dr.	01.02.2019 – 30.09.2022	Informatik
* Widjaja, Thomas, Prof. Dr.	01.09.2020 – 30.04.2023	Wirtschaftswissenschaften
* Zimmermann, Verena, Ass. Prof. Dr.	01.08.2022 – 30.09.2024	Psychologie

1.3. Zahl der Doktorandinnen und Doktoranden, Postdocs sowie studentischen Hilfskräfte

aus Mitteln des Graduiertenkollegs finanzierte Personen	Anzahl
Promovierende, [Stipendium oder Stellen mit 100 % Umfang]	46
Postdoktorandinnen und Postdoktoranden	4
studentische Hilfskräfte	98
anderweitig finanzierte Personen	
Promovierende	16
Postdoktorandinnen und Postdoktoranden	23

2. Zusammenfassung

Privatheit und Vertrauen sind seit Jahrhunderten essenziell für jedes soziale Gefüge und deshalb Forschungsobjekt dreier Disziplinen: der Sozial-, Wirtschafts- und Rechtswissenschaften. Milliarden von Menschen nehmen aber inzwischen vermehrt über Smartphones und Internet an der Gesellschaft teil. Neue Fragen von *Privatheit und Vertrauen* bei dieser *mobilen digitalen* Teilhabe standen im Fokus des hier berichteten Graduiertenkollegs (GRK). Folglich war die Informatik als vierte Disziplin überproportional vertreten sowie als Fünftes die *Usability*-Forschung für die Mensch-Technik-Schnittstelle.

Um die Kooperation im GRK zu maximieren, wurde es nicht nach beteiligten Disziplinen gegliedert oder nach den Kernthemen (*Privatheit, Vertrauen*), sondern nach den vier relevanten Anwendungsdomänen. Dies bewährte sich und wurde für Phase II nur zeitgemäß angepasst an Aspekte, deren Brisanz Phase I aufgedeckt hatte. Bereich A bearbeitete weiterhin *digitale Dienste allgemein*, dabei aber neue Fragen der *Internetökonomie* bzgl. Cybersicherheit, zunehmender KI und (EU-)verfahrensrechtlicher Aspekte. Bereich B untersuchte weiterhin *soziale Netze*, darin aber speziell sog. *digitale Kollektive*, digitales Sozialkapital und Datenschutz-Zielkonflikte. Bereich C beforschte weiterhin die Unterstützung Nutzender in *Sensor-gestützten Umgebungen*, nahm aber kommerzielle „Ökosysteme“ des *Internet-der-Dinge*, neue Rechtsfragen sowie innovative Lernsettings ins Visier. Bereich D verfolgte weiter die Rolle von Endgeräten als digitale Stellvertreter der Nutzenden (*ALTEREGO* genannt) gegenüber „dem Netz“, nun aber v. a. für *kooperierende Komponenten* – im Endgerät, lokalen Netz und Internet. Wichtiges übergreifendes Forschungsthema in Phase II waren sog. *Intermediäre*, die zwischen Nutzende und die „Akteure im Netz“ treten, um die Vertrauenswürdigkeit dieser zu bewerten und die *Privatheit* jener zu schützen. Angesichts zahlreicher grundlegender Alternativen für *Intermediäre* (über Experten oder als KI-Agenten? mit staatlichen, gemeinnützigen oder kommerziellen Trägern? usw.) und des neuen Problems ihrer eigenen *Vertrauenswürdigkeit* konnte das GRK hier erste Schritte gehen als Wegbereiter eines hochspannenden Forschungsfelds.

Die Corona-gestählte exzellente Zusammenarbeit über drei Standorte hinweg – belegt u.a. durch erstklassige Publikationen –, tiefgehende Wirkung in die beteiligten Disziplinen hinein, gut funktionierende Betreuungs-Tandems, Einbeziehung vieler ausgezeichneten junger Forscher auf allen (EU-)Niveaus R1–R4, enge Interaktion mit Verbünden vor Ort sowie ein individuell zugeschnittenes Qualifizierungskonzept machten das GRK 2050 zu einer Erfolgsgeschichte.

Abstract

Privacy and trust have been essential to every social construct for centuries and are hence the subject of research in three disciplines: social sciences, economics, and law. However, billions of people participate now in society increasingly via smartphones and the Internet. New questions of *privacy and trust* in this *mobile digital* participatory experience constituted the focus of the Research Training Group (RTG) reported here; as a result, *computer science* was over-proportionally represented as the fourth discipline, and fifthly, *usability* research focused on the human-technology interaction.

To maximize cooperation within the RTG, it was not divided according to the disciplines involved or the core topics (privacy, trust), but rather into four relevant application domains. This proved successful and was only adapted for Phase II to reflect aspects whose pressing nature Phase I had uncovered. Area A continued to deal with *digital services in general* but addressed new questions of the *Internet economy* concerning cyber security, the rise of AI, and (EU) procedural law. Area B continued to investigate *social networks* but emphasized so-called *digital collectives*, digital social capital, and goal conflicts of data protection. Area C continued to research user support in *sensor-equipped environments* but focused on commercial “ecosystems” of the *Internet of Things*, new legal issues, and innovative learning settings. Area D continued to pursue the role of end devices as digital representatives of users (called ALTEREGO) vis-à-vis “the Net”, but now primarily for cooperating components—in the end device, local network, and Internet. An important overarching research topic of Phase II was so-called intermediaries, who intervene between users and the “actors in the network” to assess the latter’s trustworthiness and protect the former’s privacy. In view of numerous fundamental alternatives for intermediaries (via experts or as AI agents? with state, non-profit, or commercial providers? etc.) and the new problem of their own trustworthiness, the RTG was able to take the first steps here as a pioneer in a large and exciting new field of research.

The “Corona-hardened” excellent collaboration across three locations—evidenced, among other things, by first-class publications—, the profound impact on the participating disciplines, well-functioning mentoring tandems, involvement of many excellent young scientists at all (EU) levels R1—R4, close interaction with collaborative research centers on-site, and an individually tailored qualification concept made the RTG 2050 a success story.

3. Wissenschaftlicher Arbeits- und Ergebnisbericht

3.1. Ausgangsfragen und Zielsetzung des Graduiertenkollegs

Genesis. Die Konzeption des GRK fußte auf folgenden Erkenntnissen aus jahrelanger Vorlaufforschung: (i) Während Milliarden von Weltbürgern über Smartphones umfangreich an der digitalen Gesellschaft teilhaben, bleiben essenzielle Fragen ihres *Privatheitsschutzes* ungelöst. (ii) *Vertrauen* ist Voraussetzung und Triebfeder sozialer und ökonomischer Interaktion und vielfältig mit *Privatheit* verflochten, wird aber noch nicht adäquat für die digitale Welt verstanden und unterstützt; (iii) Die traditionell mit *Vertrauen* und *Privatheit* befassten Disziplinen haben zwar die digitale Gesellschaft als Forschungsthema für sich „entdeckt“, aber in enger Verflechtung mit Informatik- und Usability-Forschung sind erheblich weitreichendere Ergebnisse zu erwarten, weil rasante technische und sozial-ökonomisch-rechtliche Fortschritte eng ineinandergreifen sollten.

Ziel. So entstand das Ziel des GRK: Steuerung und Schutz von *Privatheit* (1) eng verflochten mit der Bewertung von *Vertrauenswürdigkeit* (kurz: *Privatheit* und *Vertrauen*, **P+T**) und (2) als *fünfdisziplinär* eng kooperierendes Forschen, wobei empirisch-deskriptive („Was ist?“) und empirisch-konstruktive Methoden („Was ist (neu) möglich?“) sich befruchten sollten. Das Desiderat enger Verflechtung in (1) und (2) verbot eine Strukturierung des GRK nach diesen Dimensionen. Gegliedert wurde stattdessen in die Anwendungsdomänen *Digitale Dienste allgemein* (A), *Soziale Netze* (B), *Sensor-gestützte Umgebungen* (C) sowie die *Ertüchtigung mobiler Endgeräte als ALTER EGO* (D). Letzteres adressiert das Machtgefälle zwischen Dienst-/Plattform-Anbietern und Endnutzenden, das die P+T-Interessen der Nutzenden in (vernetzten) Endgeräten diskriminiert; künftig

sollen Endgeräte als ALTER EGO die Nutzenden besser in der digitalen Welt repräsentieren, indem sie Privatheit individuell schützen und die Vertrauenswürdigkeit der „Gegenüber im Netz“ (Dienste, Plattformen, Sozialkontakte ...) bewerten.

Fragestellungen. Ausgehend von den grundlegenden Zielen wurden interdisziplinär befruchtete Forschungsfragen verfolgt. Bspw. war es immer wieder spannend, wo und wie P+T jenseits der technischen Grenzen durch geeignete rechtliche Setzungen unterstützt werden kann, wie rechtliche Vorgaben (bspw. *informed consent*) durch Usability- und technische Mittel besser durchgesetzt werden können, wie Privatheit-schützende Dienste durch neue Geschäftsmodelle gefördert werden können, welche sozio-technischen Prozesse ein besseres ALTER EGO befördern können usw.

Standortübergreifende Betreuung und Qualifizierung, Corona. Die in Darmstadt vorhandene Informatik- und Usability-Expertise war aufgrund der dortigen Schwerpunkte exzellent, für die drei anderen Disziplinen wurde in Kassel und (nach personellen Wechseln, in Phase II) in Frankfurt erstklassige Verstärkung gefunden. Die Vorerfahrungen aus anderen GRKs bzgl. Betreuung und Qualifikation (bei verteilten Standorten und Interdisziplinarität) wurden deutlich weiterentwickelt (s. Kap. 4). Die Corona-Pandemie hatte erhebliche Auswirkungen und verzögerte viele Arbeiten, wurde aber auch genutzt, um die *hybride* Betreuung und Qualifizierung weiterzuentwickeln, was sich bis zum GRK-Ende äußerst förderlich auswirkte.

Weitere Entwicklungen. Wesentliches aus Phase I wie die GRK-Ziele und Anwendungsdomänen erwiesen sich als so zielführend und erfolgreich, dass sie in Phase II weiterverfolgt wurden (was Kontinuität sicherte). Dabei wurden die Bereiche A—D auf Fragestellungen zugespitzt, die sich in Phase I als besonders bedeutend erwiesen hatten. Bspw. wurde die wachsende Bedeutung von KI in der Forschung zu Vertrauen (ökonomisch zentriert in A) und Privatheit reflektiert (Technik-zentriert in A u. B). Neu hinzugekommene Mit-Antragstellende konnten Settings betrachten, in denen die GRK-Ziele P+T mit anderen Zielen im Konflikt stehen, bspw. in Katastrophenfällen (A) oder in Lernsettings (C). In der Soziale-Netze-Forschung wurden u. a. die zunehmend relevanten Phänomene digitaler Kollektive und digitalen Sozialkapitals erforscht. Technische Entwicklungen, bspw. bessere sichere Mehrparteienberechnungen, hatten ebenso starken Einfluss auf die GRK-Agenda wie rechtliche Neuerungen, bspw. die Datenschutz-Grundverordnung mit ihren negativen Seiteneffekten wie einer kaum bewältigbaren Anzahl an „Cookie-Bannern“ für Nutzende. Letzteres beflügelte in Phase II das Vorhaben, Ansätze für Intermediäre mit-zu-betrachten, welche für die Nutzenden deren P+T-Ziele durchsetzen (bspw. als *Privacy Buddy* in Bereich D).

GRK-Fazit. Beim GRK-Abschluss-symposium in Brüssel würdigten Teilnehmende aus Politik, Wirtschaft, Forschung und Gesellschaft die erzielten Ergebnisse als herausragend. Mehrere Teilprojekte stehen in engem Bezug zu aufziehenden Bedrohungen der KI, andere, insb. zu Intermediären, stießen die Tür zu einem neuen Forschungsfeld auf. Anschlussforschung ist daher dringend geboten. Hinsichtlich Praxisrelevanz erfreute bspw. die industrielle Nutzung von GRK-Ergebnissen bei einem führenden Hersteller der deutschen Automobilindustrie. Nicht zuletzt zeigen die Karriereerfolge der GRK-Alumni, dass der Geist des *Formats Graduiertenkolleg* sehr ernst genommen und mit großem Erfolg gelebt wurde.

3.2. Beschreibung der projektspezifischen Ergebnisse und Erkenntnisse der neunjährigen Förderperiode

Hinweise: (1) Über die Sicherstellung von Validität und Nachvollziehbarkeit, die Forschungsdaten-Handhabung sowie Veranstaltungen und Wissenschaftskommunikation berichtet zusammenfassend Abschnitt 3.2.5. (2) Aus Platzgründen werden in Kapitel 3 nur die in Abschnitt 5.2 aufgeführten 20 repräsentativen Publikation zitiert, für die vollständige Liste sei auf 5.1 verwiesen.

3.2.1. Forschungsbereich A

Ausgangspunkt, Ergebnisse u. Erkenntnisse. Das GRK-Thema wurde in Bereich A für Digitale Dienste allgemein beforscht, in Phase II auf Internet-Ökonomie konzentriert. A.1 nahm in Phase I zunächst eine quantitative Bewertung der Privatheit verschiedener Dienste vor (Crowdsourcing, Smart Meters, Online-Kaufempfehlungen) zur Unterstützung datenschutzbewusster Entscheidungen der Nutzenden. Dann wurden Ansätze für Privatheitsschutz bei der Systementwicklung erarbeitet [T1]. In Phase II wurden sichere Maschinelle Lernverfahren und große Datenmengen fokussiert (mit beteiligtem Wissenschaftler Prof. Kersting). U. a. gelang es, Summen-Produkt-Netzwerke sicher auszuwerten und erhebliche Effizienzgewinne zu erzielen

[T2] sowie Schwachstellen verwandter Arbeiten nachzuweisen. Mit einem Datenbankhersteller wurden Sicherheitsgarantien für durchsuchbare Verschlüsselung analysiert. Mit A.4 und der Polizei Hamburg wurde gezeigt, dass ein im GRK entwickeltes Verfahren erstmals rechtssicher Datenfusion über Strafverfolgungsbehörden hinweg ermöglicht [T3].

A.2 wurde in Phase II nach D.5 überführt und wird in 3.2.4 reflektiert. **A.3** entwickelte Geschäftsmodelle, die Privatheitsschutz für Nutzende mit Wirtschaftlichkeit für Anbieter in Einklang bringen. Anschlussarbeiten erforschten Aspekte wie bspw. akzeptable Preise für Daten-(Foto-)Überlassung, Details zugehöriger Treiber und Hemmnisse sowie geeignete Strategien für Unternehmen, die ökonomischen Nutzen und Privatheitsschutz kombinieren wollen [T4]. Phase II adressierte den wachsenden KI-Einsatz und als Konsequenz stärker den *Vertrauens*-Aspekt. Als Einsatzfelder wurden zunächst *Autonomes Fahren* und *Medizin* untersucht, danach in konstruktiv-empirischen Arbeiten wieder der Unternehmens-Kontext: Messenger-Dienst Discord wurde mit ChatGPT erweitert, Auswirkungen auf Vertrauen wurden untersucht und neue Ansätze für *Unternehmenskommunikation unter Einbeziehung von KI-Agenten* entwickelt.

A4 untersuchte das Zusammenspiel materieller datenschutzrechtlicher Normen und ihrer prozeduralen Absicherungen, speziell in der DSGVO. Ein Fokus lag auf kommerziellem Profiling und gesellschaftlich marginalisierten Gruppen, mündend in einen innovativen verfahrensbasierten Vorschlag [T5]. Da materielle Beweisvorschriften der Prozessordnungen (v. a. digital) durch strenge Verfahrensvorschriften flankiert werden, wurde an technischen Hilfsmitteln geforscht, zusammen mit C.1 umgesetzt als sog. *Online Evidence Collector*. Auch gesetzlich institutionalisierte Verfahrensabsicherung wurde als Brücke zwischen materiellen und technisch-prozeduralen Anforderungen untersucht. Mit A.1 wurden Möglichkeiten der Erfüllung verfahrensrechtlicher Hürden zur Absicherung materieller datenschutzrechtlicher Erlaubnisse mittels Verschlüsselungstechnik untersucht und wie erwähnt die Praktikabilität des überlegenen Ansatzes aus A.1 gezeigt [T3].

Entwicklung des Forschungsplans. Bereich A erreichte alle wissenschaftlichen und Promovierenden-Förderziele, Corona-Verzögerungen waren teils erheblich, aber im Ergebnis unschädlich, ebenso Elternzeiten. Anpassungen betrafen den „Umzug“ von Usabiliy (A.2 → D.5, siehe dort), Hinzunahme der neuen Frankfurter Rechts-Expertise (A.4) und den Fortschritt in Recht und Informatik (EU-DSGVO, Privatsphäre schützendes maschinelles Lernen, sichere Mehrparteienverarbeitung).

3.2.2. Forschungsbereich B

Ausgangspunkt, Ergebnisse u. Erkenntnisse. Forschungsbereich B konzentrierte sich auf soziale Netze (engl. Online Social Networks, OSNs); deren Prozesse sind (oft unbewusst) stark vom *Vertrauen* in Plattformanbieter und Nutzende geprägt, zumal angesichts von Manipulationen, Fehl- und Desinformation. Phase II nahm kohärente Gruppen in OSNs ins Visier, sog. Kollektive. **B.1** erforschte soziotechnische Vertrauensinfrastrukturen, die der Gewährleistung von Privatheit durch Intermediäre dienen, sowie Praktiken und Prozesse der digitalen Infrastrukturierung von Vertrauen, etwa durch Plattformunternehmen. Soziologie-typisch sind als Ausflüsse v. a. die Dissertationen hervorzuheben, darauf wird weiter unten eingegangen. Förderlich waren v. a.: mehrfacher internationaler Forschungsaufenthalt, u. a. am *Surveillance Studies Centre* in Kingston, Kanada, sowie enge Kooperation mit Gastwissenschaftlern wie Paula Helm von der University of Amsterdam.

B.2 beforschte Privatheitsschutz für Kollektive und entwickelte Beiträge zu anonymer Gruppenkommunikation, die für geschützten Austausch sensibler Daten bzw. Meinungen unerlässlich ist. Die Ansätze betrafen u. a. effiziente dezentrale Gruppenkommunikation, Resilienz bei Nutzerfluktuation, Senderanonymität sowie Privatheitsschutz durch geschützte Seitenkanäle (als Erweiterung populärer, nicht vertrauenswürdiger OSNs). In Phase II gelang innovativer Privatsphärenschutz von Kollektiven, die Mehrwert durch kollektives maschinelles Lernen generieren wollen. Abhilfen gegen identifizierte Schwachstellen bekannter Federated-Learning-Ansätze wurden vorgeschlagen [T6]. Zuletzt kooperierte B.2 eng mit D.5.

B.3 beforschte erfolgreich *Vertrauen und soziales Kapital* in OSNs, insb. Konstitution, Mechanismen und Quantifizierung. In jüngerer Zeit wurde dabei *Algorithmische Rekursivität* ins Visier genommen mit ihrem Diskriminierungspotenzial. Fachartikel wurden in renommierten Fachzeitschriften wie *MIS Quarterly*, *Schmalenbach Journal of Business Research* und *Electronic Markets* [T7] veröffentlicht, auch im *Journal of the Association of Information Systems* sowie zahlreichen Konferenzbänden.

B.4 untersuchte Privatheitsschutz und Vertrauen in digitalen Kollektiven im Spannungsfeld von Zielkonflikten, insb. der Notfall- und Krisenbewältigung. Geforscht wurde zum Nutzerverhalten bei Fluchtbewegungen [T8], zu Contact-Tracing-Apps in der Pandemie, zur Messung von Privacy-Wissen und -Verhalten (mit methodischem Beitrag zur Fragebogenentwicklung) u. v. m. Die entstandenen Arbeiten konnten in den Proceedings hochrenommierter Konferenzen und in angesehenen Fachzeitschriften veröffentlicht werden. Zusätzlich entstand ein Buchkapitelbeitrag zum im GRK-Umfeld entstandenen Buch *Human Factors in Privacy Research* [T9].

Entwicklung des Forschungsplans. Die Forschung wurde wie oben angeführt an aufkommende Problemstellungen wie bspw. *Kollektive* angepasst. Die starken Pandemie-Folgen wurden ohne langfristige Schäden gemeistert.

3.2.3. Forschungsbereich C

Ausgangspunkt, Ergebnisse und Erkenntnisse. Forschungsbereich C erforschte Privatheit und Vertrauen für zwei Arten sensorgestützter Netze: Mensch-nahe (z.B. Sensorik aus Smartphones und Wearables) und Mensch-ferne Varianten („intelligente“ Räume, Städte und Infrastrukturen). Phase II blickte verstärkt auf das Internet-of-Things (IoT), wo passive Sensorik über digitale „Aktorik“ rückwirkt. **C.1** beforschte Mensch-nahe Netze mit technischem Schwerpunkt. Neue Erkenntnisse betrafen Vertrauens-Themen wie das Geräte-„Pairing“ ebenso wie Privatheitsrisiken. Die gewonnene Expertise wurde in ein GRK-Projekt namens *PrivacyScore* zu Webseiten-Privatheitstransparenz eingebracht, das mit C.2, A.3 und D.5 sowie der Uni Bamberg eine der mustergültigen interdisziplinären Kooperationen darstellt. In erstklassigen Fachzeitschriften wurden neue Mechanismen zur Wahrung von Sicherheit und Privatheit in IoT-Systemen publiziert sowie Sicherheits- und Privatheitsanalysen von IoT-Ökosystemen (Geräte-Dienste-Verbünde mit Hersteller-Dominanz). In Phase II wurden diese Arbeiten weiterentwickelt bzgl. der Angreifbarkeit von Nutzenden und Unbeteiligten durch Wearables [T10].

C.2 thematisierte v. a. Mensch-ferne Sensorik; eine wichtige GRK-relevante Besonderheit liegt darin, dass diese ggf. erst auf den zweiten Blick bzw. mit ausgefeilter Algorithmik personenbezogene Daten „erzeugt“; dies erfasst der Europäische Rechtsrahmen noch kaum, was juristische Fragen aufwirft. Durchgeführte vergleichende Analysen des europäischen mit dem japanischen Recht erwiesen sich als sehr fruchtbar, hieraus wurden Vorschläge v. a. über rechtliche Vorsorgemaßnahmen zur Vermeidung von Re-Identifizierbarkeit erarbeitet. Für Phase II hatte sich das Problem des *information overload* für Nutzende – auch angesichts stark zunehmender Verbreitung von Sensorik – als besonders drängend erwiesen. Deshalb wurde hierfür das Konzept eines verbindlichen standardisierten *Data Protection Information Document* erarbeitet, das EU-weit vorgeschrieben werden könnte. Die für den C-Bereich übergreifenden Fragen rechtskonformer Gestaltung cyber-physischer Systeme wurden ebenfalls adressiert [T11], hierfür wurden rechtliche Vorgaben erarbeitet, die sich im ersten Schritt im betrieblichen Umfeld durch Intermediäre (GRK-Querschnittsthema!) konkretisieren lassen.

C.3 kam in Phase II hinzu. Mit psychologischem Schwerpunkt – genauer: von Beginn an aus der Nutzendenperspektive getrieben – wurden hier IoT-gestützte Lernumgebungen adressiert. Zunächst wurde gezeigt, wie die (IoT-)Systemzuverlässigkeit als bedeutender Treiber für Vertrauenskonstitution wirkt. Weitreichende Arbeiten betrafen und betreffen noch (s.u.) die Bedingungen, unter denen KI-basierte pädagogische Agenten erheblichen Einfluss auf Lernverhalten und -erfolg haben [T12].

Entwicklung des Forschungsplans. Die Pandemie erschwerte v. a. empirische Arbeiten in Bereich C wesentlich, auch individuelle Promotionsfortschritte waren durch eingeschränkte lokale und internationale Interaktion betroffen. Dennoch konnte der Forschungsplan – leicht verzögert, aber vollständig – erfolgreich verfolgt werden.

3.2.4. Forschungsbereich D

Ausgangspunkt, Ergebnisse und Erkenntnisse. Bereich D widmete sich wie erwähnt der Unterstützung von P+T im Endgerät (Smartphone usw.) im Sinne einer digitalen Repräsentanz bzw. Stellvertretung von Nutzenden (ALTEREGO) –

offensichtlich eine spezielle Form von *Intermediär*, einem Querschnittsthema von Phase II. In dieser Phase forschte Bereich D vermehrt an *Föderationen* von Komponenten bzw. Geräten. D.1 und A.2 werden gemeinsam behandelt, weil sie in Phase II (Wegberufung Fr. Prof. Volkamer) in D.5 überführt wurden. D.2, D.3 und D.4 beforschten v. a. technische Aspekte des ALTEREGO-Paradigmas in den ringförmigen Zonen Endgerät(-Föderation) (D.4) → Nutzenden-Umfeld (D.2) → Internet (D.3). In **D.1** und **A.2** wurden Methoden zur Modellierung von menschlichen Privatheits- und Vertrauensentscheidungen erforscht [T13] sowie Abbildungen von Vertrauensbewertungen, mentale Modelle und die Kommunikation von Privatheitsrisiken [T14].

D.2 erweiterte und optimierte kryptographische Verfahren im Umfeld des elektronischen Personalausweises und analysierte grundsätzliche Sicherheitsannahmen klassischer Verfahren aus diesem Feld [T15]. Mit der Konzentration auf Föderationen (Phase II) wurden hierfür Möglichkeiten erforscht, auch unsichere (Hardware- oder Software-)Komponenten tolerieren zu können, zudem wurde die Bindung von Protokollen an bestimmte Hardware untersucht.

D.3 beforschte Ansätze, um Bedrohungen für P+T durch Schwächen des Kern-Internet zu bekämpfen. In diesem riesigen Problemkreis wurden zunächst Themen exploriert wie die Bekämpfung von Falschinformation und die Sicherung von P+T durch föderierte eIDs, außerdem die Beseitigung Internet-seitiger Schwächen verschlüsselten Rechnens. Dann konzentrierte sich die Forschung auf die mangelhafte Verbreitung sicherer Erweiterungen der Internet-Infrastruktur wie DNSSEC und das globale Routing-Verfahren BGP (absicherbar mittel RPKI): dieser Mangel eröffnet Kompromittierungen von P+T Tür und Tor. Die Ursachen wurden systematisch analysiert und Ansätze zur Abhilfe wurden entwickelt [T16]. Zuletzt wurden v. a. für DNSSEC modulare Ansätze erforscht, die höhere Sicherheit bspw. im Lichte von Quantencomputern ermöglichen.

In Postdoc-Projekt **D.4** wurde mit Soziologie-Unterstützung an einem soziotechnischen ALTEREGO-Entwicklungsprozess gearbeitet unter Einbindung der „Stakeholder“. Schon ab Phase I wurde eng mit B.2 kooperiert, u. a. zu neuen Ansätzen für anonyme Kommunikation als Voraussetzung für die Nutzung nicht-vertrauenswürdiger Kommunikationsinfrastrukturen, ab Phase II zudem an der Föderation von Komponenten und flexiblen ALTEREGO-Verbünden, insb. für Privatheitsschutz bei Recommender-Systemen [T17] und (schwerpunktmäßig, s. B.2) bei föderiertem Maschinellen Lernen. Jüngste Arbeiten betreffen datenschutzfreundliche Maßnahmen gegen Bedrohungen der Privatheit durch Soft- und Hardwarekomponenten.

In **D.5** wurden Erwartungen von Nutzenden an die Gestaltung von Intermediären und die Kommunikation mit diesen untersucht, bspw. in Bezug auf Privatheitseinstellungen, informierte Einwilligung und Automatisierungsgrad [T18].

Teilprojekt-**übergreifend** betrachtet wurden zudem: die Rolle psychologischer Bedürfnisse (D.5, D.4), Kontaktnachverfolgung (D.4, D.2, C.1), Secure Messaging (D.2, A.2) und datenschutzkonforme Gestaltung von Diensten [T19] (D.5, C.1).

Entwicklung des Forschungsplans. Wie erwähnt wurden in Phase II (Wegberufung von Fr. Prof. Volkamer) A.2 und D.1 nach D.5 überführt, das zur Radnabe für die Usability-Aspekte wurde, ergänzt u.a. durch (Fr. Prof.) K. Marky. D.2 war (wie A.1) naturgemäß eng mit kryptographischen Fragestellungen verknüpft, hier wurde zunehmend auch Post-Quantum-Sicherheit für elektronische Identitäten sehr erfolgreich mitverfolgt [T20] (>80-mal zitiert, Best-Paper-Award bei der ESORICS 2019).

3.2.5. Qualitätssicherung, Forschungsdaten-Handhabung, Kommunikation

Sicherstellung der Validität und Nachvollziehbarkeit. Die im GRK vertretenen Disziplinen sind von unterschiedlichen wissenschaftlichen Methoden geprägt, welche konsequent verfolgt wurden (GRK-Motto: *eng interdisziplinär kooperieren, disziplinär publizieren*). Bspw. verlangt Informatik bei experimentellen Arbeiten vergleichende Evaluationen der (Software-)Prototypen. Wichtige Konferenzen ähneln dort im Stellenwert guten Fachzeitschriften, Peer-Reviews im Doppelblind-Verfahren sind Standard. Wirtschaftsinformatik hat rigide Publikationserfordernisse der bevorzugten VHB-gerankten Konferenzen und Fachzeitschriften. Auch für Rechtswissenschaften gelten strenge Erfordernisse der Fachzeitschriften, methodischer Diskurs erfolgt zudem in- und außerhalb von Konferenzen. Die Soziologische Theorie (B.1) ist auf die Dissertationen (als Monographien) fokussiert, deren methodische Qualitätssicherung hohen Standards genügt (v. a. für qualitative empirische Falluntersuchungen). Open-Science-Strategien wurden im GRK-Verlauf von den Universitäten zunehmend implementiert und dann im GRK umgesetzt (soweit datenschutzrechtlich möglich); sie zielen auf umfassende Bereitstellung der erhobenen

Daten und Resultate für die Öffentlichkeit (s. nächster Abschnitt). Studien mit Beteiligung von Nutzenden waren jeweils von der zuständigen Ethikkommission zu begutachten. Qualitative Auswertungen erfolgten zur Erhöhung der Objektivität von mindestens zwei unabhängigen Forschenden. Beispielhaft sei an die übergreifenden Arbeiten in Bereich A erinnert, wo die Praktikabilität in Pilotprojekten und Studien mit Anwendern (Polizei, s. A.1 u. A.4), Nutzenden und Unternehmen (technisch wie wirtschaftlich) in einem Ausmaß nachgewiesen wurde, das für derart innovative Forschung seinesgleichen sucht.

Handhabung von Forschungsdaten. Die im GRK-Verlauf entstandenen Regeln und Unterstützungsangebote der beteiligten Universitäten wurden u. a. durch jeweils aktualisierte Qualifizierungsmaßnahmen zu Forschungsdaten-Management ins GRK getragen. Das Spannungsfeld zwischen Datentransparenz und -schutz wurde sehr ernst genommen, an zwei Standorten waren Mitantragsteller Mitglieder der zentralen Ethikkommission (Lamla, Hollick). Die im Laufe von Phase II von den Universitäten etablierten Metadaten-Standards wurden jeweils umgesetzt, die FAIR-Prinzipien sind inzwischen fest etabliert. Open Access wird forciert, Veröffentlichung unter DBLP per eindeutiger DOI ist selbstverständlich Quasistandard. Schon ab Phase I wurden Forschungsdaten (soweit datenschutzrechtlich unbedenklich), Software-Artefakte und -Bibliotheken auf Plattformen wie insb. Github bereitgestellt, s. bspw. <https://github.com/tklab-tud/HOSN> und ... /LLC. Zum Einsatz kommen auch z.B. OSF Open Materials und für Sensordaten die Plattform Zenodo (s. <https://zenodo.org/records/5594651>), Mathematische Beiträge sind auf Archiven wie <https://eprint.iacr.org/> abgelegt. Mess- und Textdaten wurden auf internen Servern gespeichert und gesichert. Die Einholung von Ethikkommissions-Voten bei allen relevanten Arbeiten führte bspw. bei B.4 (Datenerhebung im Fluchtcontext) dazu, dass erhobene Daten unter Verschluss blieben, unbedenkliche Forschungsdaten und die Fragebogenentwicklung aber in TUDatalib als Open Data publiziert wurden.

Veranstaltungen, Wissenschaftskommunikation. Wissenschaftlich war neben den unmittelbaren Veröffentlichungen die Mitwirkung in der akademischen Gemeinschaft essenziell: Wissenschaftstreibende des GRK sind im ganzen Spektrum akademischer Rollen aktiv. Besondere Strahlkraft erzielten die leitend organisierten Veranstaltungen, insb. 2018–2021 und 2023 der *Interdisciplinary Workshop on Privacy & Trust (iPAT)* vom kollegfinanzierten wissenschaftlichen Nachwuchs sowie weiteren GRK-Mitgliedern, 2016 die *Darmstadt Security Week* als Kolokation von drei einschlägigen Konferenzen (IFIPTM Trust-Konferenz mit General Chair M. Mühlhäuser, WiSec mit General Chair M. Hollick) und sieben Workshops, 2016 und 2018 der *Workshop on Secure Key Exchange and Channel Protocols (SKECH2 und SK3CH)* von M. Fischlin mit B. Warinschi, 2018 bzw. 2019 die Konferenzen *Security Standardisation Research (SSR)* und *Eurocrypt* (General Chair: M. Fischlin), 2023 das *International Symposium on Technikpsychologie* (General Chair: J. Vogt), der 10. *Workshop Theory and Practice of Multi-Party Computation 2024* in Darmstadt, s. <https://encrypto.de/TPMPC24>). Zu erwähnen sind auch die vielen Turnus-Veranstaltungen des GRK (Female Scientist Lecture Series, GRK-Termine der Verbund-übergreifenden Distinguished Lecture Series, GRK-Tage etc.)

Am Übergang zwischen internationaler und lokaler Wirkung fanden ebenfalls viele Veranstaltungen statt, so ein Disziplin- und Orts-übergreifendes Seminar für Studierende, organisiert und supervidiert von GRK-Promovierenden und -Postdocs (gleichzeitig Qualifizierungsmaßnahme), die Tagung *Partizipatives Privacy by Design* am ITeG in Kassel und mehr. Hervorzuheben ist auch eine Vielzahl an Aktivitäten im halbwissenschaftlichen, öffentlichen und politischen Kontext, die nur auszugsweise aufgeführt seien. Das Anwendungsprojekt von A.1 und A.4 mit der Hamburger Polizei erhielt breite Resonanz, u. a. beim Praxiskolleg der Akademie der Polizei (2021), im Hamburger Polizei Journal, beim 21sten Workshop *Privacy in the Electronic Society (WPES)* der Leuchtturm-Konferenz ACM CCS und der Abschlussveranstaltung *Kryptografischer Datenaustausch zwischen Sicherheitsbehörden* (beides 2022). Erwähnt seien weiter Veranstaltungs-zentrale Auftritte bei der 60. *Assistenten-tagung Öffentliches Recht* in Trier, beim Darmstädter CAST-Workshop *KI und Cybersecurity 2024*, beim Gründerstammtisch *StartUpSecure Special* ab 2019, beim *AI Summit 2023* und bei diversen weiteren Veranstaltungen wie denen des Instituts *eFl-the Data Science*. Besondere Strahlkraft erzielte die GRK-Abschlussveranstaltung in Brüssel bei EU-Politik, Presse und Öffentlichkeit. Genannt sei erneut das Open-Access-Buch *Human Factors in Privacy Research* von und mit GRK-Forschenden [T9].

4. Bilanz zu Qualifizierung, Betreuung und Kooperationen des Kollegs

Überblick: Die Organisations- und Governance-Strukturen des GRK bewährten sich, von der Aufteilung in die vier Forschungsbereiche bis zu den Gremien und Formaten (Plenum, Direktorium, PI-Meeting, GRK-Tage). In Phase II wurden die PI-Rollen optimiert durch fixe Zuordnungen für alle Antragstellenden. Das Qualifizierungskonzept erfolgte i. W. antragsgemäß. Es beinhaltete u. a. die curricularen Fixpunkte (Einführung, jährlich Barcamp und Retreat, wöchentlich-halbtags Seminar und Treffen), einschlägige Schlüsselqualifikationen (oft speziell für das GRK, immer Standort-übergreifend), internationale Kooperationen und Aufenthalte, Vernetzung mit Verbänden der Standorte (bspw. SFB CROSSING) und durchgeplanten wissenschaftlichen Austausch inkl. selbst-organisierter Formate (s. 3.2.5). Die Rekrutierung erfolgte Arbeitsmarkt-bedingt vermehrt universitätsintern, mit großem Erfolg. Das Betreuungskonzept mit interdisziplinären Tandems wurde ständig weiterentwickelt, bspw. mit Einbeziehung der Nachwuchsforschenden, s. u. Die Bearbeiter-Teams wurden flexibilisiert, um wechselnde Detailaktivitäten abzubilden. Wichtige weitere Aspekte werden nachfolgend skizziert.

Gesamtzahl der Geförderten	bislang lediglich eingereichte Dissertationen	abgeschlossene Promotionsverfahren	durchschnittliche Promotoinsdauer in Monaten	Unterbrechungen (Krankheit, Elternzeit ...)	Promotionsabbrüche
46	0	22	45,1 (42,4 o. Elternzeit)	4	1+3, 4 Wechsel

Promotionsbilanz: Die Zahlen der obigen Tabelle spiegeln insb. deutliche Corona-bedingte Verlängerungen der Promotionszeit wieder, z.T. auch mit mitfolgenden gesundheitlichen Einschränkungen. Schon ohne dies erforderten die meist stark empirisch-experimentellen Arbeiten mehr als drei Jahre. Große gemeinsame Anstrengungen verhinderten aber Corona-bedingte Abbrüche. Von den 46 geförderten Promovierenden haben zum Berichtszeitpunkt 22 abgeschlossen (sechs mit Auszeichnung). Die restlichen 24 setzen sich zusammen aus vier Abbrüchen (3+1, s.u.), vier Wechseln und 16 laufenden Promotionen wie folgt. Von den vier Abbrüchen erfolgten drei in der Findungsphase (Borgwart, El-Hanafi, Penner) nach wenigen Monaten. Die Betroffenen hatten die Promotion unter falschen Vorstellungen begonnen, obwohl ausführliche Beratung beim Bewerbungsprozess dies verhindern sollte; alle wechselten in die freie Wirtschaft. Beim bedauerlichen vierten Fall (Fr. Laubach) war die Promotion im vierten GRK-Jahr quasi abgeschlossen, nur letzte Kommentare von Betreuer Roßnagel waren noch einzuarbeiten. Sie trat dann eine Stelle als Richterin an und ließ leider die fertige Arbeit bis heute liegen, trotz zahlreicher Ermutigungen. Von den vier Wechselnden erkannte einer (Almon) – nach einem knappen Jahr –, dass andere Themen des Fachgebiets von PI Hollick seinen Neigungen stärker entsprachen. Bei zweien (Milde, Fr. Kahlert) hatten die Ortswechsel persönliche Gründe, wobei bei Fr. Kahlert inhaltliche Kontinuität gegeben ist. Bei Herrn Frankenbach schließlich tat sich völlig überraschend ein Förderprojekt zu seinem „Traum“-Thema in Saarbrücken auf, diese Chance konnte er sich nicht nehmen lassen. Alle vier Genannten brachen ihre Promotion nicht ab, sondern wechselten den Ort und/oder das Thema; sie verließen damit allerdings den GRK-Betreuungsrahmen. Von den 16 laufenden Promotionen gehören acht zu den Corona-verzögerten; diese sind allesamt weit fortgeschritten, die Dissertationen von vier (Müllmann, Lurtz, Franckenbach, Fr. Fecho) sind abgabereif. Zwei Juristen (Lurtz, Kassel; Müllmann, Ffm.) wollen berufsbegleitend abschließen, Fr. Fecho in Kürze innerhalb ihrer Elternzeit. Die letztgenannten drei wurden im GRK ersetzt, die restlichen fünf Corona-Verzögerten bilden mit acht ab Ende 2021 ins GRK Aufgenommenen die letzten 13, die von den 13 Antragstellenden betreut werden (vgl. Tabelle 6.2.1, Nr. 32-46 ohne 34, 45). Für alle wurde direkte Anschlussfinanzierung ermöglicht, teils aus Rückstellungen der Universitäten zur Kompensation von DFG-Kürzungen bei Phase II (Schmitt weiterfinanziert bei PI Waidner am ATHENE-Forschungszentrum, Fr. Sanina bei PI Fischlin am SFB 1119). Die Antragsteller werten die Bilanz mit nur vier echten Abbrüchen bei 44 Personen, davon drei noch in der Findungsphase, als sehr beachtlich, zumal im Lichte der Pandemie.

Frauenanteil: Die jeweils letzten der DFG-geförderten Promovierenden (13 Stellen, 2 Elternzeit-Pausen) repräsentieren ein nahezu ausgeglichenes Verhältnis (8 männlich, 7 weiblich: 47%), die im Phase-II-Antrag anvisierten 48% wurden also quasi

erreicht; bei den extern-finanzierten konnte sogar über die neun Jahre hinweg ein ausgeglichenes Verhältnis erreicht werden (8:8). Als DFG-geförderte Postdocs kamen nur Informatiker in Frage, was leider zu (vier) rein männlichen Besetzungen führte; dagegen wurde bei den extern finanzierten Postdocs das Verhältnis 11m:9w erreicht, in Summe also 15:9; das anvisierte Ziel (ein Drittel weiblich) wurde bei Postdocs also deutlich übererfüllt.

Förderung wissenschaftlicher Selbständigkeit und Karriere: Hier ist zunächst die besonders hohe Durchlässigkeit zwischen allen wissenschaftlichen Karrierestufen und deren starke Einbeziehung hervorzuheben wie folgt. (a) Forschungsstudierende wurden ans GRK herangeführt; (b) die stark und zahlreich eingebundenen Postdocs *profitierten* einerseits stark von interdisziplinärer Kooperation im GRK, *leisteten* andererseits wichtige Beiträge v. a. der Vermittlung von Kenntnissen und Fertigkeiten. (c) In der weiteren Karriere wurden diese Postdocs tw. sogar beteiligte Wissenschaftler des GRK. Beispielhaft sei Karola Marky genannt, die schon als assoziierte Doktorandin eng integriert war, dann als Postdoc und schließlich als beteiligte Wissenschaftlerin das GRK stark beförderte. Heute verantwortet sie als „tenured“ W2-Professorin am Exzellenzcluster CASA selbst DFG-Anträge. Als zweiter wichtiger Beitrag seien die bedarfs-orientierten Workshops genannt. Diese adressierten tw. Standard-Themen wie *Gute wissenschaftliche Praxis* und *Forschungsdatenmanagement*, aber auch viele Aspekte wissenschaftlich-methodischen Vorgehens und Schulung für wichtige Werkzeuge. Förderlich waren die persönlichen Qualifizierungs-Portfolios, die im Rahmen von Betreuungsmaßnahmen festgelegt und fortgeschrieben wurden.

Rückwirkungen auf Promotionsbedingungen der Hochschulen: Die Ingenieurs-Disziplinen der GRK-Standorte standen früher „verschulten“ Promotionsprogrammen skeptisch gegenüber, inzwischen sind auch dort Graduiertenschulen verbreitet. Zum Abbau der Skepsis trug das GRK (von dessen Antragstellenden viele ingenieurwissenschaftlich arbeiten) wesentlich bei, indem es sich auf nachweislich förderliche Maßnahmen fokussierte und deren Erfolge nachwies. Neue standortübergreifende Schulen wie ELIZA und GS|EFM sowie neue DFG-Verbundanträge orientierten sich deshalb an den Erfolgsmodellen des GRK. Außerdem wurden Formate wie die *Distinguished Lectures*, der *Female Student Travel Award* u. s. w. Verbund-übergreifend veranstaltet und vom GRK initiierte Formate der Softskill-Akademien der Hochschulen dauerhaft ins Portfolio übernommen.

Chancengleichheitsmaßnahmen: Das GRK 2050 ist stolz auf seine konzertierten Maßnahmen in diesem Bereich, gegliedert in fünf Aktionslinien: a) Die herausragend erfolgreiche Vortragsreihe *Female Scientist Lecture Series* FSLs, wo Wissenschaftlerinnen als Rollenmodelle sowohl GRK-relevante Inhalte als auch gender-spezifische Karriere-Erfahrungen vortrugen und tw. sehr umfangreiche interaktive Formate gestalteten; b) Themen-vielfältige einschlägige Workshops (bspw. *Female Leadership Training*); c) der Female Student Travel Award; d) fortlaufende proaktive Information und Kommunikation sowie individuelle Beratung; e) vielfältige Elternunterstützung bspw. mit Räumen und Betreuungsangeboten. Im Ergebnis werteten Kollegiatinnen den Nutzen als sehr hoch und schrieben aktiv den Maßnahmenkatalog fort.

Kooperationsbilanz: Das GRK wirkte nachhaltig in die thematisch relevanten internationalen Forschungsgemeinden hinein, trotz Corona. Die breit gefächerten Kooperationsmaßnahmen wurden in 3.2.5 skizziert. Mit lokalen Verbünden wie dem Kasseler iTeG oder dem SFB CROSSING und dem nationalen Sicherheitsforschungszentrum ATHENE in Darmstadt stand das GRK in engster Verbindung, u. a. durch Organisation gemeinsamer Formate und personelle Überlappungen. Aus dem regelmäßig beschickten Dagstuhl-Seminar der Informatik-GRKs ergaben sich diverse Anknüpfungspunkte und Kontakte, auch mit großen Verbünden wie dem Exzellenzcluster CASA, Zentren wie CISPA oder EU-Netz *Privacy&Us* sowie Universitäten im In- und Ausland stand das GRK im engen Austausch. In Phase II wurde das Format der Mercator-Fellows (8 Personen in Phase I) antragsgemäß durch vermehrte Gastwissenschaftler-Aufenthalte ersetzt (17 trotz Corona).

Gesamtbilanz: Neben dem erfolgreichen Qualifikations- und Betreuungskonzept sind von den GRK-Erfolgsfaktoren folgende besonders hervorzuheben: das starke Koordinationsteam (wiss. Postdoc und Sprecher, Programm-Managerin 0,5*E13, Sekretariat 0,5*E9), hervorragende standortübergreifende Kooperation der Promovierenden (DFG- und extern finanziert), äußerst gelungene Einbeziehung des wissenschaftlichen Nachwuchses, weibliche Rollenmodelle und die hohen wissenschaftlichen Maßstäbe, außerdem die Synergien mit den thematisch verwandten Verbünden vor Ort. Das GRK diene und dient als Blaupause etlicher vergleichbarer Forschungsvorhaben weit über seine Standorte hinaus.

5. Projektergebnisse

5.1. Projektergebnisse der Doktorandinnen und Doktoranden sowie ggf. der Postdoktorandinnen und Postdoktoranden

5.1.1. Projektergebnisse der Doktorandinnen und Doktoranden sowie ggf. der Postdoktorandinnen und Postdoktoranden (finanziert aus Mitteln des Graduiertenkollegs)

Die nachfolgende Auflistung der Projektergebnisse, an denen kollegfinanzierte (Post-)Doktorandinnen und (Post-)Doktoranden (ggf. maßgeblicher) beteiligt waren, ist sortiert nach dem jeweiligen Erscheinungsjahr. Alle am Kolleg beteiligten (Post-)Doktorandinnen und (Post-)Doktoranden sind hervorgehoben. Open-Access-Publikationen sind mit einem Symbol  am Seitenrand markiert.

Publikationen mit wissenschaftlicher Qualitätssicherung

- [1] L. Bock, S. Karuppayah, **T. Grube**, M. Mühlhäuser und M. Fischer. „Hide and Seek: Detecting Sensors in P2P Botnets“. In: *2015 IEEE Conference on Communications and Network Security, CNS 2015, Florence, Italy, September 28-30, 2015*. IEEE Conference on Communications and Network Security. Open Access (ePrint). IEEE, Sep. 2015, S. 731–732. DOI: 10.1109/CNS.2015.7346908. eprint: <https://download.hrz.tu-darmstadt.de/media/FB20/Dekanat/Publikationen/TK/Submitted-sensorDetection15.pdf>. 
- [2] **A. Borgwart**, **S. Boukoros**, **H. Shulman**, C. van Rooyen und M. Waidner. „Detection and Forensics of Domains Hijacking“. In: *Proceedings of the Global Communications Conference (GLOBECOM 2015)*. 2015 IEEE Global Communications Conference (GLOBECOM). IEEE, Dez. 2015, S. 1–6. DOI: 10.1109/glocom.2015.7417736.
- [3] C. G. Cordero, **E. Vasilomanolakis**, N. Milanov, C. Koch, D. Hausheer und M. Mühlhäuser. „ID2T: A DIY Dataset Creation Toolkit for Intrusion Detection Systems“. In: *Proceedings of the IEEE Conference on Communications and Network Security (CNS 2015)*. IEEE / IEEE, Sep. 2015, S. 739–740. DOI: 10.1109/cns.2015.7346912.
- [4] C. G. Cordero, **E. Vasilomanolakis**, M. Mühlhäuser und M. Fischer. „Community-Based Collaborative Intrusion Detection“. In: *Proceedings of the International Conference on Security and Privacy in Communication Systems (SecureComm 2015)*. Hrsg. von B. Thuraisingham, X. Wang und V. Yegneswaran. Bd. 164. Security and Privacy in Communication Networks. Springer Nature / Springer, Okt. 2015, S. 665–681. ISBN: 978-3-319-28864-2. DOI: 10.1007/978-3-319-28865-9_44.
- [5] V. Gazis, M. Görtz, M. Huber, A. Leonardi, K. Mathioudakis, A. Wiesmaier, F. Zeiger und **E. Vasilomanolakis**. „A Survey of Technologies for the Internet of Things“. In: *Proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC 2015)*. IEEE / IEEE, Aug. 2015, S. 1090–1095. DOI: 10.1109/iwcmc.2015.7289234.
- [6] **I. Heimbach**, J. Gottschlich und O. Hinz. „The Value of User’s Facebook Profile Data for Product Recommendation Generation“. In: *Electronic Markets* 25.2 (März 2015), S. 125–138. ISSN: 1019-6781. DOI: 10.1007/s12525-015-0187-9.
- [7] **I. Heimbach**, D. S. Kostyra und O. Hinz. „Marketing Automation“. In: *Business & Information Systems Engineering* 57.2 (März 2015), S. 129–133. ISSN: 1867-0202. DOI: 10.1007/s12599-015-0370-8.
- [8] **I. Heimbach**, B. Schiller, T. Strufe und O. Hinz. „Content Virality on Online Social Networks: Empirical Evidence from Twitter, Facebook, and Google+ on German News Websites“. In: *Proceedings of the 26th Conference on Hypertext & Social Media*. Hrsg. von Y. Yesilada, R. Farzan und G.-J. Houben. ACM Conference on Hypertext & Social Media. ACM / ACM, Aug. 2015, S. 39–47. DOI: 10.1145/2700171.2791032.
- [9] **M. Nebel**. „Facebook knows your vote! – Big Data und der Schutz politischer Meinung in sozialen Netzwerken“. In: *Privatheit, öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data*. Nomos / Nomos Verlagsgesellschaft mbH & Co. KG, 2015, S. 89–110.
- [10] **M. Nebel**. „Schutz der Persönlichkeit – Privatheit oder Selbstbestimmung“. In: *Verfassungsrechtliche Zielsetzungen im deutschen und europäischen Recht*, ZD 517 (2015).
- [11] A. Roßnagel und **M. Nebel**. „(Verlorene) Selbstbestimmung im Datenmeer“. In: *Datenschutz und Datensicherheit - DuD* 39.7 (Juni 2015), S. 455–459. ISSN: 1614-0702. DOI: 10.1007/s11623-015-0449-x.

- [12] A. Roßnagel, **M. Nebel** und **P. Richter**. „Was bleibt vom europäischen Datenschutzrecht“. In: *Überlegungen zum Ratsentwurf der DS-GVO*, ZD 455 (2015).
- [13] **E. Vasilomanolakis**, **J. Daubert**, M. Luthra, V. Gazis, A. Wiesmaier und P. Kikiras. „On the Security and Privacy of Internet of Things Architectures and Systems“. In: *Proceedings of the International Workshop on Secure Internet of Things (SIoT 2015)*. Hrsg. von G. Ghinita und P. Peris-Lopez. International Workshop on Secure Internet of Things. Open Access (ePrint). IEEE Computer Society, Sep. 2015, S. 49–57. DOI: 10.1109/siot.2015.9. eprint: <https://download.hrztu-darmstadt.de/media/FB20/Dekanat/Publikationen/TK/SIoTpaper.pdf>. 
- [14] **E. Vasilomanolakis**, S. Karuppayah, P. Kikiras und M. Mühlhäuser. „A Honeypot-Driven Cyber Incident Monitor: Lessons Learned and Steps Ahead“. In: *Proceedings of the 8th International Conference on Security of Information and Networks (SINCONF 2015)*. Hrsg. von O. B. Makarevich, R. Poet, A. Elçi, M. S. Gaur, M. A. Orgun, L. K. Babenko, M. S. Ferdous, A. T. S. Ho, V. Laxmi und J. Pieprzyk. International Conference on Security of Information and Networks. ACM / ACM, Sep. 2015, S. 158–164. DOI: 10.1145/2799979.2799999.
- [15] **E. Vasilomanolakis**, S. Karuppayah, M. Mühlhäuser und M. Fischer. „Taxonomy and Survey of Collaborative Intrusion Detection“. In: *ACM Computing Surveys (CSUR)* 47.4 (Mai 2015), S. 55. ISSN: 0360-0300. DOI: 10.1145/2716260.
- [16] **E. Vasilomanolakis**, M. Krügl, C. G. Cordero, M. Mühlhäuser und M. Fischer. „Skipmon: A Locality-Aware Collaborative Intrusion Detection System“. In: *Proceedings of the International Performance Computing and Communications Conference (IPCCC 2015)*. Open Access (ePrint). IEEE / IEEE, Dez. 2015, S. 1–8. DOI: 10.1109/pccc.2015.7410282. eprint: <https://download.hrztu-darmstadt.de/media/FB20/Dekanat/Publikationen/TK/vasilomanolakis15skipmon.pdf>. 
- [17] **E. Vasilomanolakis**, S. Srinivasa und M. Mühlhäuser. „Did You Really Hack a Nuclear Power Plant? An Industrial Control Mobile Honeypot“. In: *Proceedings of the Conference on Communications and Network Security (CNS 2015)*. IEEE / IEEE, Sep. 2015, S. 729–730. DOI: 10.1109/cns.2015.7346907.
- [18] **E. Vasilomanolakis**, M. Stahn, C. G. Cordero und M. Mühlhäuser. „Probe-Response Attacks on Collaborative Intrusion Detection Systems: Effectiveness and Countermeasures“. In: *Proceedings of the Conference on Communications and Network Security (CNS 2015)*. IEEE / IEEE, Sep. 2015, S. 699–700. DOI: 10.1109/cns.2015.7346892.
- [19] **A. Borgwart**, **H. Shulman** und M. Waidner. „Towards Automated Measurements of Internet’s Naming Infrastructure“. In: *Proceedings of the International Conference on Software Science, Technology and Engineering (SWSTE 2016)*. IEEE International Conference on Software Science, Technology and Engineering. IEEE, Juni 2016, S. 117–124. DOI: 10.1109/SWSTE.2016.25.
- [20] **S. Boukoros**, A. Kalampogia und P. Koutsakis. „A New Highly Accurate Workload Model for Campus Email Traffic“. In: *Proceedings of the International Conference on Computing, Networking and Communications (ICNC 2016)*. 2016 International Conference on Computing, Networking and Communications (ICNC). IEEE / IEEE, Feb. 2016, S. 1–7. DOI: 10.1109/icnc.2016.7440639.
- [21] **N. Büscher**, S. Schiffner und M. Fischer. „Consumer Privacy on Distributed Energy Markets“. In: *Proceedings of the Annual Privacy Forum (APF 2016)*. Hrsg. von S. Schiffner, J. Serna, D. Ikonomidou und K. Rannenberg. Bd. 9857. Lecture Notes in Computer Science. Springer, Sep. 2016, S. 96–114. ISBN: 978-3-319-44759-9. DOI: 10.1007/978-3-319-44760-5_7.
- [22] G. Chehraz, **I. Heimbach** und O. Hinz. „The Impact of Security by Design on the Success of Open Source Software“. In: *Proceedings of the European Conference on Information Systems (ECIS 2016)*. European Conference on Information Systems. AIS eLibrary, 2016, 179:1–179:18.
- [23] C. G. Cordero, **S. Hauke**, M. Mühlhäuser und M. Fischer. „Analyzing Flow-Based Anomaly Intrusion Detection Using Replicator Neural Networks“. In: *14th Annual Conference on Privacy, Security and Trust (PST 2016)*. IEEE, Dez. 2016, S. 317–324. DOI: 10.1109/pst.2016.7906980.
- [24] **N. Eling**, C. Büchner und P. Buxmann. „Business Models for Free Digital Goods and Services“. In: *49th Hawaii International Conference on System Sciences (HICSS 2016)*. Hrsg. von T. X. Bui und R. H. S. Jr. Hawaii International Conference on System Sciences. University of Hawai’i at Manoa / IEEE, Jan. 2016, S. 1487–1496. DOI: 10.1109/hicss.2016.188.

- [25] **N. Eling**, S. Rasthofer, M. Kolhagen, E. Bodden und P. Buxmann. „Investigating Users’ Reaction to Fine-Grained Data Requests: A Market Experiment“. In: *49th Hawaii International Conference on System Sciences (HICSS 2016)*. Hrsg. von T. X. Bui und R. H. S. Jr. Hawaii International Conference on System Sciences. University of Hawai’i at Manoa / IEEE, Jan. 2016, S. 3666–3675. DOI: 10.1109/hicss.2016.458.
- [26] **I. Heimbach** und O. Hinz. „The Impact of Content Sentiment and Emotionality on Content Virality“. In: *International Journal of Research in Marketing* 33.3 (Sep. 2016), S. 695–701. ISSN: 0167-8116. DOI: 10.1016/j.ijresmar.2016.02.004.
- [27] **O. Kulyk**, **P. Gerber**, **M. El-Hanafi**, B. Reinheimer, K. Renaud und M. Volkamer. „Encouraging Privacy-Aware Smartphone App Installation: What Would the Technically-Adept Do“. In: *NDSS Workshop on Usable Security (USEC 2016)*. Open Access. Internet Society, Feb. 2016, S. 10. ISBN: 1-891562-42-8. DOI: 10.14722/usec.2016.23016.
- [28] **B. Milde**, J. Wacker, S. Radomski, M. Mühlhäuser und C. Biemann. „Demonstrating Ambient Search: Implicit Document Retrieval for Speech Streams“. In: *Proceedings of International Conference on Computational Linguistics (COLING 2016)*. Hrsg. von H. Watanabe. International Conference on Computational Linguistics. ACL, Dez. 2016, S. 233–237. URL: <https://aclanthology.org/C16-2049/>.
- [29] **B. Milde**, J. Wacker, S. Radomski, M. Mühlhäuser und C. Biemann. „Ambient Search: A Document Retrieval System for Speech Streams“. In: *Proceedings of International Conference on Computational Linguistics (COLING 2016)*. Hrsg. von N. Calzolari, Y. Matsumoto und R. Prasad. International Conference on Computational Linguistics. ACL, Dez. 2016, S. 2082–2091. URL: <https://aclanthology.org/C16-1196/>.
- [30] **K. Shrishak**, Z. Erkin und R. Schaar. „Enhancing Privacy of Users in eID Schemes“. In: *Proceedings of the 37th WIC Symposium on Information Theory in the Benelux*. 2016, S. 158–165. URL: <https://www.narcis.nl/publication/RecordID/oai%3Atudelft.nl%3Auuid%3Ae278daa5-a035-49cb-896c-ee36621861c0>.
- [31] **K. Shrishak**, Z. Erkin und R. Schaar. „Enhancing User Privacy in Federated eID Schemes“. In: *Proceedings of the 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS 2016)*. Hrsg. von M. Badra, G. Pau und V. Vassiliou. International Conference on New Technologies, Mobility and Security. IEEE / IEEE, Nov. 2016, S. 1–5. DOI: 10.1109/ntms.2016.7792448.
- [32] S. Valipour, F. Volk, **T. Grube**, L. Böck, L. Karg und M. Mühlhäuser. „A Formal Holon Model for Operating Future Energy Grids during Blackouts“. In: *SMARTGREENS 2016 - Proceedings of the 5th International Conference on Smart Cities and Green ICT Systems, Rome, Italy, April 23-25, 2016*. Hrsg. von C. Klein, B. Donnellan und M. Helfert. International Conference on Smart Grids and Green IT Systems. Open Access. SciTePress, Apr. 2016, S. 146–153. DOI: 10.5220/0005768801460153.
- [33] **E. Vasilomanolakis**, C. G. Cordero, N. Milanov und M. Mühlhäuser. „Towards the Creation of Synthetic, yet Realistic, Intrusion Detection Datasets“. In: *Proceedings of the Network Operations and Management Symposium (NOMS 2016)*. Hrsg. von S. Oktug, M. Ulema, C. Cavdar, L. Z. Granville und C. R. P. dos Santos. Open Access (ePrint). IEEE / IEEE, Apr. 2016, S. 1209–1214. DOI: 10.1109/noms.2016.7502989. eprint: <https://download.hrz.tu-darmstadt.de/media/FB20/Dekanat/Publikationen/TK/id2t-f.pdf>.
- [34] **E. Vasilomanolakis**, S. Srinivasa, C. G. Cordero und M. Mühlhäuser. „Multi-Stage Attack Detection and Signature Generation with ICS Honeypots“. In: *Proceedings of the Network Operations and Management Symposium (NOMS 2016)*. Hrsg. von S. Oktug, M. Ulema, C. Cavdar, L. Z. Granville und C. R. P. dos Santos. IEEE/IFIP Network Operations and Management Symposium. Open Access (ePrint). IEEE / IEEE, Apr. 2016, S. 1227–1232. DOI: 10.1109/noms.2016.7502992. eprint: https://download.hrz.tu-darmstadt.de/media/FB20/Dekanat/Publikationen/TK/hostage_multi_stage.pdf.
- [35] **L. Almon**, M. Riecker und M. Hollick. „Lightweight Detection of Denial-of-Service Attacks on Wireless Sensor Networks Revisited“. In: *Proceedings of the Conference on Local Computer Networks (LCN 2017)*. IEEE Conference on Local Computer Networks. IEEE Computer Society, Okt. 2017, S. 444–452. DOI: 10.1109/LCN.2017.110.
- [36] D. Bernhard, **O. Kulyk** und M. Volkamer. „Security Proofs for Participation Privacy, Receipt-Freeness and Ballot Privacy for the Helios Voting Scheme“. In: *Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES 2017)*. ARES. Open Access (ePrint). ACM / ACM, Aug. 2017, 1:1–1:10. DOI: 10.1145/3098954.3098990. eprint: <https://kau.diva-portal.org/smash/get/diva2:1174180/FULLTEXT01>.

- [37] **S. Boukoros**, N. P. Karvelas und S. Katzenbeisser. „A Lightweight Protocol for Privacy Preserving Division“. In: *Proceedings of the 13th International Wireless Communications and Mobile Computing Conference (IWCMC 2017)*. 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC). IEEE / IEEE, Juni 2017, S. 717–722. DOI: 10.1109/iwcmc.2017.7986373.
- [38] **S. Boukoros** und S. Katzenbeisser. „Measuring Privacy in High Dimensional Microdata Collections“. In: *Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES 2017)*. ACM / ACM, Aug. 2017, S. 15. DOI: 10.1145/3098954.3098977.
- [39] **S. Boukoros**, A. Nugaliyadde, A. Marnerides, C. Vassilakis, P. Koutsakis und K. W. Wong. „Modeling Server Workloads for Campus Email Traffic Using Recurrent Neural Networks“. In: *Proceedings of the International Conference on Neural Information Processing (ICONIP 2017)*. Hrsg. von D. Liu, S. Xie, Y. Li, D. Zhao und E.-S. M. El-Alfy. Bd. 10638. Open Access (ePrint). Springer Science+Business Media / Springer, 2017, S. 57–66. ISBN: 978-3-319-70138-7. DOI: 10.1007/978-3-319-70139-4_6. eprint: https://eprints.lancs.ac.uk/id/eprint/87700/1/RNN_to_Model_Server_Workloads_for_Campus_Email_Traffic_Submitted.pdf. 
- [40] **J. Brendel** und M. Fischlin. „Zero Round-Trip Time for the Extended Access Control Protocol“. In: *Proceedings of the 22nd European Symposium on Research in Computer Security (ESORICS 2017)*. Hrsg. von S. N. Foley, D. Gollmann und E. Sneekenes. Bd. 10492. Lecture Notes in Computer Science. Springer, Sep. 2017, S. 297–314. ISBN: 978-3-319-66401-9. DOI: 10.1007/978-3-319-66402-6_18.
- [41] **J. Brendel**, M. Fischlin, F. Günther und C. Janson. „PRF-ODH: Relations, Instantiations, and Impossibility Results“. In: *Advances in Cryptology – CRYPTO 2017*. Hrsg. von J. Katz und H. Shacham. Bd. 10403. Cham: Springer International Publishing, Aug. 2017, S. 651–681. ISBN: 978-3-319-63696-2 978-3-319-63697-9. DOI: 10.1007/978-3-319-63697-9_22.
- [42] N. Buescher, **S. Boukoros**, S. Bauregger und S. Katzenbeisser. „Two Is Not Enough: Privacy Assessment of Aggregation Schemes in Smart Metering“. In: *Proceedings on Privacy Enhancing Technologies (PoPETs) 2017.4* (Okt. 2017). Open Access, S. 198–214. ISSN: 2299-0984. DOI: 10.1515/popets-2017-0045. 
- [43] **N. Büscher** und S. Katzenbeisser. *Compilation for Secure Multi-party Computation*. In: SpringerBriefs in Computer Science. Open Access (ePrint). Cham: Springer International Publishing, 2017. ISBN: 978-3-319-67521-3 978-3-319-67522-0. DOI: 10.1007/978-3-319-67522-0. eprint: <https://tuprints.ulb.tu-darmstadt.de/8495/>. 
- [44] **N. Eling**. *Der Wert von Nutzerinformationen aus Anbieter- und Nutzerperspektive: Analyse des Trade-offs zwischen Datenverwendung und Datenschutz*. Springer, Okt. 2017. ISBN: 978-3-658-19546-5. URL: <https://tubiblio.ulb.tu-darmstadt.de/89744/>.
- [45] **C. L. Geminn** und **M. Nebel**. „Internationalisierung vs. Nationalisierung im Zeitalter der digitalen Gesellschaft“. In: *Informationelle Selbstbestimmung im digitalen Wandel*. Springer, 2017, S. 287–318. ISBN: 978-3-658-17661-7. DOI: 10.1007/978-3-658-17662-4_17.
- [46] **T. Grube**, **S. Hauke**, **J. Daubert** und M. Mühlhäuser. „Ant Colonies for Efficient and Anonymous Group Communication Systems“. In: *2017 International Conference on Networked Systems, NetSys 2017, Göttingen, Germany, March 13-16, 2017*. 2017 International Conference on Networked Systems (NetSys). IEEE, März 2017, S. 1–8. DOI: 10.1109/NETSYS.2017.7903958.
- [47] **T. Grube**, **S. Hauke**, **J. Daubert** und M. Mühlhäuser. „Ant Colony Optimisation - A Solution to Efficient Anonymous Group Communication?“ In: *14th IEEE Annual Consumer Communications & Networking Conference, CCNC 2017, Las Vegas, NV, USA, January 8-11, 2017*. Consumer Communications and Networking Conference. IEEE, Jan. 2017, S. 337–340. DOI: 10.1109/CCNC.2017.7983129.
- [48] **T. Grube**, M. Thummerer, **J. Daubert** und M. Mühlhäuser. „Cover Traffic: A Trade of Anonymity and Efficiency“. In: *Security and Trust Management - 13th International Workshop, STM 2017, Oslo, Norway, September 14-15, 2017, Proceedings*. Hrsg. von G. Livraga und C. J. Mitchell. Bd. 10547. Lecture Notes in Computer Science. Springer, Sep. 2017, S. 213–223. ISBN: 978-3-319-68062-0. DOI: 10.1007/978-3-319-68063-7_15.
- [49] **T. Grube**, F. Volk, M. Mühlhäuser, S. Bhairav, V. Sachidananda und Y. Elovici. „Complexity Reduction in Graphs: A User Centric Approach to Graph Exploration“. In: *Proceedings of the International Conference on Advances in Human-Oriented and Personalized Mechanisms, Technologies, and Services (CENTRIC 2017)*. IARA, Okt. 2017, S. 24–31. URL: <https://tubiblio.ulb.tu-darmstadt.de/101540/>.

- [50] N. Islam, P. Buxman und **N. Eling**. „Why Should Incumbent Firms Jump on the Start-up Bandwagon in the Digital Era? – A Qualitative Study“. In: *Wirtschaftsinformatik*. Hrsg. von J. M. Leimeister und W. Brenner. WIRTSCHAFTSINFORMATIK. Springer Nature, Feb. 2017.
- [51] S. Karuppayah, L. Böck, **T. Grube**, S. Manickam, M. Mühlhäuser und M. Fischer. „SensorBuster: On Identifying Sensor Nodes in P2P Botnets“. In: *Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, August 29 - September 01, 2017*. ARES. ACM, Aug. 2017, 34:1–34:6. DOI: 10.1145/3098954.3098991.
- [52] F. Kohnhäuser, M. Stute, L. Baumgärtner, **L. Almon**, S. Katzenbeisser, M. Hollick und B. Freisleben. „SEDCOS: A Secure Device-to-Device Communication System for Disaster Scenarios“. In: *Proceedings of the Conference on Local Computer Networks, (LCN 2017)*. IEEE Conference on Local Computer Networks. Open Access (ePrint). IEEE Computer Society, Okt. 2017, S. 195–198. DOI: 10.1109/LCN.2017.47. eprint: <https://tuprints.ulb.tu-darmstadt.de/13329/1/Stute-SEDCOS-2017.pdf>. 
- [53] H. Krasnova, N. F. Veltri, **N. Eling** und P. Buxmann. „Why Men and Women Continue to Use Social Networking Sites: The Role of Gender Differences“. In: *The Journal of Strategic Information Systems* 26.4 (Dez. 2017), S. 261–284. ISSN: 0963-8687. DOI: 10.1016/j.jsis.2017.01.004.
- [54] **O. Kulyk**, S. Neumann, J. Budurushi und M. Volkamer. „Nothing Comes for Free: How Much Usability Can You Sacrifice for Security?“ In: *IEEE Security & Privacy* 15.3 (Juni 2017). Open Access (ePrint), 1:1–1:10. ISSN: 1540-7993. DOI: 10.1109/msp.2017.70. eprint: <https://publikationen.bibliothek.kit.edu/1000081985/15236979>. 
- [55] **O. Kulyk**, S. Neumann, **K. Marky** und M. Volkamer. „Enabling Vote Delegation for Boardroom Voting“. In: *Proceedings of the International Conference on Financial Cryptography and Data Security (FC 2017)*. Hrsg. von M. Brenner, K. Rohloff, J. Bonneau, A. Miller, P. Y. A. Ryan, V. Teague, A. Bracciali, M. Sala, F. Pintore und M. Jakobsson. Bd. 10323. Financial Cryptography Workshops. Open Access (ePrint). Springer Science+Business Media / Springer, Apr. 2017, S. 419–433. ISBN: 978-3-319-70277-3. DOI: 10.1007/978-3-319-70278-0_26. eprint: <https://publikationen.bibliothek.kit.edu/1000081994/50008975>. 
- [56] **O. Kulyk**, B. M. Reinheimer und M. Volkamer. „Sharing Information with Web Services – a Mental Model Approach in the Context of Optional Information“. In: *Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust (HAS 2017)*. Hrsg. von T. Tryfonas. Bd. 10292. Interacción. Springer Science+Business Media / Springer, Juli 2017, S. 675–690. ISBN: 978-3-319-58459-1. DOI: 10.1007/978-3-319-58460-7_46.
- [57] **O. Kulyk**, B. M. Reinheimer, **P. Gerber**, F. Volk, M. Volkamer und M. Mühlhäuser. „Advancing Trust Visualisations for Wider Applicability and User Acceptance“. In: *Proceedings of the Trustcom/BigDataSE/ICSS*. Open Access. IEEE / IEEE, Aug. 2017, S. 562–569. DOI: 10.1109/trustcom/bigdatase/icess.2017.285. eprint: <https://publikationen.bibliothek.kit.edu/1000081998/15445050>. 
- [58] **M. Maass**, **A. Laubach** und D. Hermann. „PrivacyScore: Analyse von Webseiten auf Sicherheits- und Privatheitsprobleme – Konzept und rechtliche Zulässigkeit“. In: *Proceedings of the INFORMATIK 2017*. Hrsg. von M. Eibl und M. Gaedke. Series of the Gesellschaft für Informatik (GI). Open Access, Erweiterte Fassung in arXiv. Bonn: Lecture Notes in Informatics (LNI), Gesellschaft für Informatik e.V. (GI), 2017, S. 1049–1060. ISBN: 978-3-88579-669-5. DOI: 10.18420/in2017_107. arXiv: 1705.08889. 
- [59] **M. Maass** und D. Wegemer. „NFCGate - Ein interaktives Exponat zur Sicherheit von NFC-Systemen“. In: *Proceedings of the Nationale Konferenz IT-Sicherheit*. 2017.
- [60] **M. Maass**, P. Wichmann, H. Pridöhl und D. Herrmann. „PrivacyScore: Improving Privacy and Security via Crowd-Sourced Benchmarks of Websites“. In: *Proceedings of the Annual Privacy Forum (APF 2017)*. Hrsg. von E. Schweighofer, H. Leitold, A. Mitrasak und K. Rannenber. Bd. abs/1705.05139. Annual Privacy Forum. Open Access (arXiv). Springer, Mai 2017, S. 178–191. ISBN: 978-3-319-67279-3. DOI: 10.1007/978-3-319-67280-9_10. arXiv: 1705.05139. 

- [61] **T. Schürmann**. „Psychological Evaluation of Human Choice Behavior in Socio-Technical Systems: A Rational Process Model Approach“. In: *Proceeding of the 11th IFIP International Conference on Trust Management (TM 2017)*. Hrsg. von J.-P. Steghöfer und B. Esfandiari. Bd. AICT-505. HAL (Le Centre Pour La Communication Scientifique Directe). Open Access. Gothenburg, Sweden: Springer, Juni 2017, S. 226–228. URL: <https://hal.inria.fr/hal-01651187>. 
- [62] M. Stute, **M. Maass**, T. Schons und M. Hollick. „Reverse Engineering Human Mobility in Large-Scale Natural Disasters“. In: *Proceedings of the 20th International Conference on Modelling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM '17)*. Hrsg. von A. Loureiro, H.-C. Wu und F. R. Yu. International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems. Open Access (arXiv). ACM, Nov. 2017. DOI: 10.1145/3127540.3127542. arXiv: 1708.02151. 
- [63] **L. Almon**, F. Álvarez, P. Lieser, T. Meuser und F. Schaller. „Ad-Hoc-Kommunikation – Gesellschaftlich wünschenswert, rechtlich ungeregt“. In: *Die Fortentwicklung des Datenschutzes*. Springer, 2018, S. 77–98. ISBN: 978-3-658-23726-4. DOI: 10.1007/978-3-658-23727-1_5.
- [64] F. Álvarez, **L. Almon**, P. Lieser, T. Meuser, Y. Dylla, B. Richerzhagen, M. Hollick und R. Steinmetz. „Conducting a Large-Scale Field Test of a Smartphone-Based Communication Network for Emergency Response“. In: *Proceedings of the 13th Workshop on Challenged Networks (CHANTS@MobiCom 2018)*. Hrsg. von M. Feldmann und M. Hassan. CHANTS@MOBICOM. Open Access (arXiv). ACM, Okt. 2018, S. 3–10. DOI: 10.1145/3264844.3264845. arXiv: 1808.04684v1. 
- [65] S. Aragon, M. Tiloca, **M. Maass**, M. Hollick und S. Raza. „ACE of Spades in the IoT Security Game: A Flexible Ipcsec Security Profile for Access Control“. In: *Proceedings of the Conference on Communications and Network Security (CNS 2018)*. IEEE Conference on Communications and Network Security. Open Access (arXiv). IEEE, Mai 2018, S. 1–9. DOI: 10.1109/CNS.2018.8433209. arXiv: 1808.04581. 
- [66] T. Bile, **C. Geminn**, O. Grigorjew, C. Husemann, **M. Nebel** und A. Roßnagel. „Fördern und Fordern: Regelungsformen zur Anreizgestaltung für einen wirksameren Schutz von Privatheit und informationeller Selbstbestimmung“. In: *Privatheit und selbstbestimmtes Leben in der digitalen Welt: Interdisziplinäre Perspektiven auf aktuelle Herausforderungen des Datenschutzes*. Springer, 2018.
- [67] **N. Büscher**, D. Demmler, S. Katzenbeisser, D. Kretzmer und T. Schneider. „HyCC: Compilation of Hybrid Protocols for Practical Secure Computation“. In: *25. ACM Conference on Computer and Communications Security (CCS'18)*. Hrsg. von D. Lie, M. Mannan, M. Backes und X. Wang. Conference on Computer and Communications Security. Code: <https://gitlab.com/securityengineering/HyCC>, Open Access (ePrint). Toronto, Canada: ACM, 19. Okt. 2018, S. 847–861. DOI: 10.1145/3243734.3243786. eprint: <https://crypto.de/papers/BDKKS18.pdf>. 
- [68] **N. Büscher**, A. Weber und S. Katzenbeisser. „Towards Practical RAM Based Secure Computation“. In: *Proceedings of the European Symposium on Research in Computer Security (ESORICS 2018)*. Hrsg. von J. López, J. Zhou und M. Soriano. Bd. 11099. Lecture Notes in Computer Science. Springer, 2018, S. 416–437. ISBN: 978-3-319-98988-4. DOI: 10.1007/978-3-319-98989-1_21.
- [69] **C. L. Geminn**, **A. Laubach** und S. Fujiwara. „Das neue Bundesdatenschutzgesetz im Rahmen der Datenschutzgrundverordnung“. In: *Jichi kenkyū, Forschung zur Selbstverwaltung* 12 (2018). (Übersetzung: Prof. Shizuo Fujiwara).
- [70] **N. Gerber**, **P. Gerber**, H. Drews, E. Kirchner, N. Schlegel, T. Schmidt und L. Scholz. „FoxIT: Enhancing Mobile Users' Privacy Behavior by Increasing Knowledge and Awareness“. In: *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust (STAST'17)*. New York, NY, USA: ACM, Dez. 2018, S. 53–63. DOI: 10.1145/3167996.3167999.
- [71] **N. Gerber**, **P. Gerber** und M. Volkamer. „Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior“. In: *Computers & Security* 77 (Aug. 2018), S. 226–261. ISSN: 0167-4048, 1872-6208. DOI: 10.1016/j.cose.2018.04.002.
- [72] **N. Gerber**, B. Reinheimer und M. Volkamer. „Home Sweet Home? Investigating Users' Awareness of Smart Home Privacy Threats“. In: *Proceedings of an Interactive Workshop on the Human Aspects of Smart Home Security and Privacy (WSSP) in Conjunction with the USENIX Symposium on Usable Privacy and Security (SOUPS 2018)*. Internet Society, 2018. URL: <https://publikationen.bibliothek.kit.edu/1000083578>.

- [73] **N. Gerber, V. Zimmermann**, B. Henhapl, S. Emeröz und M. Volkamer. „Finally Johnny Can Encrypt: But Does This Make Him Feel More Secure?“ In: *Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES 2018)*. Hrsg. von S. Doerr, M. Fischer, S. Schrittwieser und D. Herrmann. ARES. New York, NY, USA: ACM, Aug. 2018, 11:1–11:10. ISBN: 978-1-4503-6448-5. DOI: 10.1145/3230833.3230859.
- [74] J. P. Gerlach, **N. Eling, N. Wessels** und P. Buxmann. „Flamingos on a Slackline: Companies’ Challenges of Balancing the Competing Demands of Handling Customer Information and Privacy“. In: *Information Systems Journal* 29.2 (Aug. 2018), S. 548–575. ISSN: 1350-1917. DOI: 10.1111/isj.12222.
- [75] M. Chiglieri, B. Henhapl und **N. Gerber**. „Evaluation der Nutzbarkeit von PGP und S/MIME in Thunderbird“. In: *Proceedings of the Mensch und Computer (MuC 2018)*. Hrsg. von R. Dachsel und G. Weber. Bonn: Gesellschaft für Informatik e.V., 2018, S. 439–447. DOI: 10.18420/muc2018-ws08-0542.
- [76] **T. Grube, J. Daubert** und M. Mühlhäuser. „Asymmetric Dcnets for Effective and Efficient Sender Anonymity“. In: *IEEE Global Communications Conference, GLOBECOM 2018, Abu Dhabi, United Arab Emirates, December 9–13, 2018*. Bd. 297. 2015 IEEE Global Communications Conference (GLOBECOM). IEEE, Dez. 2018, S. 1–7. DOI: 10.1109/GLOCOM.2018.8647607.
- [77] **T. Grube**, F. Volk, M. Mühlhäuser, S. Bhairav, V. Sachidananda und Y. Elovici. „User-Guided Graph Exploration: A Framework for Algorithmic Complexity Reduction in Large Data Sets“. In: *International Journal On Advances in Intelligent Systems* 11 (1 & 2) Juni 2018), S. 68–80. URL: <https://tubiblio.ulb.tu-darmstadt.de/113815/>.
- [78] **I. Heimbach** und O. Hinz. „The Impact of Sharing Mechanism Design on Content Sharing in Online Social Networks“. In: *Information Systems Research* 29.3 (Sep. 2018), S. 592–611. ISSN: 1047-7047.
- [79] F. Karegar, **N. Gerber**, M. Volkamer und S. Fischer-Hübner. „Helping John to Make Informed Decisions on Using Social Login“. In: *Proceedings of the 33rd Annual Symposium on Applied Computing (SAC 2018)*. Hrsg. von H. M. Haddad, R. L. Wainwright und R. Chbeir. ACM Symposium on Applied Computing. Open Access (ePrint). New York, NY, USA: ACM, Apr. 2018, S. 1165–1174. DOI: 10.1145/3167132.3167259. eprint: <https://publikationen.bibliothek.kit.edu/1000083574/14753733>. 
- [80] N. P. Karvelas, **A. Treiber** und S. Katzenbeisser. „Examining Leakage of Access Counts in ORAM Constructions“. In: *Workshop on Privacy in the Electronic Society (WPES)*. Hrsg. von D. Lie, M. Mannan und A. Johnson. WPES@CCS. ACM / ACM, Jan. 2018, S. 66–70. DOI: 10.1145/3267323.3268963.
- [81] **O. Kulyk**, A. Hilt, **N. Gerber** und M. Volkamer. „“This Website Uses Cookies”: Users’ Perceptions and Reactions to the Cookie Disclaimer“. In: *European Workshop on Usable Security (EuroUSEC)*. Open Access. Internet Society, 2018. DOI: 10.14722/eurosec.2018.23012. 
- [82] **O. Kulyk**, P. Mayer, M. Volkamer und O. Käfer. „A Concept and Evaluation of Usable and Fine-Grained Privacy-Friendly Cookie Settings Interface“. In: *Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). Open Access (ePrint). IEEE / IEEE, Aug. 2018, S. 1058–1063. DOI: 10.1109/trustcom/bigdatase.2018.00148. eprint: <https://zenodo.org/records/1488644/files/08456017-2.pdf>. 
- [83] **O. Kulyk** und M. Volkamer. „Usability Is Not Enough: Lessons Learned from ‘human Factors in Security’ Research for Verifiability“. In: *Proceedings of the Joint International Conference on Electronic Voting (e-Vote-ID 2018)*. Bd. 2018. IACR Cryptology ePrint Archive. Springer, 2018, S. 66–81. URL: <https://eprint.iacr.org/2018/683.pdf>.
- [84] **A. Laubach**. „Schutz anonymisierter Daten im japanischen Datenschutzrecht – Kommentierung der neu eingeführten Kategorie der Anonymously Processed Information“. In: *Zeitschrift für Datenschutz – ZD* 9 (Dez. 2018), S. 413–420.
- [85] **A. Laubach**. „Übermittlung personenbezogener Daten in Drittländer“. In: *Das neue Datenschutzrecht – Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze*. Hrsg. von A. Roßnagel. 1. Aufl. Wiesbaden: Nomos, 2018, S. 115–124.

- [86] N. Matyunin, N. A. Anagnostopoulos, **S. Boukoros**, M. Heinrich, A. Schaller, M. Kolinichenko und S. Katzenbeisser. „Tracking Private Browsing Sessions Using CPU-based Covert Channels“. In: *Proceedings of the 11th Conference on Security & Privacy in Wireless and Mobile Networks (WiSec 2018)*. Hrsg. von P. Papadimitratos, K. Butler und C. Pöpper. ACM / ACM, Juni 2018, S. 63–74. DOI: 10.1145/3212480.3212489.
- [87] **M. Nebel**. „Big Data und Datenschutz in der Arbeitswelt, Risiken der Digitalisierung und Abhilfemöglichkeiten“. In: *Zeitschrift für Datenschutz – ZD 11* (2018), S. 520–524.
- [88] A. Roßnagel, T. Bile, M. Friedewald, **C. Geminn**, O. Grigorjew, M. Karaboga und **M. Nebel**. *Nationale Implementierung der Datenschutz-Grundverordnung: Herausforderungen – Ansätze – Strategien*. Policy Paper des Forum Privatheit, Open Access. Zenodo, 1. Jan. 2018. DOI: 10.5281/ZENODO.1184295.
- [89] **K. Shrishak**, **H. Shulman** und M. Waidner. „Removing the Bottleneck for Practical 2PC“. In: *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS 2018)*. Hrsg. von D. Lie, M. Mannan, M. Backes und X. Wang. ACM, Okt. 2018, S. 2300–2302. DOI: 10.1145/3243734.3278521.
- [90] **M. Uhlmann**, **K. Shrishak** und **M. Weiler**. „The Role of the Trust Category for the Development of New Data Protection Approaches“. In: *Proceedings of the Amsterdam Privacy Conference (APC 2018)*. 2018.
- [91] M. Volkamer, K. Renaud, B. Reinheimer, P. Rack, M. Ghiglieri, P. Mayer, A. Kunz und **N. Gerber**. „Developing and Evaluating a Five Minutes Security Awareness Video“. In: *Proceedings of the 15th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2018)*. Regensburg, 2018, S. 119–134.
- [92] **M. Weiler**. „Measuring Real-World Tie Strength with Digital Footprint Data: An Assessment of Convergent Validity“. In: *Proceedings of the International Conference on Information Systems – Bridging the Internet of People, Data, and Things (ICIS 2018)*. Hrsg. von J. Pries-Heje, S. Ram und M. Rosemann. International Conference on Information Systems. Association for Information Systems, Dez. 2018. URL: <https://aisel.aisnet.org/icis2018/social/Presentations/1>.
- [93] **M. Weiler** und O. Hinz. „Without Each Other, We Have Nothing: A State-of-the-Art Analysis on How to Operationalize Social Capital“. In: *Review of Managerial Science* 13.5 (März 2018), S. 1–33. ISSN: 1863-6683. DOI: 10.1007/s11846-018-0280-5.
- [94] **V. Zimmermann**, **N. Gerber**, M. Kleboth, A. von Preuschen, K. Schmidt und P. Mayer. „The Quest to Replace Passwords Revisited – Rating Authentication Schemes“. In: *International Symposium on Human Aspects of Information Security Assurance (HAISA 2018)*. 2018, S. 38–48.
- [95] S. P. Bayerl, F. Brasser, C. Busch, T. Frassetto, P. Jauernig, J. Kolberg, A. Nautsch, K. Riedhammer, A.-R. Sadeghi, T. Schneider, E. Stapf, **A. Treiber** und C. Weinert. *Privacy-Preserving Speech Processing via STPC and TEEs (Poster)*. *Privacy Preserving Machine Learning (PPML'19) – CCS'19 Workshop*. Nov. 2019. URL: <https://tubiblio.ulb.tu-darmstadt.de/115811/>.
- [96] N. Bindel, **J. Brendel**, M. Fischlin, B. Goncalves und D. Stebila. „Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange“. en. In: *Post-Quantum Cryptography*. Hrsg. von J. Ding und R. Steinwandt. Bd. 11505. Lecture Notes in Computer Science. Open Access (ePrint: longer version in iacr.org). Cham: Springer International Publishing, 2019, S. 206–226. ISBN: 978-3-030-25509-1 978-3-030-25510-7. DOI: 10.1007/978-3-030-25510-7_12. eprint: <https://eprint.iacr.org/2018/903.pdf>.
- [97] **J. Brendel**, M. Fischlin und F. Günther. „Breakdown Resilience of Key Exchange Protocols: NewHope, TLS 1.3, and Hybrids“. en. In: *Computer Security – ESORICS 2019*. Hrsg. von K. Sako, S. Schneider und P. Y. A. Ryan. Bd. 11736. Open Access (ePrint). Cham: Springer International Publishing, 2019, S. 521–541. ISBN: 978-3-030-29961-3 978-3-030-29962-0. DOI: 10.1007/978-3-030-29962-0_25. eprint: <https://eprint.iacr.org/2017/1252.pdf>.
- [98] R. Egert, **T. Grube**, D. Born und M. Mühlhäuser. „AVAIN – a Framework for Automated Vulnerability Indication for the IoT in IP-based Networks“. In: *2019 International Conference on Networked Systems, NetSys 2019, Munich, Germany, March 18-21, 2019*. Bd. 10. 2019 International Conference on Networked Systems (NetSys). IEEE, März 2019, S. 1–3. DOI: 10.1109/NETSYS.2019.8854493.
- [99] R. Egert, **T. Grube**, D. Born und M. Mühlhäuser. „Modular Vulnerability Indication for the IoT in IP-based Networks“. In: *2019 IEEE Globecom Workshops, Waikoloa, HI, USA, December 9-13, 2019*. Bd. 10. 2019 IEEE Globecom Workshops (GC Wkshps). IEEE, Dez. 2019, S. 1–6. DOI: 10.1109/GCWKSHPS45667.2019.9024519.

- [100] J. Gedeon, F. Brandherm, R. Egert, **T. Grube** und M. Mühlhäuser. „What the Fog? Edge Computing Revisited: Promises, Applications and Future Challenges“. In: *IEEE access : practical innovations, open solutions* 7 (Okt. 2019). Open Access, S. 152847–152878. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2948399. 
- [101] **N. Gerber**, B. Reinheimer und M. Volkamer. „Investigating People's Privacy Risk Perception“. en. In: *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2019.3 (1. Juli 2019). Open Access, S. 267–288. ISSN: 2299-0984. DOI: 10.2478/popets-2019-0047. 
- [102] K. Keller, K. V. Carl, **H. Jöntgen**, B. M. Abdel-Karim, M. Mühlhäuser und O. Hinz. „KIT, Where Are You?“ Why Smart Assistance Systems in Cars Enrich People's Lives“. In: *Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers*. 2019, S. 1120–1132.
- [103] **O. Kulyk**, **P. Gerber**, **K. Marky**, C. Beckmann und M. Volkamer. „Does This App Respect My Privacy? Design and Evaluation of Information Materials Supporting Privacy-Related Decisions of Smartphone Users“. In: *Proceedings 2019 Workshop on Usable Security*. Workshop on Usable Security. Open Access. San Diego, CA: Internet Society, 2019, S. 1–10. ISBN: 978-1-891562-57-0. DOI: 10.14722/usec.2019.23029. 
- [104] **H. Lurtz** und G. Hornung. „Cyber-physische Systeme zwischen rechtlichen Anforderungen und rechtskonformer Gestaltung“. In: *Handbuch Industrie 4.0 und Digitale Transformation. Betriebswirtschaftliche, technische und rechtliche Herausforderungen* (2019). Hrsg. von R. Obermaier, S. 113–136. DOI: 10.1007/978-3-658-24576-4_5.
- [105] **M. Maass**, S. Schwär und M. Hollick. „Towards Transparency in Email Tracking“. In: *Proceedings of the Annual Privacy Forum (APF 2019)*. Hrsg. von M. Naldi, G. F. Italiano, K. Rannenberg, M. Medina und A. Bourka. Bd. 11498. Annual Privacy Forum. Open Access (ePrint). Springer Science+Business Media, Juni 2019, S. 18–27. ISBN: 978-3-030-21751-8. DOI: 10.1007/978-3-030-21752-5_2. eprint: <https://maass.xyz/publication/maass-2019-b/maass-2019-b.pdf>. 
- [106] **M. Maass**, N. Walter, D. Herrmann und M. Hollick. „On the Difficulties of Incentivizing Online Privacy through Transparency: A Qualitative Survey of the German Health Insurance Market“. In: *Proceedings of the 14. Internationale Tagung Wirtschaftsinformatik*. Hrsg. von T. Ludwig und V. Pipek. University of Siegen, Germany / AISel, 2019.
- [107] P. Mayer, **N. Gerber**, B. Reinheimer, P. Rack, K. Braun und M. Volkamer. „I (Dont) See What You Typed There! Shoulder-surfing Resistant Password Entry on Gamepads“. Englisch. In: *Proceedings of the Conference on Human Factors in Computing Systems (CHI 2019)*. Hrsg. von S. A. Brewster, G. Fitzpatrick, A. L. Cox und V. Kostakos. International Conference on Human Factors in Computing Systems. Open Access (ePrint). ACM, Mai 2019. DOI: 10.1145/3290605.3300779. eprint: <https://publikationen.bibliothek.kit.edu/1000089237/21945031>. 
- [108] C. Meurisch, S. Kauschke, **T. Grube**, B. Bayrak und M. Mühlhäuser. „{P}Net: Privacy-Preserving Personalization of AI-based Models by Anonymous Inter-Person Similarity Networks“. In: *MobiQuitous 2019, Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Houston, Texas, USA, November 12-14, 2019*. Hrsg. von H. V. Poor, Z. Han, D. Pompili, Z. Sun und M. Pan. Bd. 11. International Conference on Mobile and Ubiquitous Systems: Networking and Services. ACM, Nov. 2019, S. 60–69. DOI: 10.1145/3360774.3360819.
- [109] A. Nautsch, A. Jiménez, **A. Treiber**, J. Kolberg, C. Jasserand, E. Kindt, H. Delgado, M. Todisco, M. A. Hmani, A. Mtibaa u. a. „Preserving Privacy in Speaker and Speech Characterisation“. In: *Computer Speech & Language* 58 (Nov. 2019). Open Access, S. 441–480. ISSN: 0885-2308. DOI: 10.1016/j.cs1.2019.06.001. 
- [110] A. Nautsch, J. Patino, **A. Treiber**, T. Stafylakis, P. Mezira, M. Todisco, T. Schneider und N. Evans. „Privacy-Preserving Speaker Recognition with Cohort Score Normalisation“. In: *Annual Conference of the International Speech Communication Association (INTERSPEECH)*. Hrsg. von G. Kubin und Z. Kacic. Interspeech. Open Access. ISCA / ISCA, Sep. 2019, S. 2868–2872. DOI: 10.21437/interspeech.2019-2638. 
- [111] **A. Treiber**, A. Nautsch, J. Kolberg, T. Schneider und C. Busch. „Privacy-Preserving PLDA Speaker Verification Using Outsourced Secure Computation“. In: *Speech Communication* 114 (Nov. 2019). Open Access (ePrint), S. 60–71. ISSN: 0167-6393. DOI: 10.1016/j.specom.2019.09.004. eprint: <https://encrypto.de/papers/TNKS19.pdf>. 

- [112] **M. Uhlmann, F. Pittroff** und J. Lamla. „Vertrauensinfrastrukturen der digitalen Gesellschaft: Vertrauen als Schlüsselkategorie zur Weiterentwicklung des Datenschutzes“. In: Bd. 1. Open Access. vz-nrw (Verbraucherzentrale Nordrhein-Westfalen e. V.), 2019. ISBN: 978-3-86336-921-7. DOI: 10.15501/978-3-86336-922-4_2. 
- [113] **A. Wainakh, T. Grube, J. Daubert** und M. Mühlhäuser. „Efficient Privacy-Preserving Recommendations Based on Social Graphs“. In: *Proceedings of the 13th ACM Conference on Recommender Systems, RecSys*. Hrsg. von T. Bogers, A. Said, P. Brusilovsky und D. Tikk. Bd. 1215. ACM, Sep. 2019, S. 78–86. DOI: 10.1145/3298689.3347013.
- [114] **A. Wainakh, T. Grube, J. Daubert**, C. Porth und M. Mühlhäuser. „Tweet beyond the Cage: A Hybrid Solution for the Privacy Dilemma in Online Social Networks“. In: *2019 IEEE Global Communications Conference (GLOBECOM)*. 2019 IEEE Global Communications Conference (GLOBECOM). IEEE / IEEE, Dez. 2019, S. 1–6. DOI: 10.1109/globecom38437.2019.9013901.
- [115] **N. Wessels, A. Laubach** und P. Buxmann. „Personenbezogene Daten in der digitalen Ökonomie – Eine wirtschaftliche und juristische Betrachtung“. In: *Die Zukunft der Datenökonomie: Gestaltungsperspektiven zwischen Geschäftsmodellen, Kollektivgut und Verbraucherschutz*. Hrsg. von M. Friedewald, **C. Ochs**, T. Hess und J. Lamla. Springer, 2019, S. 11–27. ISBN: 978-3-658-27510-5. DOI: 10.1007/978-3-658-27511-2_2.
- [116] **N. Wessels, A. Wagner**, J. Prakash Sarswat und P. Buxmann. „What Is Your Selfie Worth? A Field Study on Individuals' Valuation of Personal Data“. In: *Proceedings of the 14th International Conference on Wirtschaftsinformatik*. Hrsg. von T. Ludwig und V. Pipek. Publications of Darmstadt Technical University, Institute for Business Studies (BWL). University of Siegen, Germany / AISEL, Jan. 2019, S. 1322–1336. URL: <https://ideas.repec.org/p/dar/wpaper/110641.html>.
- [117] **T. Grube**, A. Heinrich, J.-P. Stroscher und S. Schomberg. „Datensicherheit von Corona-Apps nach der DSGVO“. In: *Datenschutz und Datensicherheit - DuD* 44.8 (Juli 2020). Open Access, S. 501–505. ISSN: 1614-0702. DOI: 10.1007/S11623-020-1314-0. 
- [118] **H. Jöntgen**. „Fueling the Firestorm: Effects of Social Capital on Users' Persuasiveness during Online Firestorms“. In: *Proceedings of the 28th European Conference on Information Systems (ECIS)*. Hrsg. von F. Rowe, R. E. Amrani, M. Limayem, S. Newell, N. Pouloudi, E. van Heck und A. E. Quammah. European Conference on Information Systems. 2020.
- [119] **D. Müllmann**. „Brauchen wir ein Recht auf „digitalen Herdenschutz“? – Die Gefahren kommerziellen Profilings für die pluralistische Demokratie und gesellschaftliche Minderheiten“. In: *Der digitalisierte Staat - Chancen und Herausforderungen für den modernen Staat*. Hrsg. von R. Greve, B. Gwiasda, T. Kemper, J. Moir, S. Müller, A. Schönberger, S. Stöcker, J. Wagner und L. Wolff. Open Access. Nomos Verlagsgesellschaft mbH & Co. KG, 2020, S. 129–152. ISBN: 978-3-7489-0749-7. DOI: 10.5771/9783748907497-129. 
- [120] T. Schneider und **A. Treiber**. „A Comment on Privacy-Preserving Scalar Product Protocols as Proposed in “SPOC”“. In: *IEEE Transactions on Parallel and Distributed Systems (TPDS)* 31 (März 2020). Open Access (arXiv), S. 543–546. ISSN: 1045-9219. DOI: 10.1109/tpds.2019.2939313. arXiv: 1906.04862. 
- [121] **T. Schürmann** und P. Beckerle. „Personalizing Human-Agent Interaction through Cognitive Models“. In: *Frontiers in Psychology* 11 (Sep. 2020). Open Access, S. 561510. ISSN: 1664-1078. DOI: 10.3389/fpsyg.2020.561510. 
- [122] **A. Stöver**, F. Kretschmer, C. Cornel und **K. Marky**. „Work in Progress: How i Met My Privacy Assistant—a User-Centric Workshop“. In: *Mensch Und Computer 2022-Workshopband*. Hrsg. von C. Hansen, A. Nürnberger und B. Preim. Mensch & Computer Workshopband. Gesellschaft für Informatik eV, Sep. 2020. DOI: 10.18420/muc2020-ws119-005.
- [123] **A. Treiber**, A. Molina, C. Weinert, T. Schneider und K. Kersting. „CryptoSPN: Expanding PPML beyond Neural Networks“. In: *Privacy Preserving Machine Learning in Practice (PPMLP'20) – CCS'20 Workshop*. Hrsg. von B. Zhang, R. A. Popa, M. Zaharia, G. Gu und S. Ji. PPMLP@CCS. Open Access (arXiv). ACM / ACM, Nov. 2020. DOI: 10.1145/3411501.3419417. arXiv: 2002.00801. 
- [124] **A. Treiber**, A. Molina, C. Weinert, T. Schneider und K. Kersting. „CryptoSPN: Privacy-preserving Sum-Product Network Inference“. In: *European Conference on Artificial Intelligence (ECAI)*. Hrsg. von G. De Giacomo, A. Catalá, B. Dilkina, M. Milano, S. Barro, A. Bugarin und J. Lang. Open Access. IOS Press, Feb. 2020. DOI: 10.3233/faia200313. arXiv: 2002.00801. 

- [125] **A. Wainakh**, A. S. Guinea, **T. Grube** und M. Mühlhäuser. „Enhancing Privacy via Hierarchical Federated Learning“. In: *2020 IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*. Open Access (arXiv). Genoa, Italy: IEEE Computer Society, Sep. 2020, S. 344–347. DOI: 10.1109/eurospw51379.2020.00053. arXiv: 2004.11361. 
- [126] A. Borchert, **A. Wainakh**, N. Krämer, M. Mühlhäuser und M. Heisel. „Mitigating Privacy Concerns by Developing Trust-Related Software Features for a Hybrid Social Media Application“. In: *ENASE*. Hrsg. von R. Ali, H. Kaindl und L. A. Maciaszek. International Conference on Evaluation of Novel Approaches to Software Engineering. Open Access. SCITEPRESS - Science and Technology Publications, 2021, S. 269–280. DOI: 10.5220/0010450302690280. 
- [127] R. Egert, **T. Grube**, F. Volk und M. Mühlhäuser. „Holonic System Model for Resilient Energy Grid Operation“. In: *Energies* 14.4120 (14 Juli 2021). Open Access, S. 4120. ISSN: 1996-1073. DOI: 10.3390/en14144120. 
- [128] M. Fischlin und **O. Sanina**. „Cryptographic Analysis of the Bluetooth Secure Connection Protocol Suite“. In: *Advances in Cryptology—ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part II*. Hrsg. von M. Tibouchi und H. Wang. Bd. 13091. International Conference on the Theory and Application of Cryptology and Information Security. Open Access (ePrint). Berlin, Heidelberg: Springer-Verlag, 2021, S. 696–725. ISBN: 978-3-030-92074-6. DOI: 10.1007/978-3-030-92075-3_24. eprint: <https://eprint.iacr.org/2021/1597>. 
- [129] **M. Gazzari**, A. Mattmann, **M. Maass** und M. Hollick. „My(o) Armband Leaks Passwords: An EMG and IMU Based Keylogging Side-Channel Attack“. Englisch. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5.4 (27. Dez. 2021). Open Access (arXiv), S. 1–24. ISSN: 2474-9567. DOI: 10.1145/3494986. arXiv: 2112.02382. 
- [130] **T. Grube**, R. Egert, M. Mühlhäuser und **J. Daubert**. „The Cost of Path Information: Routing in Anonymous Communication“. In: *18th IEEE Annual Consumer Communications & Networking Conference, CCNC 2021, Las Vegas, NV, USA, January 9-12, 2021*. Consumer Communications and Networking Conference. IEEE, Jan. 2021, S. 1–6. DOI: 10.1109/CCNC49032.2021.9369639.
- [131] S. Linsner, F. Kuntke, **E. Steinbrink**, J. Franken und C. Reuter. „The Role of Privacy in Digitalization – Analysing the German Farmers’ Perspective“. In: *Proceedings on Privacy Enhancing Technologies (PoPETs) 2021.3* (Apr. 2021). Open Access, S. 334–350. ISSN: 2299-0984. DOI: 10.2478/popets-2021-0050. 
- [132] **M. Maass**, **A. Stöver**, H. Pridöhl, **S. Bretthauer**, D. Herrmann, M. Hollick und I. Spiecker gen. Döhmman. „Effective Notification Campaigns on the Web: A Matter of Trust, Framing, and Support“. In: *30th USENIX Security Symposium (USENIX Security 21)*. Hrsg. von M. Bailey und R. Greenstadt. USENIX Security Symposium. Open Access. USENIX Association, Aug. 2021, S. 2489–2506. ISBN: 978-1-939133-24-3. URL: <https://www.usenix.org/system/files/sec21-maass.pdf>. 
- [133] **D. Müllmann** und M. Volkamer. „Meldepflicht von IT-Sicherheits- und Datenschutzvorfällen durch Mitarbeitende – Betrachtung möglicher arbeitsrechtlicher Konsequenzen“. In: *Zeitschrift für Datenschutz - ZD*. Bd. 11. 1. 1. Jan. 2021, S. 8–12.
- [134] **D. Müllmann** und M. Volkamer. „Meldepflicht von IT-Sicherheits- und Datenschutzvorfällen durch Mitarbeitende – Betrachtung möglicher arbeitsrechtlicher Konsequenzen“. In: *50. Jahrestagung der Gesellschaft für Informatik, INFORMATIK 2020, Back to the Future*. Hrsg. von H. Reussner Koziolk. Bd. P-307. GI-Jahrestagung. GI, 2021, S. 829–840. DOI: 10.18420/inf2020_74.
- [135] L. Pumplun, **M. Fecho**, N. Wahl-Islam und P. Buxmann. „Machine Learning Systems in Clinics—How Mature Is the Adoption Process in Medical Diagnostics?“ In: *Proceedings of the 54th Hawaii International Conference on System Sciences*. Open Access. Hamilton Library, University of Hawaii at Mānoa, Honolulu, 2021, S. 1–10. DOI: 10125/71382. 
- [136] L. Pumplun, **M. Fecho**, N. Wahl-Islam, F. Peters und P. Buxmann. „Adoption of Machine Learning Systems for Medical Diagnostics in Clinics: Qualitative Interview Study“. In: *Journal of Medical Internet Research*. Bd. 23. Journal of Medical Internet Research 10. Open Access. JMIR Publications Inc., Okt. 2021, e29301. DOI: 10.2196/29301. 
- [137] **K. Shrishak** und **H. Shulman**. „Privacy Preserving and Resilient RPKI“. In: *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*. IEEE Conference on Computer Communications. Open Access (arXiv). IEEE, Mai 2021, S. 1–10. DOI: 10.1109/INFOCOM42981.2021.9488759. arXiv: 2102.02456. 

- [138] **E. Steinbrink**, L. Reichert, M. Mende und C. Reuter. „Digital Privacy Perceptions of Asylum Seekers in Germany - An Empirical Study about Smartphone Usage during the Flight“. In: *Proceedings of the ACM: Human Computer Interaction (PACM): Computer-Supported Cooperative Work and Social Computing 5 (CSCW2 Okt. 2021)*, S. 1–24. ISSN: 2573-0142. DOI: 10.1145/3479526.
- [139] **A. Stöver**, **N. Gerber**, S. Kaushik, M. Mühlhäuser und **K. Marky**. „Investigating Simple Privacy Indicators for Supporting Users When Installing New Mobile Apps“. In: *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. Hrsg. von Y. Kitamura, A. Quigley, K. Isbister und T. Igarashi. Bd. 25. CHI Extended Abstracts. ACM, Mai 2021, S. 1–7. DOI: 10.1145/3411763.3451791.
- [140] T. Sturm, **M. Fecho** und P. Buxmann. „To Use or Not to Use Artificial Intelligence? A Framework for the Ideation and Evaluation of Problems to Be Solved with Artificial Intelligence“. In: *Proceedings of the 54th Hawaii Conference on System Sciences*. Open Access. Hamilton Library, University of Hawaii at Mānoa, Honolulu, Jan. 2021, S. 1–10. DOI: 10125/70634. 
- [141] **A. Wainakh**, T. Müßig, **T. Grube** und M. Mühlhäuser. „Label Leakage from Gradients in Distributed Machine Learning“. In: *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*. Consumer Communications and Networking Conference. IEEE / IEEE, Jan. 2021, S. 1–4. DOI: 10.1109/ccnc49032.2021.9369498.
- [142] **A. Wainakh**, A. Strassheim, **T. Grube**, **J. Daubert** und M. Mühlhäuser. „Enabling Privacy-Preserving Rule Mining in Decentralized Social Networks“. In: *The 16th International Conference on Availability, Reliability and Security*. Hrsg. von D. Reinhardt und T. Müller. Bd. 32. Proceedings of the 17th International Conference on Availability, Reliability and Security. ACM, Aug. 2021, S. 1–11. DOI: 10.1145/3465481.3465482.
- [143] **E. Zimmer**, C. Burkert und H. Federrath. „Insiders Dissected: New Foundations and a Systematisation of the Research on Insiders“. Englisch. In: *Digital Threats: Research and Practice 3.1 (Okt. 2021)*. Open Access, S. 1–35. ISSN: 2692-1626, 2576-5337. DOI: 10.1145/3473674. 
- [144] **A. Zöll**, C. M. Olt und P. Buxmann. „Privacy-Sensitive Business Models: Barriers of Organizational Adoption of Privacy Enhancing Technologies“. In: *European Conference on Information Systems (ECIS 2021)*. Hrsg. von F. Rowe, R. E. Amrani, M. Limayem, S. Matook, C. Rosenkranz, E. A. Whitley und A. E. Quammah. European Conference on Information Systems. Marrakesh, Morocco, 14. Juni 2021. URL: https://aisel.aisnet.org/ecis2021_rp/34/.
- [145] A. Borchert, **A. Wainakh**, N. Krämer, M. Mühlhäuser und M. Heisel. „The Relevance of Privacy Concerns, Trust, and Risk for Hybrid Social Media“. In: *Communications in Computer and Information Science (CCIS)*. International Conference on Evaluation of Novel Approaches to Software Engineering. Springer International Publishing / Springer, 2022, S. 88–111. ISBN: 978-3-030-96647-8. DOI: 10.1007/978-3-030-96648-5_5.
- [146] **A. Brüggemann**, M. Breuer, A. Klinger, T. Schneider und U. Meyer. „Secure Maximum Weight Matching Approximation on General Graphs“. In: *Proceedings of the 21st Workshop on Privacy in the Electronic Society (WPES'22)*. Hrsg. von Y. Hong und L. Wang. Bd. 1. IACR Cryptology ePrint Archive. Open Access (ePrint). Association for Computing Machinery, Nov. 2022, S. 83–87. DOI: 10.1145/3559613.3563209. eprint: <https://ia.cr/2022/1173>. 
- [147] **A. Brüggemann**, T. Schneider, A. Suresh und H. Yalame. „Poster: Efficient Three-Party Shuffling Using Precomputation“. In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS'22)*. Hrsg. von H. Yin, A. Stavrou, C. Cremers und E. Shi. Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. Association for Computing Machinery, Nov. 2022, S. 3331–3333. DOI: 10.1145/3548606.3563511.
- [148] L. Buhleier, S. Linsner, **E. Steinbrink** und C. Reuter. „Eine Klassifikation sicherheitskritischer UX-Design-Patterns“. In: *Mensch und Computer 2022 - Workshopband (Sep. 2022)*. Hrsg. von **K. Marky**, U. Grünefeld und T. Kosch. Open Access. DOI: 10.18420/muc2022-mci-ws10-275. 
- [149] V. Eitle, **A. Zöll** und P. Buxmann. „Organizational Readiness Concept for AI: A Quantitative Analysis of a Multi-Stage Adoption Process from the Perspective of Data Scientists“. In: *30th European Conference on Information Systems - New Horizons in Digitally United Societies, ECIS 2022, Timisoara, Romania, June 18-24, 2022*. Hrsg. von R. Beck, D. Petcu, M. Fotache, S. Matook, R. Helms, M. Wiener, L. Rusu und T. Tuunanen. European Conference on Information Systems. Timisoara, Romania, 2022. URL: https://aisel.aisnet.org/ecis2022_rp/30/.

- [150] **M. Fecho** und J. Wiefel. „Trust Transfer toward Automated Vehicles: The Role of Vendor’s Innovativeness“. In: *26th Pacific Asia Conference on Information Systems, PACIS*. 2022.
- [151] **H. Jöntgen**. „Appreciating Support-Antecedents of Subscription-Based Crowdfunding Campaign Success.“ In: *Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS)*. Open Access. Hamilton Library, University of Hawaii at Mānoa, Honolulu, 2022, S. 1–10. DOI: 10.1257/79431.
- [152] S. Kamara, A. Kati, T. Moataz, T. Schneider, **A. Treiber** und M. Yonli. „SoK: Cryptanalysis of Encrypted Search with LEAKER - a Framework for Leakage Attack Evaluation on Real-World Data“. In: *IEEE European Symposium on Security and Privacy (EuroS&P)*. European Symposium on Security and Privacy. Open Access. IEEE / IEEE, Juni 2022, S. 90–108. DOI: 10.1109/eurosp53844.2022.00014.
- [153] K. Keller, **H. Jöntgen**, B. M. Abdel-Karim und O. Hinz. „User Cognition Antecedents of Smart Assistant Systems in Cars“. In: *IEEE transactions on intelligent transportation systems* 24.1 (Dez. 2022), S. 37–53. ISSN: 1524-9050. DOI: 10.1109/tits.2022.3216029.
- [154] F. Kuntke, S. Linsner, **E. Steinbrink**, J. Franken und C. Reuter. „Resilience in Agriculture: Communication and Energy Infrastructure Dependencies of German Farmers“. In: *International Journal of Disaster Risk Science* 13.2 (März 2022). Open Access, S. 214–229. ISSN: 2095-0055. DOI: 10.1007/s13753-022-00404-7.
- [155] F. Kuntke, V. Romanenko, S. Linsner, **E. Steinbrink** und C. Reuter. „LoRaWAN Security Issues and Mitigation Options by the Example of Agricultural IoT Scenarios“. In: *Transactions on Emerging Telecommunications Technologies* 33.5 (Jan. 2022). Open Access, e4452. ISSN: 2161-3915. DOI: 10.1002/ett.4452.
- [156] S. Linsner, **E. Steinbrink**, F. Kuntke, J. Franken und C. Reuter. „Supporting Users in Data Disclosure Scenarios in Agriculture through Transparency“. In: *Behaviour & Information Technology (BIT)* 41.10 (Mai 2022), S. 2137–2159. ISSN: 0144-929X. DOI: 10.1080/0144929X.2022.2068070.
- [157] L. Pumplun, **A. Wagner**, C. M. Olt, **A. Zöll** und P. Buxmann. „Acting Egoistically in a Crisis: How Emotions Shape Data Donations“. In: *Proceedings of the 55th Hawaii International Conference on System Sciences*. Open Access. Virtual, Maui, Hawaii: Hamilton Library, University of Hawaii at Mānoa, Honolulu, 2022, S. 1–10. DOI: 10.1257/79828.
- [158] **A. Stöver**, **N. Gerber**, C. Cornel, M. Henz, **K. Marky**, **V. Zimmermann** und J. Vogt. „Website Operators Are Not the Enemy Either-Analyzing Options for Creating Cookie Consent Notices without Dark Patterns“. In: *Mensch Und Computer 2022-Workshopband*. Hrsg. von **K. Marky**, U. Grünefeld und T. Kosch. Message Understanding Conference. Gesellschaft für Informatik e.V., 2022. DOI: 10.18420/muc2022-mci-ws01-458.
- [159] **A. Treiber**, **D. Müllmann**, T. Schneider und I. Spiecker gen. Döhmman. „Data Protection Law and Multi-Party Computation: Applications to Information Exchange between Law Enforcement Agencies“. In: *21. Workshop on Privacy in the Electronic Society (WPES’22)*. Hrsg. von Y. Hong und L. Wang. Bd. 202. IACR Cryptology ePrint Archive. Open Access (ePrint). Los Angeles, CA, USA: ACM, 7. Nov. 2022, S. 69–82. DOI: 10.1145/3559613.3563192. eprint: <https://ia.cr/2022/1242>.
- [160] **A. Wainakh**, F. Ventola, T. Müßig, J. Keim, C. G. Cordero, **E. Zimmer**, **T. Grube**, K. Kersting und M. Mühlhäuser. „User-Level Label Leakage from Gradients in Federated Learning“. In: *Proceedings on Privacy Enhancing Technologies (PoPETs) 2022.2* (März 2022). Open Access, S. 227–244. ISSN: 2299-0984. DOI: 10.2478/popets-2022-0043.
- [161] **A. Wainakh**, **E. Zimmer**, S. Subedi, J. Keim, **T. Grube**, S. Karuppayah, A. Sanchez Guinea und M. Mühlhäuser. „Federated Learning Attacks Revisited: A Critical Discussion of Gaps, Assumptions, and Evaluation Setups“. In: *Sensors* 23.1 (20. Dez. 2022). Open Access, S. 31. ISSN: 1424-8220. DOI: 10.3390/s23010031.
- [162] **A. Zöll**, V. Eitle und P. Buxmann. „Machine Learning Adoption Based on the TOE Framework: A Quantitative Study“. In: *Pacific Asia Conference on Information Systems (PACIS 2022)*. Hrsg. von M.-H. Huang, G. Gable, C. M. K. Cheung und D. Xu. Pacific Asia Conference on Information Systems. Taipei (virtual), 5. Juli 2022, S. 131. URL: <https://aisel.aisnet.org/pacis2022/131/>.
- [163] **A. Zöll**, **A. Wagner** und M. Reuter-Oppermann. „Giving Users Control over How Peers Handle Their Data: A Design Science Study“. In: *ICIS 2022: Digitization for the next Generation*. Hrsg. von N. Bjørn-Andersen, R. Beck, S. Petter, T. B. Jensen, T. Böhmman, K. L. Hui und V. Venkatesh. International Conference on Interaction Sciences. Copenhagen, Denmark: Association for Information Systems, 9. Dez. 2022. URL: <https://aisel.aisnet.org/icis2022/security/security/3/>.

- [164] **A. Brüggemann**, R. Hundt, T. Schneider, A. Suresh und H. Yalame. „FLUTE: Fast and Secure Lookup Table Evaluations“. In: *2023 IEEE Symposium on Security and Privacy (S&P'23)*. IEEE Symposium on Security and Privacy. Open Access (ePrint). IEEE Computer Society, Mai 2023, S. 515–533. DOI: 10.1109/SP46215.2023.10179345. eprint: <https://eprint.iacr.org/2023/499.pdf>. 
- [165] P. Buxmann und **A. Zöll**. „Ökonomische Effekte von ChatGPT“. In: *Controlling & Management Review* 67.5 (Okt. 2023), S. 16–21. ISSN: 2195-8262. DOI: 10.1007/s12176-023-1066-4.
- [166] D. Dittert, T. Schneider und **A. Treiber**. „Too Close for Comfort? Measuring Success of Sampled-Data Leakage Attacks against Encrypted Search“. In: *Cloud Computing Security Workshop (CCSW)*. Bd. 30. IACR Cryptology ePrint Archive. Open Access (ePrint). ACM / ACM, Nov. 2023, S. 3–15. DOI: 10.1145/3605763.3625243. eprint: <https://ia.cr/2023/1465>. 
- [167] **M. Fecho** und N. Wahl. „Organizational Adoption of Green Artificial Intelligence: An Institutional Perspective“. In: *27th Pacific Asia Conference on Information Systems, PACIS*. Hrsg. von P. Chau, J. Jing, M. T. Siponen, A. Burton-Jones, C.-H. Tan und B. S. Xiao. Pacific Asia Conference on Information Systems. 2023, S. 142. URL: <https://aisel.aisnet.org/pacis2023/142>.
- [168] **M. Fecho** und **A. Zöll**. „The Power of Trust: Designing Trustworthy Machine Learning Systems in Healthcare“. In: *International Conference on Information Systems*. Hrsg. von R. De', S. Paul, S. Sarker, V. K. Tuunainen, W. D. Fernández, J. Nandhakumar und R. Santhanam. International Conference on Interaction Sciences. Association for Information Systems, 2023.
- [169] M. Gräf, **A. Zöll**, N. Wahl, S. Ellenrieder, F. Hager, T. Sturm und O. Vetter. „Designing the Organizational Metaverse for Effective Socialization“. In: *PACIS 2023 Proceedings*. Hrsg. von P. Chau, J. Jing, M. T. Siponen, A. Burton-Jones, C.-H. Tan und B. S. Xiao. Nanchang, China, 8. Juli 2023. URL: <https://aisel.aisnet.org/pacis2023/46/>.
- [170] **P. Hendriks**, T. Sturm, C. M. Olt und P. Buxmann. „The Impact of Human-Artificial Intelligence Partnerships on Organizational Learning“. In: *Proceedings of the 31st European Conference on Information Systems*. Hrsg. von M. Aanestad, S. Klein, M. Tarafdar, S. Han, S. Laumer und I. Ramos. European Conference on Information Systems. Kristiansand, 2023, S. 359. URL: https://aisel.aisnet.org/ecis2023_rp/359.
- [171] A. Khalil, **A. Wainakh**, **E. Zimmer**, J. Parra-Arnau, A. F. Anta, T. Meuser und R. Steinmetz. „Label-Aware Aggregation for Improved Federated Learning“. In: *2023 Eighth International Conference on Fog and Mobile Edge Computing (FMEC)*. International Conference on Fog and Mobile Edge Computing. IEEE / IEEE, Sep. 2023, S. 216–223. DOI: 10.1109/fmec59375.2023.10306055.
- [172] M. F. Mehler, M. Turan Akdag und **A. Zöll**. „Exploring the Effect of National Culture on Emerging Technologies: A Glimpse into the Future“. In: *PACIS 2023 Proceedings*. Hrsg. von P. Chau, J. Jing, M. T. Siponen, A. Burton-Jones, C.-H. Tan und B. S. Xiao. Pacific Asia Conference on Information Systems. Nanchang, China, 8. Juli 2023, S. 12. URL: <https://aisel.aisnet.org/pacis2023/12/>.
- [173] M. Omerovic Smajlovic, **A. Zöll** und A. Rami. „Building Sustainable Business Practices: Design Principles for Reusable Artificial Intelligence“. In: *Wirtschaftsinformatik 2023 Proceedings*. Wirtschaftsinformatik. Paderborn, Germany: AISel, 18. Sep. 2023, S. 55. URL: <https://aisel.aisnet.org/wi2023/55/>.
- [174] T. Panahi und **L. Seyda**. „KI-generierte Fakes - Wem müssen wir jetzt vertrauen? Herstellung und Schutz von Vertrauen in und Vertrauenswürdigkeit von Informationen im Schatten von ChatGPT & Co“. In: *Das IT-Recht vor der (europäischen) Zeitenwende?* Hrsg. von A. K. Bernzen, J. Fritzsche, C. Heinze und O. Thomsen. Okt. 2023, S. 459–482. ISBN: 978-3-95599-077-0.
- [175] **E. Steinbrink**, **T. Biselli**, S. Linsner, F. Herbert und C. Reuter. „Privacy Perception and Behaviour in Safety-Critical Environments“. In: *Human Factors in Privacy Research*. Hrsg. von **N. Gerber**, **A. Stöver** und **K. Marky**. Open Access. Cham: Springer International Publishing, 2023, S. 237–251. ISBN: 978-3-031-28643-8. DOI: 10.1007/978-3-031-28643-8_12. 
- [176] **A. Stöver**, **N. Gerber**, H. Pridöhl, **M. Maass**, **S. Bretthauer**, I. Spiecker gen. Döhmman, M. Hollick und D. Herrmann. „How Website Owners Face Privacy Issues: Thematic Analysis of Responses from a Covert Notification Study Reveals Diverse Circumstances and Challenges“. In: *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2023.2 (Apr. 2023). Open Access, S. 251–264. ISSN: 2299-0984. DOI: 10.56553/popets-2023-0051. 

- [177] **A. Stöver, S. Hahn**, F. Kretschmer und **N. Gerber**. „Investigating How Users Imagine Their Personal Privacy Assistant“. In: *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2023.2 (Apr. 2023). Open Access, S. 384–402. ISSN: 2299-0984. DOI: 10.56553/popets-2023-0059. 
- [178] O. Vetter, T. Sturm, **M. Fecho** und P. Buxmann. „Machine Learning Developments as Stimuli for Organizational Learning“. In: *International Conference on Information Systems*. Hrsg. von R. De', S. Paul, S. Sarker, V. K. Tuunainen, W. D. Fernández, J. Nandhakumar und R. Santhanam. Association for Information Systems, 2023.
- [179] J. Witte, K. Gao und **A. Zöll**. „Artificial Intelligence: The Future of Sustainable Agriculture? A Research Agenda“. In: *Proceedings of the 56th Hawaii International Conference on System Sciences*. Hrsg. von T. X. Bui. Open Access. Maui, Hawaii: Hamilton Library, University of Hawaii at Mānoa, Honolulu, 2023, S. 733–742. DOI: 10.125/102722. 
- [180] K. Bauer, **R. Heigl**, O. Hinz und M. Kosfeld. „Feedback Loops in Machine Learning: A Study on the Interplay of Continuous Updating and Human Discrimination“. In: *Journal of The Association for Information Systems* 25.4 (2024), S. 9. ISSN: 1536-9323. DOI: 10.17705/1jais.00853.
- [181] **A. Brüggemann**, O. Schick, T. Schneider, A. Suresh und H. Yalame. „Don't Eject the Impostor: Fast Three-Party Computation with a Known Cheater“. In: 45. *IEEE Symposium on Security and Privacy (IEEE S&P'24)*. Bd. ab-s/2112.13338. IEEE Symposium on Security and Privacy. Open Access. San Francisco, CA, USA: IEEE, 23. Mai 2024, S. 503–522. DOI: 10.1109/SP54263.2024.00164. eprint: <https://ia.cr/2023/1744>. 
- [182] P. Buxmann, A. Glauben und **P. Hendriks**. „Die Nutzung von ChatGPT in Unternehmen: Ein Fallbeispiel zur Neugestaltung von Serviceprozessen“. In: *HMD Praxis der Wirtschaftsinformatik* 61.2 (Apr. 2024). Open Access, S. 436–448. ISSN: 1436-3011. DOI: 10.1365/s40702-024-01053-8. 
- [183] S. Ellenrieder, N. Ellenrieder, **P. Hendriks** und M. Mehler. „Pilots and Pixels : A Comparative Analysis of Machine Learning Error Effects on Aviation Decision Making“. In: *Proceedings of the 32nd European Conference on Information Systems*. European Conference on Information Systems. 2024, S. 1366. URL: https://aisel.aisnet.org/ecis2024/track06_humanaicollab/track06_humanaicollab/6.
- [184] **M. Fecho**, A. von Ahsen, N. Wahl und V. Oliver. „Paving the Way to a Green Future with Artificial Intelligence – Exploring Organizational Adoption Factors“. In: *Proceedings of the 57th Hawaii International Conference on System Sciences*. Hrsg. von T. X. Bui. Open Access. Hamilton Library, University of Hawaii at Mānoa, Honolulu, 2024, S. 821–830. DOI: 10.125/70634. 
- [185] M. Fischlin und **O. Sanina**. „Fake It till You Make It: Enhancing Security of Bluetooth Secure Connections via Deferrable Authentication“. In: *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security, October 14–18, 2024*. Ccs '24. New York, NY, USA: Association for Computing Machinery, 2024. ISBN: 979-8-4007-0636-3. DOI: 10.1145/3658644.3670360.
- [186] A. Glauben, **A. Zöll**, B. Sharma und F. Kristo. „The Dialog Trap: Exploring Potentially Detrimental Effects of Dialog-Based Interfaces for Generative AI Content Creation“. In: *Proceedings of the Pacific-Asia Conference on Information System*. Hrsg. von T. Q. Phan, B. C. Y. Tan, H. S. Le, N. H. Thuan, M. Chau und K.-Y. Goh. Ho Chi Minh City, Vietnam, 7. Jan. 2024. URL: https://aisel.aisnet.org/pacis2024/track01_aibussoc/track01_aibussoc/15/.
- [187] M. Gräf, **A. Zöll** und N. Wahl. „Navigating Virtual Frontiers: The Willingness of Virtual Teams to Use the Metaverse“. In: *Proceedings of European Conference on Information Systems*. Paphos, Cyprus, 13. Juni 2024. URL: https://aisel.aisnet.org/ecis2024/track24_socialmedia/track24_socialmedia/12/.
- [188] **S. Hahn**, N. Al-Amrani, S. Allagah, H. R. Huang, E. Kircher, C. Rehs, J. Vogt, **K. Marky** und **N. Gerber**. „How to Respect Bystanders' Privacy in Smart Homes - A Co-Creation Study“. en. In: *Nordic Conference on Human-Computer Interaction*. NordiCHI 2024: Nordic Conference on Human-Computer Interaction. Bd. 79. Nordic Conference on Human-Computer Interaction. Uppsala Sweden: ACM, 13. Okt. 2024, S. 1–19. ISBN: 9798400709661. DOI: 10.1145/3679318.3685340.
- [189] **F. Hapsari**, R. I. Stemler und S. Pieschl. „Trust Resilience in Pedagogical Agents: Will Anthropomorphism Help Against Trust Decline?“ In: *Proceedings of the Annual Meeting of the Cognitive Science Society* 46.0 (2024). Open Access. URL: <https://escholarship.org/uc/item/3bz0w09k> (besucht am 10. 01. 2025). 

- [190] **R. M. Heigl**, P. Weber und O. Hinz. „The TikTok Equation: How Congruence Drives Influencer Marketing Success—a Mixed-Methods Study“. In: *ECIS 2024 Proceedings*. European Conference on Information Systems. 2024. URL: https://aisel.aisnet.org/ecis2024/track24_socialmedia/track24_socialmedia/3/.
- [191] **P. Hendriks**, C. M. Olt, T. Sturm und C. C. Moos. „Exploring Team Collaboration in the Metaverse from a Human Capital Perspective“. In: *Journal of Intellectual Capital* 25.4 (Juli 2024), S. 686–710. ISSN: 1469-1930. DOI: 10.1108/JIC-02-2024-0055.
- [192] **P. Hendriks**, T. Sturm, M. Geis, T. Grimminger und B. Mast. „Exploring Collaboration in Human-Artificial Intelligence Teams: A Design Science Approach to Team-AI Collaboration Systems Completed Research Paper“. In: *Proceedings of the Pacific Asia Conference on Information Systems*. 2024, S. 1408. URL: https://aisel.aisnet.org/pacis2024/track08_digtech_fow/track08_digtech_fow/1.
- [193] P. H. Jacquemin, M. Gräf, **P. Hendriks** und N. Wahl. „Beyond the Screen : Developing Design Principles and Nudges for Enhancing Virtual Team Collaboration in the Metaverse“. In: *Proceedings of the Pacific Asia Conference on Information Systems*. Hrsg. von T. Q. Phan, B. C. Y. Tan, H. S. Le, N. H. Thuan, M. Chau und K.-Y. Goh. Pacific Asia Conference on Information Systems. 2024, S. 1559.
- [194] **H. Jöntgen**, N. V. Lingnau, O. Hinz und R. Holten. „This Is Why We Pay—Motivational Factors for Supporting Subscription-Based Crowdfunding Campaigns“. In: *Electronic Markets* 34.1 (Apr. 2024). Open Access, S. 1–21. ISSN: 1019-6781. DOI: 10.1007/s12525-024-00710-6.
- [195] S. Kamara, A. Kati, T. Moataz, J. DeMaria, A. Park und **A. Treiber**. „MAPLE: MARKov Process Leakage Attacks on Encrypted Search“. In: *Proceedings on Privacy Enhancing Technologies (PoPETs) 2024* (Jan. 2024). Open Access, S. 430–446. ISSN: 2299-0984. DOI: 10.56553/popets-2024-0025.
- [196] C. M. Olt, **P. Hendriks**, T. Sturm und C. C. Moos. „From Avatars to Allies: Exploring Team Collaboration in the Metaverse“. In: *Proceedings of the 57th Hawaii International Conference on System Sciences*. Hrsg. von T. X. Bui. Hawaii International Conference on System Sciences. Open Access. Hawaii International Conference on System Sciences, 2024, S. 4921–4930. ISBN: 978-0-9981331-7-1. DOI: 10.1255/106974.
- [197] **L. Seyda**, **A. Brüggemann**, G. Hornung und T. Schneider. „Multi-Party Computation als Instrument zur Umsetzung datenschutzkonformer behördlicher Datenabgleiche - Eine interdisziplinäre Analyse am Beispiel der Diskussionen um das Gesetz zur Selbstbestimmung über den Geschlechtseintrag“. In: *Recht und Technik: Datenschutz im Diskurs (RuT'24)*. Hrsg. von M. Klein, D. Krupka, C. Winter, M. Gergeleit und L. Martin. Bd. P-352. Jahrestagung der Gesellschaft für Informatik. Open Access. LNI, Gesellschaft für Informatik, 2024, S. 153–167. DOI: 10.18420/inf2024_11.
- [198] **E. Steinbrink** und C. Reuter. „The Impact of Transparency and Trust on User Acceptance of Contact Tracing Apps: Implications for the Adoption of Crisis Response Apps“. In: *International Journal of Disaster Risk Reduction* 112 (Juli 2024). Open Access, S. 104661. ISSN: 2212-4209. DOI: 10.1016/j.ijdr.2024.104661.
- [199] **A. Stöver**, **S. Hahn**, **S. Althaus**, **E. Zimmer** und **N. Gerber**. „Wie stellen sich Nutzende ihren Privatsphäre-Assistenten vor?“ In: *Datenschutz und Datensicherheit - DuD* 48.10 (Okt. 2024), S. 633–636. ISSN: 1862-2607. DOI: 10.1007/s11623-024-1991-1.
- [200] P. Weber, **R. M. Heigl** und L. Baum. „Understanding (X)AI in Healthcare: Patients' Perspective on Global and Local Explanations“. In: *28th Pacific Asia Conference on Information Systems, PACIS 2024, Ho Chi Minh City, Vietnam, July 1-5, 2024*. Hrsg. von T. Q. Phan, B. C. Y. Tan, H.-S. Le, N. H. Thuan, M. Chau und K. Y. Goh. Pacific Asia Conference on Information Systems. 2024. URL: https://aisel.aisnet.org/pacis2024/track11_healthit/track11_healthit/10.
- [201] **A. Zöll**, V. Eitle und **P. Hendriks**. „Uncovering Cultural Differences in Organizational Readiness for Artificial Intelligence: A Comparison between Germany and the United States“. In: *Proceedings of the 57th Hawaii International Conference on System Sciences*. Hrsg. von T. X. Bui. Open Access. Hawaii, USA: Hamilton Library, University of Hawaii at Mānoa, Honolulu, 3. Jan. 2024, S. 787–798. URL: https://aisel.aisnet.org/hicss-57/c1/distributed_collaboration/6/.
- [202] **S. Gaballah**, L. Abdullah, **E. Zimmer**, S. Fahl, M. Mühlhäuser und **K. Marky**. „It's Not My Data Anymore": Exploring Non-Users' Privacy Perceptions of Medical Data Donation Apps“. In: *Proceedings on Privacy Enhancing Technologies*. 2025.

Weitere Publikationen und öffentlich gemachte Ergebnisse

- [203] **I. Heimbach**, J.-Y. Kim u. a. *The Effects of Monetary Incentives on Word of Mouth Generation*. Darmstadt Technical University, Department of Business Administration, 2016. URL: <https://ideas.repec.org/p/dar/wpaper/84845.html>.
- [204] **A. Laubach**, C. Barlag, S. Blazy, **C. Geminn**, J. Hofmann, C. Hohmann, D. Hoidn, **S. Jandt**, P. C. Johannes, N. Maier, K. Marschall, J. Müller, **M. Nebel**, V. Ossoinig, **P. Richter**, F. Schaller und R. Weinhold. „Arbeitshilfe zur Datenschutz - Grundverordnung – Synopse der deutschen Übersetzung der DSGVO in der Entwurfsfassung vom 28. Januar 2016 zur Verkündeten Fassung“. In: *ITeG Technical Report Nr. 4*. Hrsg. von A. Roßnagel. Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG) an der Universität Kassel, 2016.
- [205] **E. Vasilomanolakis**. „On Collaborative Intrusion Detection“. Diss. Technische Universität Darmstadt, Germany, Juli 2016, S. 1–205.
- [206] **M. Maass**. *Code RED: Freie Software auf WLAN-Routern und Smartphones unter Beschuss*. Open Access. 2017. URL: <https://netzpolitik.org/2017/code-red-funkabschottung-rueckt-naeher-unklarheit-bleibt/>. 
- [207] **T. Grube**. „Efficient Anonymous Group Communication“. Diss. Technische Universität Darmstadt, Germany, 2018. URL: <http://tuprints.ulb.tu-darmstadt.de/7704/>.
- [208] **A. Laubach**. „1st Interdisciplinary Workshop on Privacy and Trust (iPAT 2018)“. In: *Zeitschrift für Datenschutz aktuell - ZDaktuell* 14 (Sep. 2018). 06253.
- [209] **A. Laubach** und M. Dräger. „Brasilien: Neues Datenschutzgesetz“. In: *Zeitschrift für Datenschutz aktuell - ZDaktuell* 14 (Sep. 2018). 06254.
- [210] A. Taha, **S. Boukoros**, J. Luna, S. Katzenbeisser und N. Suri. „QRES: Quantitative Reasoning on Encrypted Security Slas“. In: *Cryptology ePrint Archive* abs/1804.04426 (Apr. 2018). Open Access (arXiv), S. 1–29. ISSN: 2331-8422. DOI: 10.48550/arxiv.1804.04426. arXiv: 1804.04426. 
- [211] **S. Boukoros**, M. Humbert, S. Katzenbeisser und C. Troncoso. „Why Johnny Can't Develop Mobile Crowdsourcing Applications with Location Privacy“. In: *arXiv preprint* (2019). Open Access (arXiv). arXiv: 1901.04923. 
- [212] **H. Lurtz**. „Angriff der (privaten) Drohnen - Die Privatsphäre schießt zurück!“ In: *Zeitschrift für Datenschutz aktuell - ZDaktuell* (2019).
- [213] **H. Lurtz** und S. Schindler. „Gemeinsame Verantwortlichkeit des Websitebetreibers bei Social-Plug-ins“. In: *VuR* (2019). Anmerkung zu EuGH, Urteil vom 29.07.2019 - C-40/17.
- [214] **H. Lurtz** und S. Schomberg. „Pflicht zur Benennung eines Datenschutzbeauftragten“. In: *Zeitschrift für Datenschutz aktuell - ZDaktuell* (2019).
- [215] **D. Müllmann**. „Unpatchable? - Der gesetzliche Umgang mit von menschlichem Verhalten ausgehenden Risiken für die IT-Sicherheit kritischer Infrastrukturen“. In: *Die Macht der Daten und der Algorithmen - Regulierung von IT, IoT und KI*. Hrsg. von J. Taeger. 2019, S. 245–260.
- [216] **A. Stöver**. *Ongoing Research: Trust in Automation in the Context of Privacy*. Posterbeitrag im Rahmen des 15. Symposium on Usable Privacy and Security (SOUPS), Santa Clara, CA, USA. 2019.
- [217] **N. Wessels**. „Eine ökonomische Analyse des Wertes von Privatsphäre und personenbezogener Daten aus Unternehmens- und Nutzerperspektive“. Diss. Dez. 2019. DOI: 10.25534/tuprints-00009476.
- [218] R. Cammarota, M. Schunter, A. Rajan, F. Boemer, Á. Kiss, **A. Treiber**, C. Weinert, T. Schneider, E. Stapf, A.-R. Sadeghi u. a. „Trustworthy AI Inference Systems: An Industry Research View“. In: *Intel Technical Report*. Bd. abs/2008.04449. arXiv (Cornell University). Open Access (arXiv). Cornell University / Intel AI, Aug. 2020. DOI: 10.48550/arxiv.2008.04449. arXiv: 2008.04449. 
- [219] **D. Müllmann**, A. Ebert und **L. Reissner**. „Homeland Security Act vs. BSIG - Eine rechtsvergleichende Betrachtung der IT-Sicherheit kritischer Infrastrukturen in den USA und Deutschland“. In: *Den Wandel begleiten - IT-Rechtliche Herausforderungen der Digitalisierung*. Hrsg. von J. Taeger. 2020, S. 459–473. URL: <https://publikationen.bibliothek.kit.edu/1000124708>.

- [220] **D. Müllmann**, A. Ebert und **L. Reissner**. „IT-Sicherheitsgesetz 2.0 und das Vorbild USA“. In: *Computer & Recht*. Bd. 35. Computer und Recht 9. Verlag Dr. Otto Schmidt, 15. Sep. 2020, S. 584–592. DOI: 10.9785/cr-2020-360910.
- [221] **D. Müllmann** und H. Thomas. „Der Wille zur Beibehaltung der Vorratsdatenspeicherung - Zugleich Kommentar zu BVerwG, Beschluss vom 25.9.2019 - 6 C 12.18, K&R 2019, 819 ff.“ In: *Kommunikation & Recht*. Bd. 23. 2. 2. Jan. 2020, S. 103–105.
- [222] **A. Wainakh**, A. S. Guinea, **T. Grube** und M. Mühlhäuser. „Enhancing Privacy via Hierarchical Federated Learning“. In: *CoRR abs/2004.11361* (Apr. 2020). Open Access (arXiv). arXiv: 2004.11361. URL: <https://arxiv.org/abs/2004.11361>. 
- [223] M. Fischlin und **O. Sanina**. *Cryptographic Analysis of the Bluetooth Secure Connection Protocol Suite*. Hrsg. von M. Tibouchi und H. Wang. Cryptology ePrint Archive. Open Access (ePrint). 2021. eprint: <https://eprint.iacr.org/2021/1597>. 
- [224] **M. Gazzari**, A. Mattmann, **M. Maass** und M. Hollick. *Myo Keylogging Dataset*. Open Access. European Organization for Nuclear Research, Nov. 2021. DOI: 10.5281/zenodo.5594651. 
- [225] **D. Müllmann**, E. Schomakers und e. al. „Insights on Data Sensitivity from the Technical, Legal and the Users' Perspective“. In: *Computer Law Review International*. Bd. 17. 1. 2021, S. 8–15.
- [226] **L. Seyda**. „Das Gesetz zum Autonomen Fahren“. In: *Zeitschrift für Datenschutz aktuell - ZDaktuell* (2021), S. 0536. URL: <https://beck-online-1beck-1de-1y3moak261419.han-ub.uni-kassel.de/Bcid/Y-300-Z-ZDAKTUELL-B-2021-N-0536>.
- [227] **A. Wainakh**, F. Ventola, T. Müßig, J. Keim, C. G. Cordero, **E. Zimmer**, **T. Grube**, K. Kersting und M. Mühlhäuser. „User Label Leakage from Gradients in Federated Learning“. In: *CoRR abs/2105.09369* (Mai 2021). Open Access (arXiv). ISSN: 2331-8422. arXiv: 2105.09369. 
- [228] **A. Wainakh**, F. Ventola, T. Müßig, J. Keim, C. G. Cordero, **E. Zimmer**, **T. Grube**, K. Kersting und M. Mühlhäuser. „User Label Leakage from Gradients in Federated Learning“. In: *CoRR abs/2105.09369* (Mai 2021). Open Access (arXiv). ISSN: 2331-8422. arXiv: 2105.09369. 
- [229] **A. Wainakh**, F. Ventola, T. Müßig, J. Keim, C. G. Cordero, **E. Zimmer**, **T. Grube**, K. Kersting und M. Mühlhäuser. „User Label Leakage from Gradients in Federated Learning“. In: *CoRR abs/2105.09369* (Mai 2021). Open Access (arXiv). ISSN: 2331-8422. arXiv: 2105.09369. 
- [230] **S. Althaus**. *Empowering Users through Technical Transparency*. Juni 2022. URL: https://www.cybercrime.fau.de/files/2022/06/poster_simon_althaus.pdf.
- [231] **S. Althaus**. „User Empowerment through Technical Transparency“. In: *Proceedings of the 2022 Joint Workshop of the German Research Training Groups in Computer Science*. Hrsg. von F. Freiling und H. Seidl. Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), 31. Mai 2022. DOI: 10.25593/opus4-fau-19321.
- [232] **M. Gazzari** und A. Mattmann. *Myo Keylogging Source Code*. Secure Mobile Networking Lab, 10. Jan. 2022. URL: <https://github.com/seemoo-lab/myo-keylogging> (besucht am 26. 08. 2024).
- [233] **H. Jöntgen**. „Usage of Social Capital in Digital Collectives“. Diss. Johann Wolfgang Goethe-Universität Frankfurt am Main, 2022.
- [234] **D. Müllmann** und M. Maas. „Online Evidence Collector - Ein Onlinetool zur vereinfachten Nutzung elektronischer Beweise in Prozessen“. In: *Zeitschrift für das gesamte Verfahrensrecht*. Bd. 5. 2. 2. Jan. 2022, S. 1–17.
- [235] **D. Müllmann** und I. Spiecker gen. Döhmman. „Extra DSGVO nulla salus? - Zur weiteren Zulässigkeit nicht akkreditierter Datenschutzsiegel neben akkreditierten Gütesiegeln im Sinne der Art. 42 f. DSGVO“. In: *Deutsches Verwaltungsblatt*. Bd. 137. 4. 15. Feb. 2022, S. 208–214.
- [236] L. Pumplun, **A. Wagner**, T. Störzinger, **M. Fecho**, P. Buxmann und C. Misselhorn. *Empowering Citizen Science through Digital Technologies: New Participatory Approaches to Data Collection, Sharing, and Analysis*. Hrsg. von **K. Marky**, U. Grünefeld und T. Kosch. Workshop Veröffentlichung: Mensch und Computer 22: Facing Realities, Darmstadt. Gesellschaft für Informatik e.V., 2022. DOI: 10.18420/muc2022-mci-ws05-111.

- [237] T. Setz und **L. Seyda**. „Der Umgang der EU mit Propaganda und Desinformation russischer Staatsmedien in Zeiten des Ukrainekriegs“. In: *Zeitschrift für Datenschutz aktuell - ZDaktuell* 8 (2022), S. 01167. URL: <https://beck-online-1beck-1de-1y3moak261419.han.ub.uni-kassel.de/Bcid/Y-300-Z-ZDAKTUELL-B-2022-N-01167>.
- [238] **L. Seyda** und F. Böning. „Sicherheitslücken bei der Praxissoftware „InSuite““. In: *Zeitschrift für Datenschutz aktuell - ZDaktuell* (2022), S. 01327. URL: <https://beck-online-1beck-1de-1y3moak261419.han.ub.uni-kassel.de/Bcid/Y-300-Z-ZDAKTUELL-B-2022-N-01327>.
- [239] **L. Seyda** und P. Zurawski. „Die Nutzung hochpreisiger Endgeräte als Anfangsverdacht – EncroChat“. In: *Zeitschrift für Datenschutz aktuell - ZDaktuell* (2022), S. 01168. URL: <https://beck-online-1beck-1de-1y3moak261419.han.ub.uni-kassel.de/Bcid/Y-300-Z-ZDAKTUELL-B-2022-N-01168>.
- [240] **V. Zimmermann, P. Gerber** und **A. Stöver**. *That Depends—Assessing User Perceptions of Authentication Schemes across Contexts of Use*. arXiv preprint. Open Access (arXiv). Cornell University, Sep. 2022. DOI: 10.48550/arXiv.2209.13958. arXiv: 2209.13958. 
- [241] **S. Althaus**. „User Empowerment through Technical Transparency“. In: *Proceedings of the 2023 Joint Workshop of the German Research Training Groups in Computer Science*. Hrsg. von H. Seidl und C. Seifert. Open Access. Universität Duisburg-Essen (UDE), 4. Mai 2023. DOI: 10.17185/dupublico/78280. 
- [242] **A. Brüggemann**, T. Schneider, A. Suresh und H. Yalame. *Is Everyone Equally Trustworthy in Practice? (Short Talk)*. 2023 IEEE Symposium on Security and Privacy (S&P'23) Short Talks. 2023. URL: <https://sp2023.ieee-security.org/program-shorttalks.html>.
- [243] **F. Müller**. „Social Media und das algorithmische Streben nach „Vertrauenswürdigkeit““. In: *Daten-Fairness in einer globalisierten Welt*. Hrsg. von M. Friedewald, A. Roßnagel, R. Neuburger, F. Bieker und G. Hornung. Bd. 2. Open Access. Nomos Verlagsgesellschaft: Baden-Baden, 2023, S. 275–284. ISBN: 978-3-7489-3874-3. DOI: 10.5771/9783748938743-275. 
- [244] **L. Seyda** und L. Pfeiffer. „Fünf Jahre DS-GVO: Informationsvisualisierung – Quo Vadis?“ In: *Zeitschrift für Datenschutz aktuell - ZDaktuell* 01230 (2023). URL: <https://beck-online-1beck-1de-1y3moak261419.han.ub.uni-kassel.de/Bcid/Y-300-Z-ZDAKTUELL-B-2023-N-01230>.
- [245] **L. Seyda** und P. Zurawski. „BMJ: Referentenentwurf zur „Quick Freeze“-Regelung als unionsrechtskonforme Alternative zur Vorratsdatenspeicherung“. In: *Zeitschrift für Datenschutz aktuell - ZDaktuell* (2023), S. 01055. URL: <https://beck-online-1beck-1de-1y3moak261419.han.ub.uni-kassel.de/Bcid/Y-300-Z-ZDAKTUELL-B-2023-N-01055>.
- [246] **L. Seyda** und P. Zurawski. „Frankreich: Verdächtiges Signal – Die Kriminalisierung der Nutzung verschlüsselter Kommunikation“. In: *Zeitschrift für Datenschutz aktuell - ZDaktuell* (2023), S. 01361. URL: <https://beck-online-1beck-1de-1y3moak261419.han.ub.uni-kassel.de/Bcid/Y-300-Z-ZDAKTUELL-B-2023-N-01361>.
- [247] **A. Stöver**. „Untersuchung des Beitrags von Webseitenbetreibenden zur Entstehung und Behebung von Privatsphärenrisiken“. Diss. Darmstadt, Germany: Technische Universität Darmstadt, 2023. DOI: 10.26083/tuprints-00024110.
- [248] M. Fischlin und **O. Sanina**. *Fake It till You Make It: Enhancing Security of Bluetooth Secure Connections via Deferrable Authentication*. Cryptology ePrint Archive. Open Access (ePrint). 2024. eprint: <https://eprint.iacr.org/2024/874>. 
- [249] **M. Gazzari**. *Seemoo-Lab/Pyshimmer*. Secure Mobile Networking Lab, 12. Aug. 2024. URL: <https://github.com/seemoo-lab/pyshimmer> (besucht am 26. 08. 2024).
- [250] **L. Seyda** und T. Panahi. „Das neue Grundgesetz für das Digitalzeitalter? – Der DSA und seine Effektivität gegen Desinformation“. In: *Zeitschrift für Datenschutz aktuell - ZDaktuell* (2024), S. 01564. URL: <https://beck-online-1beck-1de-1y3moak261419.han.ub.uni-kassel.de/Bcid/Y-300-Z-ZDAKTUELL-B-2024-N-01564>.
- [251] **L. Seyda** und P. Zurawski. „Glatteis für „Quick Freeze“ – schon überholt von Hessen und dem EuGH?“ In: *Zeitschrift für Datenschutz aktuell - ZDaktuell* (2024), S. 01696. URL: <https://beck-online-1beck-1de-1y3moak261419.han.ub.uni-kassel.de/Bcid/Y-300-Z-ZDAKTUELL-B-2024-N-01696>.

5.1.2. Projektergebnisse der Doktorandinnen und Doktoranden sowie ggf. der Postdoktorandinnen und Postdoktoranden (anderweitig finanziert)

Die nachfolgende Auflistung der Projektergebnisse, an denen anderweitig finanzierte (Post-)Doktorandinnen und (Post-)Doktoranden (ggf. maßgeblicher) beteiligt waren, ist sortiert nach dem jeweiligen Erscheinungsjahr. Alle am Kolleg beteiligten (Post-)Doktorandinnen und (Post-)Doktoranden sind hervorgehoben. Open-Access-Publikationen sind mit einem Symbol  am Seitenrand markiert.

Publikationen mit wissenschaftlicher Qualitätssicherung

- [252] **J. Classen**, J. Braun, F. Volk, M. Hollick, J. Buchmann und M. Mühlhäuser. „A Distributed Reputation System for Certification Authority Trust Management“. In: *Proceedings of the Trustcom/BigDataSE/ISPA*. Bd. 1. Trust, Security And Privacy In Computing And Communications. IEEE / IEEE, Aug. 2015, S. 1349–1356. DOI: 10.1109/trustcom.2015.529.
- [253] **J. Classen**, J. Chen, D. Steinmetzer, M. Hollick und E. Knightly. „The Spy next Door: Eavesdropping on High Throughput Visible Light Communications“. In: *Proceedings of the 2nd International Workshop on Visible Light Communications Systems*. Hrsg. von C. Peng und S. Mangold. VLCS@MobiCom. ACM / ACM, Sep. 2015, S. 9–14. DOI: 10.1145/2801073.2801075.
- [254] **J. Classen**, M. Schulz und M. Hollick. „Practical Covert Channels for WiFi Systems“. In: *Proceedings of the Conference on Communications and Network Security (CNS 2015)*. IEEE Conference on Communications and Network Security. Open Access (arXiv). IEEE / IEEE, Sep. 2015, S. 209–217. DOI: 10.1109/cns.2015.7346830. arXiv: 1505.01081. 
- [255] **J. Daubert**, **T. Grube**, M. Mühlhäuser und M. Fischer. „Internal Attacks in Anonymous Publish-Subscribe P2P Overlays“. In: *2015 International Conference and Workshops on Networked Systems, NetSys 2015, Cottbus, Germany, March 9-12, 2015*. Bd. 33. Networked Systems. IEEE Computer Society, März 2015, S. 1–8. DOI: 10.1109/NetSys.2015.7089074.
- [256] **J. Daubert**, A. Wiesmaier und P. Kikiras. „A View on Privacy & Trust in IoT“. In: *IEEE International Conference on Communication, ICC 2015, London, United Kingdom, June 8-12, 2015, Workshop Proceedings*. Bd. 1. 2015 IEEE International Conference on Communication Workshop (ICCW). IEEE, Juni 2015, S. 2665–2670. DOI: 10.1109/ICCW.2015.7247581.
- [257] S. Funke, **J. Daubert**, A. Wiesmaier, P. Kikiras und M. Mühlhäuser. „End-2-End Privacy Architecture for IoT“. In: *2015 IEEE Conference on Communications and Network Security, CNS 2015, Florence, Italy, September 28-30, 2015*. Bd. 2. IEEE Conference on Communications and Network Security. IEEE, Sep. 2015, S. 705–706. DOI: 10.1109/CNS.2015.7346895.
- [258] **C. Geminn** und A. Roßnagel. „‚Privatheit‘ und ‚Privatsphäre‘ aus der Perspektive des Rechts – ein Überblick“. In: *JuristenZeitung* 70.14 (2015), S. 703–708. ISSN: 0022-6882. DOI: 10.1628/002268815x14346427046980.
- [259] **C. L. Geminn**. „Die Debatte um nationales Routing – Eine Scheindebatte“. In: *Multimedia und Recht (MMR)* 18.2 (2015), S. 98–103.
- [260] **P. Gerber** und M. Volkamer. „Usability und Privacy im Android Ökosystem“. In: *Datenschutz und Datensicherheit - DuD* 39.2 (Feb. 2015), S. 108–113. ISSN: 1614-0702. DOI: 10.1007/s11623-015-0375-y.
- [261] **P. Gerber**, M. Volkamer und K. Renaud. „Usability versus Privacy Instead of Usable Privacy: Google’s Balancing Act between Usability and Privacy“. In: *Acm Sigcas Computers and Society* 45.1 (Feb. 2015), S. 16–21. DOI: 10.1145/2738210.2738214.
- [262] J. Gerlach, **T. Widjaja** und P. Buxmann. „Handle with Care: How Online Social Network Providers’ Privacy Policies Impact Users’ Information Sharing Behavior“. In: *The Journal of Strategic Information Systems* 24.1 (März 2015), S. 33–43. ISSN: 0963-8687. DOI: 10.1016/j.jsis.2014.09.001.
- [263] **S. M. Habib**, F. Volk, **S. Hauke** und M. Mühlhäuser. „Computational Trust Methods for Security Quantification in the Cloud Ecosystem“. In: *The Cloud Security Ecosystem* Syngress/Elsevier (Juni 2015). Hrsg. von R. K. L. Ko und K.-K. R. Choo, S. 463–493. DOI: 10.1016/b978-0-12-801595-7.00021-5.

- [264] T. Hasan, P. Kikiras, A. Leonardi, H. Ziekow und **J. Daubert**. „Cloud-Based IoT Analytics for the Smart Grid: Experiences from a 3-Year Pilot“. In: *Proceedings of the 10th EAI International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities*. Bd. 1. EAI Endorsed Trans. Cloud Systems 2. Open Access. ACM, Aug. 2015, e2. DOI: 10.4108/icst.tridentcom.2015.259694.
- [265] H. Krasnova, **T. Widjaja**, P. Buxmann, **H. Wenninger** und I. Benbasat. „Why Following Friends Can Hurt You: An Exploratory Investigation of the Effects of Envy on Social Networking Sites among College-Age Users“. In: *Information Systems Research* 26.3 (2015), S. 585–605.
- [266] **J. Kropf**. „Konsekrationsinstanzen im digitalen Wandel – Beiträge zur Erweiterung des feldanalytischen Forschungsprogramms am Beispiel populärer Musik“. In: *Berliner Journal für Soziologie* 25.4 (Dez. 2015), S. 429–458. ISSN: 0863-1808. DOI: 10.1007/s11609-016-0298-y.
- [267] S. Maseberg, E. Bodden, M. Kus, A. Brucker, S. Rasthofer, B. Berger, S. Huber, K. Sohr, **P. Gerber** und M. Volkamer. „Zertifizierte Apps“. In: *Risiken Kennen, Herausforderungen Annehmen, Lösungen Gestalten, Tagungsband 14. Deutscher IT-Sicherheitskongress des BSI 2015*. SecuMedia, Jan. 2015, S. 505–516. URL: <http://tubiblio.ulb.tu-darmstadt.de/104199/>.
- [268] D. Steinmetzer, J. Chen, **J. Classen**, E. Knightly und M. Hollick. „Eavesdropping with Periscopes: Experimental Security Analysis of Highly Directional Millimeter Waves“. In: *Proceedings of the Conference on Communications and Network Security (CNS)*. IEEE Conference on Communications and Network Security. IEEE / IEEE, Sep. 2015, S. 335–343. DOI: 10.1109/cns.2015.7346844.
- [269] F. Bieker, **B. Büttner** und M. Karaboga. „Smart Cars Cruising on the Road Paved with Good Intentions? – Workshop on Big Data Applications and Individual Rights under the New European General Data Protection Regulation“. In: *Privacy and Identity Management*. Hrsg. von A. Lehmann, D. Whitehouse, S. Fischer-Hübner, L. Fritsch und C. Raab. Bd. 498. Open Access. Cham: Springer International Publishing, Aug. 2016, S. 59–75. ISBN: 978-3-319-55783-0. DOI: 10.1007/978-3-319-55783-0_6.
- [270] H. Brakemeier, **T. Widjaja** und P. Buxmann. „Calculating with Different Goals in Mind - the Moderating Role of the Regulatory Focus in the Privacy Calculus“. In: *24th European Conference on Information Systems (ECIS 2016)*. RePEc: Research Papers in Economics. AIS eLibrary, Juni 2016, 124:1–124:18. URL: <https://econpapers.repec.org/RePEc%3Aadar%3Awpaper%3A81225>.
- [271] H. Brakemeier, **T. Widjaja** und P. Buxmann. „Distinguishing Usage and Disclosure Intentions in Privacy Research: How Our Two Selves Bring about Differences in the Effects of Benefits and Risks“. In: *24th European Conference on Information Systems (ECIS 2016)*. RePEc: Research Papers in Economics. Federal Reserve Bank of St. Louis, Juni 2016, 144:1–144:18. URL: <https://econpapers.repec.org/RePEc%3Aadar%3Awpaper%3A81224>.
- [272] **J. Classen**, D. Steinmetzer und M. Hollick. „Opportunities and Pitfalls in Securing Visible Light Communication on the Physical Layer“. In: *Proceedings of the 3rd Workshop on Visible Light Communication Systems*. Hrsg. von X. Zhou und C. P. Yue. VLCS '16. ACM / ACM, Okt. 2016, S. 19–24. DOI: 10.1145/2981548.2981551.
- [273] T. Dai, **H. Shulman** und M. Waidner. „DNSSEC Misconfigurations in Popular Domains“. In: *Proceedings of the International Conference on Cryptology and Network Security (CANS 2016)*. Hrsg. von S. Foresti und G. Persiano. Bd. 10052. Springer, 2016, S. 651–660. ISBN: 978-3-319-48964-3. DOI: 10.1007/978-3-319-48965-0_43.
- [274] **J. Daubert**, M. Fischer, **T. Grube**, S. Schiffner, P. Kikiras und M. Mühlhäuser. „AnonPubSub: Anonymous Publish-Subscribe Overlays“. In: *Computer Communications* 76 (Feb. 2016), S. 42–53. ISSN: 0140-3664. DOI: 10.1016/j.comcom.2015.11.004.
- [275] **J. Daubert**, **T. Grube**, M. Mühlhäuser und M. Fischer. „On the Anonymity of Privacy-Preserving Many-to-Many Communication in the Presence of Node Churn and Attacks“. In: *13th IEEE Annual Consumer Communications & Networking Conference, CCNC 2016, Las Vegas, NV, USA, January 9-12, 2016*. Consumer Communications and Networking Conference. IEEE, Jan. 2016, S. 738–744. DOI: 10.1109/CCNC.2016.7444871.
- [276] A. Engelbrecht, J. Gerlach und **T. Widjaja**. „Understanding the Anatomy of Data-Driven Business Models – towards an Empirical Taxonomy“. In: *24th European Conference on Information Systems (ECIS 2016)*. European Conference on Information Systems. 2016, Research Paper 128.

- [277] A. Feldmann, P. Heyder, M. Kreutzer, S. Schmid, J.-P. Seifert, **H. Shulman**, K. Thimmaraju, M. Waidner und J. Sieberg. „NetCo: Reliable Routing with Unreliable Routers“. In: *46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-w 2016)*. IEEE Computer Society, Juni 2016, S. 128–135. DOI: 10.1109/dsn-w.2016.38.
- [278] M. Fischlin, A. Herzberg, H. Bin-Noon und **H. Shulman**. „Obfuscation Combiners“. In: *Proceedings of the Annual International Cryptology Conference (CRYPTO 2016)*. Hrsg. von M. Robshaw und J. Katz. Bd. 9815. Springer, 2016, S. 521–550. ISBN: 978-3-662-53007-8. DOI: 10.1007/978-3-662-53008-5_18.
- [279] M. Gassen und **H. Simo**. „Towards Privacy-Preserving Mobile Location Analytics“. In: *Proceedings of the International Conference on Extending Database Technology (EDBT/ICDT Workshops 2016)*. Hrsg. von T. Palpanas und K. Stefanidis. Bd. 1558. CEUR Workshop Proceedings, 2016.
- [280] **C. Geminn**. „Demokratie zwischen Öffentlichkeit und Privatheit“. In: *Verwaltungsarchiv* 107.4 (Jan. 2016), S. 601–630. ISSN: 2366-1992. DOI: 10.1515/verwarch-2016-0405.
- [281] **C. L. Geminn**. „Das Smart Home als Herausforderung für das Datenschutzrecht“. In: *Datenschutz und Datensicherheit - DuD* 40.9 (Aug. 2016), S. 575–580. ISSN: 1614-0702. DOI: 10.1007/s11623-016-0661-3.
- [282] **S. M. Habib**, J. Vassileva, S. Mauw und M. Mühlhäuser, Hrsg. *Proceedings of the IFIPTM: IFIP International Conference on Trust Management (Trust Management X)*. Bd. IFIP AICT 473. Springer, Juli 2016.
- [283] A. Herzberg, **H. Shulman** und M. Waidner. „Stratum Filtering: Cloud-based Detection of Attack Sources“. In: *Proceedings of the CCSW*. Hrsg. von E. R. Weippl, S. Katzenbeisser, M. Payer, S. Mangard, E. Androulaki und M. K. Reiter. ACM, 2016, S. 47–48. DOI: 10.1145/2996429.2996440.
- [284] **J. Kropf**. „Zur Konsekration populärer Musik im publizistischen Diskurs und im Bildungswesen“. In: *Kulturkritik und das Populäre in der Musik* (2016), S. 151–175.
- [285] **O. Kulyk**, **K. Marky**, S. Neumann und M. Volkamer. „Introducing Proxy Voting to Helios“. In: *Proceedings of 11th International Conference on Availability, Reliability and Security (ARES 2016)*. Open Access (ePrint). IEEE Computer Society, Aug. 2016, S. 98–106. DOI: 10.1109/ares.2016.38. eprint: <https://kau.diva-portal.org/smash/get/diva2:1138743/FULLTEXT01>. 
- [286] **K. Marky**, A. Gutmann, P. Rack und M. Volkamer. „Privacy Friendly Apps-Making Developers Aware of Privacy Violations“. Englisch. In: *Proceedings of the 1st International Workshop on Innovations in Mobile Privacy and Security, (IMPS 2016), Co-Located with the International Symposium on Engineering Secure Software and Systems (ESSoS 2016)*. Hrsg. von D. Aspinall, L. Cavallaro, M. N. Seghir und M. Volkamer. Bd. 1575. Engineering Secure Software and Systems. CEUR Workshop Proceedings, Apr. 2016, S. 46–48. URL: https://ceur-ws.org/Vol-1575/paper_4.pdf.
- [287] **C. Ochs**, **F. Pittroff**, **B. Büttner** und J. Lamla. „Governing the Internet in the Privacy Arena“. In: *Internet Policy Review* 5.3 (Sep. 2016). Open Access, S. 2. ISSN: 2197-6775. DOI: 10.14763/2016.3.426. 
- [288] M. Pfeiffer, J.-P. Kwirotek, **J. Classen**, R. Klose und M. Hollick. „Analyzing TETRA Location Privacy and Network Availability“. In: *Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices*. Hrsg. von L. Lu und M. Mannan. ACM / ACM, Okt. 2016, S. 117–122. DOI: 10.1145/2994459.2994463.
- [289] **P. Richter**. „Big Data“. In: *Handbuch Medien- und Informationsethik*. Hrsg. von J. Heesen. Springer, 2016, S. 210–216. ISBN: 978-3-476-02557-9. DOI: 10.1007/978-3-476-05394-7_28.
- [290] **P. Richter**. „Big Data, Statistik und die Datenschutz-Grundverordnung“. In: *Datenschutz und Datensicherheit - DuD* 40.9 (Aug. 2016), S. 581–586. ISSN: 1614-0702. DOI: 10.1007/s11623-016-0662-2.
- [291] **P. Richter**. „Instrumente zwischen rechtlicher Steuerung und technischer Entwicklung“. In: *Datenschutz und Datensicherheit - DuD* 40.2 (Feb. 2016), S. 89–93. ISSN: 1614-0702. DOI: 10.1007/s11623-016-0552-7.
- [292] A. Rossnagel und **P. Richter**. „Big Data and Informational Self-Determination. Regulative Approaches in Germany: The Case of Police and Intelligence Agencies“. In: *Exploring the Boundaries of Big Data*. Hrsg. von B. van der Sloot, Dennis Broeders und E. Schrijvers. Amsterdam University Press, 2016, S. 261–281.
- [293] **V. Schochlow**, S. Neumann, K. Braun und M. Volkamer. „Bewertung der GMX/Mailvelope-Ende-zu-Ende-Verschlüsselung“. In: *Datenschutz und Datensicherheit - DuD* 40.5 (Mai 2016), S. 295–299. ISSN: 1614-0702. DOI: 10.1007/s11623-016-0599-5.

- [294] **H. Shulman** und M. Waidner. „Is the Internet Ready for DNSSEC: Evaluating Pitfalls in the Naming Infrastructure“. In: *Proceedings of the TMA*. Hrsg. von A. Botta, R. Sadre und F. Bustamante. Traffic Monitoring and Analysis. IFIP, Apr. 2016. URL: <https://tubiblio.ulb.tu-darmstadt.de/107193/>.
- [295] D. Steinmetzer, **J. Classen** und M. Hollick. „Exploring Millimeter-Wave Network Scenarios with Ray-Tracing Based Simulations in mmTrace“. In: *Proceedings of the Conference on Computer Communications Workshops (INFOCOM WKSHPs)*. Open Access (ePrint). IEEE / IEEE, Apr. 2016, S. 1093–1094. DOI: 10.1109/infcomw.2016.7562269. eprint: https://download.hrz.tu-darmstadt.de/media/FB20/Dekanat/Publikationen/SEEM00/mmTrace_paper.pdf. 
- [296] D. Steinmetzer, **J. Classen** und M. Hollick. „mmTrace: Modeling Millimeter-Wave Indoor Propagation with Image-Based Ray-Tracing“. In: *Proceedings of the Conference on Computer Communications Workshops (INFOCOM WKSHPs)*. Conference on Computer Communications Workshops. Open Access (ePrint). IEEE / IEEE, Apr. 2016, S. 429–434. DOI: 10.1109/infcomw.2016.7562115. eprint: <https://download.hrz.tu-darmstadt.de/media/FB20/Dekanat/Publikationen/SEEM00/mmTrace.pdf>. 
- [297] M. Strohbach, **J. Daubert**, H. Ravkin und M. Lischka. „Big Data Storage“. In: *New Horizons for a Data-Driven Economy - A Roadmap for Usage and Exploitation of Big Data in Europe*. Hrsg. von J. M. Cavanillas, E. Curry und W. Wahlster. Open Access. Springer, 2016, S. 119–141. ISBN: 978-3-319-21568-6. DOI: 10.1007/978-3-319-21569-3_7. 
- [298] G. Traverso, D. Demirel, **M. Habib** und J. Buchmann. „AS3: Adaptive Social Secret Sharing for Distributed Storage Systems“. In: *Proceedings of the 14th Annual Conference on Privacy, Security and Trust (PST 2016)*. Conference on Privacy, Security and Trust. IEEE, Dez. 2016, S. 528–535. DOI: 10.1109/pst.2016.7907011.
- [299] M. Vigil, D. Demirel, **S. M. Habib**, **S. Hauke**, J. Buchmann und M. Mühlhäuser. „LoT: A Reputation-Based Trust System for Long-Term Archiving“. In: *Proceedings of the Tenth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2016)*. International Conference on Emerging Security Information, Systems and Technologies. Thinkmind Digital Library, Juli 2016, S. 262–270. URL: <http://tubiblio.ulb.tu-darmstadt.de/101685/>.
- [300] M. Volkamer, K. Renaud und **P. Gerber**. „Spot the Phish by Checking the Pruned URL“. In: *Information & Computer Security 24.4* (Okt. 2016). Open Access (ePrint), S. 372–385. ISSN: 2056-4961. DOI: 10.1108/ics-07-2015-0032. eprint: <https://publikationen.bibliothek.kit.edu/1000081983/15239357>. 
- [301] R. Weinhold, **P. Richter**, M. Krüger und K. Geske. „Von Kameras und Verdrängung. Rechtliche Anknüpfungspunkte für ein Recht auf Stadt unter besonderer Diskussion der Videoüberwachung öffentlicher Räume“. In: *KJ Kritische Justiz* 49.1 (2016), S. 31–46. ISSN: 0023-4834.
- [302] **H. E. Wenninger**, Z. W. Lee, C. M. Cheung, T. K. Chan und R. Y. Wong. „A Literature Analysis about Social Information Contribution and Consumption on Social Networking Sites“. In: *Proceedings of the European Conference on Information Systems (ECIS 2014)*. Publications of Darmstadt Technical University, Institute for Business Studies (BWL). 2016, S. 1–22. URL: <https://ideas.repec.org/p/dar/wpaper/80322.html>.
- [303] **S. Abdelwahab**, T. Gaber und M. Wahed. „Trust and Bio-Inspired-Based Clustering Techniques in Wireless Sensor Networks: A Survey“. In: *Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2017, AISI 2017, Cairo, Egypt, September 9-11, 2017*. Hrsg. von A. E. Hassanien, K. Shaalan, T. Gaber und M. F. Tolba. Bd. 639. Advances in Intelligent Systems and Computing. Springer, Aug. 2017, S. 714–723. DOI: 10.1007/978-3-319-64861-3_67.
- [304] **S. Abdelwahab**, T. Gaber und M. Wahed. „Trust-Based Security Models in Wireless Sensor Networks: A Survey“. In: *Int. J. Comput. Intell. Stud.* 6.2/3 (2017), S. 245–266. ISSN: 1755-4977. DOI: 10.1504/IJCISTUDIES.2017.10010048.
- [305] O. Abramova, **A. Wagner**, H. Krasnova und P. Buxmann. „Understanding Self-Disclosure on Social Networking Sites - a Literature Review“. In: *AMCIS 2017 Proceedings*. Publications of Darmstadt Technical University, Institute for Business Studies (BWL). Association for Information Systems, 2017, S. 30. URL: <https://ideas.repec.org/p/dar/wpaper/87719.html>.
- [306] **N. Alexopoulos**. „On Enhancing Trust in Cryptographic Solutions: Student Research Abstract“. In: *Proceedings of the Symposium on Applied Computing, SAC 2017, Marrakech, Morocco, April 3-7, 2017*. Hrsg. von A. Seffah, B. Penzenstadler, C. Alves und X. Peng. Bd. 200. ACM, Apr. 2017, S. 1848–1849. DOI: 10.1145/3019612.3019921.

- [307] **N. Alexopoulos, J. Daubert**, M. Mühlhäuser und **S. M. Habib**. „Beyond the Hype: On Using Blockchains in Trust Management for Authentication“. In: *2017 IEEE Trustcom/BigDataSE/ICSS, Sydney, Australia, August 1-4, 2017*. 2017 IEEE Trustcom/BigDataSE/ICSS. Open Access (arXiv). IEEE Computer Society, Aug. 2017, S. 546–553. DOI: 10.1109/TRUSTCOM/BIGDATASE/ICSS.2017.283. arXiv: 1711.04591. 
- [308] **N. Alexopoulos**, A. Kiayias, R. Talviste und T. Zacharias. „MCMix: Anonymous Messaging via Secure Multiparty Computation“. In: *26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16-18, 2017*. Hrsg. von E. Kirda und T. Ristenpart. USENIX Security Symposium. Open Access. USENIX Association, Aug. 2017, S. 1217–1234. URL: <https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/alexopoulos>. 
- [309] **N. Alexopoulos, E. Vasilomanolakis**, N. R. Ivánkó und M. Mühlhäuser. „Towards Blockchain-Based Collaborative Intrusion Detection Systems“. In: *Critical Information Infrastructures Security - 12th International Conference, CRITIS 2017, Lucca, Italy, October 8-13, 2017, Revised Selected Papers*. Hrsg. von G. D'Agostino und A. Scala. Bd. 10707. Lecture Notes in Computer Science. Springer, Okt. 2017, S. 107–118. DOI: 10.1007/978-3-319-99843-5_10.
- [310] M. Becker, C. Matt, **T. Widjaja** und T. Hess. „Understanding Privacy Risk Perceptions of Consumer Health Wearables – an Empirical Taxonomy“. In: *Proceedings of the International Conference on Information Systems (ICIS 2017)*. Hrsg. von Y. J. Kim, R. Agarwal und J. K. Lee. International Conference on Information Systems. AIS eLibrary, 2017. URL: <https://aisel.aisnet.org/icis2017/IT-and-Healthcare/Presentations/12/>.
- [311] H. Brakemeier, **A. Wagner** und P. Buxmann. „When Risk Perceptions Are Nothing but Guesses – an Evaluability Perspective on Privacy Risks“. In: *ICIS 2017 Proceedings*. Hrsg. von Y. J. Kim, R. Agarwal und J. K. Lee. International Conference on Information Systems. Association for Information Systems, 2017, S. 16.
- [312] A. Engelbrecht, J. P. Gerlach, **T. Widjaja** und P. Buxmann. „The Nature of Enterprise-Service-Fit in the Context of Digital Services“. In: *Proceedings of the International Conference on Information Systems (ICIS 2017)*. Hrsg. von Y. J. Kim, R. Agarwal und J. K. Lee. International Conference on Information Systems. AIS eLibrary, 2017. URL: <http://aisel.aisnet.org/icis2017/General/Presentations/8>.
- [313] H. Fereidooni, **J. Classen**, T. Spink, P. Patras, M. Miettinen, A.-R. Sadeghi, M. Hollick und M. Conti. „Breaking Fitness Records without Moving: Reverse Engineering and Spoofing Fitbit“. In: *Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses*. Hrsg. von M. Dacier, M. Bailey, M. Polychronakis und M. Antonakakis. Bd. 10453. Open Access (ePrint). Springer Science+Business Media / Springer, Juni 2017, S. 48–69. ISBN: 978-3-319-66331-9. DOI: 10.1007/978-3-319-66332-6_3. eprint: https://research-repository.st-andrews.ac.uk/bitstream/10023/24316/1/Fereidooni_2017_Breaking_Fitness_Records_AAM.pdf. 
- [314] S. Funke, A. Wiesmaier und **J. Daubert**. „Constrained PET Composition for Measuring Enforced Privacy“. In: *Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, August 29 - September 01, 2017*. Proceedings of the 17th International Conference on Availability, Reliability and Security. ACM, Aug. 2017, 16:1–16:10. DOI: 10.1145/3098954.3098968.
- [315] **C. Geminn**. „Die europäische Datenschutz-Grundverordnung – Eine kritische Betrachtung der neuen Datenschutzregeln in der Europäischen Union“. In: *Jichi kenkyu, Forschung zur Selbstverwaltung* 93.3 (2017), S. 3–23.
- [316] **C. Geminn** und **P. Richter**. „Telekommunikation“. In: *Europäische Datenschutz-Grundverordnung: Vorrang des Unionsrechts - Anwendbarkeit des nationalen Rechts*. Hrsg. von A. Rossnagel. Nomos, 2017. DOI: 10.1163/2352-0248_edn_a4284000.
- [317] **C. L. Geminn**. „Risikoadäquate Regelungen für das Internet der Dienste und Dinge?“ In: *Datenschutz und Datensicherheit - DuD* 41.5 (März 2017), S. 295–299. ISSN: 1614-0702. DOI: 10.1007/s11623-017-0778-z.
- [318] **N. Gerber, P. Gerber** und M. Hernando. „Sharing the ‘Real Me’—How Usage Motivation and Personality Relate to Privacy Protection Behavior on Facebook“. In: *Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings 5*. Hrsg. von T. Tryfonas. Bd. 10292. Interacción. Springer Science+Business Media / Springer International Publishing, Juli 2017, S. 640–655. ISBN: 978-3-319-58459-1. DOI: 10.1007/978-3-319-58460-7_44.

- [319] **N. Gerber** und **V. Zimmermann**. „Security vs. Privacy? User Preferences Regarding Text Passwords and Biometric Authentication“. In: *Proceedings of the Mensch Und Computer (MuC 2017)*. Hrsg. von M. Burghardt, R. Wimmer, C. Wolff und C. Womser-Hacker. Message Understanding Conference. Regensburg: Gesellschaft für Informatik e.V., Sep. 2017, S. 279. DOI: 10.18420/muc2017-ws05-0405.
- [320] **P. Gerber**, M. Volkamer und **N. Gerber**. „Das Privacy-Paradoxon – Ein Erklärungsversuch und Handlungsempfehlungen“. In: *Dialogmarketing Perspektiven 2016/2017: Tagungsband 11. Wissenschaftlicher Interdisziplinärer Kongress für Dialogmarketing*. Springer Fachmedien Wiesbaden / Springer Fachmedien Wiesbaden, 2017, S. 139–167. ISBN: 978-3-658-16834-6. DOI: 10.1007/978-3-658-16835-3_8.
- [321] **P. Gerber**, M. Volkamer und K. Renaud. „The Simpler, the Better? Presenting the COPING Android Permission-Granting Interface for Better Privacy-Related Decisions“. In: *Journal of Information Security and Applications* 34 (Juni 2017). Open Access (ePrint), S. 8–26. ISSN: 2214-2126. DOI: 10.1016/j.jisa.2016.10.003. eprint: <https://eprints.gla.ac.uk/137741/7/137741.pdf>. 
- [322] Y. Gilad, A. Cohen, A. Herzberg, M. Schapira und **H. Shulman**. „Are We There yet? On Rpk’s Deployment and Security“. In: *Proceedings of the NDSS*. The Internet Society, 2017. DOI: 10.14722/ndss.2017.23123.
- [323] P. C. Johannes und **P. Richter**. „Privilegierte Verarbeitung im BDSG-e“. In: *Datenschutz und Datensicherheit - DuD* 41.5 (März 2017), S. 300–305. ISSN: 1614-0702. DOI: 10.1007/s11623-017-0779-y.
- [324] A. Klein, V. Kravtsov, A. Perlmutter, **H. Shulman** und M. Waidner. „POSTER: X-Ray Your DNS“. In: *Proceedings of the ACM Conference on Computer and Communications Security (CCS 2017)*. Hrsg. von B. M. Thuraisingham, D. Evans, T. Malkin und D. Xu. Conference on Computer and Communications Security. ACM, Okt. 2017, S. 2519–2521. DOI: 10.1145/3133956.3138821.
- [325] A. Klein, **H. Shulman** und M. Waidner. „Counting in the Dark: DNS Caches Discovery and Enumeration in the Internet“. In: *Proceedings of the 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2017)*. Dependable Systems and Networks. IEEE Computer Society, Juni 2017, S. 367–378. DOI: 10.1109/dsn.2017.63.
- [326] A. Klein, **H. Shulman** und M. Waidner. „Internet-Wide Study of DNS Cache Injections“. In: *Proceedings of the INFOCOM*. IEEE Conference on Computer Communications. IEEE, Mai 2017, S. 1–9. DOI: 10.1109/infocom.2017.8057202.
- [327] **J. Kropf**. „Der Wert der Musik: Aushandlungsdynamiken in der digitalisierten Musikwirtschaft“. In: *Kommunikation @ Gesellschaft* 18.1 (Aug. 2017). Open Access, S. 26. ISSN: 1616-2617. DOI: 10.15460/kommges.2017.18.1.590. 
- [328] **J. Kropf**. „Hippolyte taine (1828–1893)“. In: *Klassiker der Soziologie der Künste*. Springer, 2017, S. 45–72. ISBN: 978-3-658-01454-4. DOI: 10.1007/978-3-658-01455-1_3.
- [329] **O. Kulyk**, S. Neumann, **K. Marky**, J. Budurushi und M. Volkamer. „Coercion-Resistant Proxy Voting“. In: *Computers & Security* 71.C (Nov. 2017). Open Access (ePrint), S. 88–99. ISSN: 0167-4048. DOI: 10.1016/j.cose.2017.06.007. eprint: <https://publikationen.bibliothek.kit.edu/1000081964/15444958>. 
- [330] J. Lamla und **C. Ochs**. „Der NSA-Skandal als Krise der Demokratie?“ In: *Kritische Öffentlichkeiten - Öffentlichkeiten in der Kritik*. Springer, 2017, S. 83–112. ISBN: 978-3-658-14942-0. DOI: 10.1007/978-3-658-14943-7_4.
- [331] T. Matzner und **C. Ochs**. „Sorting Things out Ethically: Privacy as a Research Issue beyond the Individual“. In: *Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts* (2017), S. 39–56.
- [332] **C. Ochs**. „Cultural Techniques, Practices, Programmes: How to Study the Anthropologic of Digitisation“. In: *Digitisation*. Routledge, 2017, S. 11–39.
- [333] **C. Ochs** und J. Lamla. „Demokratische Privacy by Design“. In: *Forschungsjournal Soziale Bewegungen* 30.2 (Juni 2017), S. 189–199. ISSN: 2192-4848. DOI: 10.1515/fjsb-2017-0040.
- [334] **F. Pittroff**. „Profile als Labore des Privaten“. In: *Profile*. Hrsg. von M. Degeling, J. Othmer, A. Weich und B. Westermann. Open Access. Lüneburg: Meson Press, Aug. 2017, S. 101–114. ISBN: 978-3-95796-100-6. DOI: 10.25969/mediarep/2098. 

- [335] K. Renaud und **V. Zimmermann**. „Enriched Nudges Lead to Stronger Password Replacements ... but Implement Mindfully“. In: *Information Security for South Africa (ISSA)* (Aug. 2017). Hrsg. von H. S. Venter, M. Look, M. Coetzee, M. M. Eloff und J. H. P. Eloff, S. 1–9. DOI: 10.1109/issa.2017.8251779.
- [336] K. Renaud, **V. Zimmermann**, J. Maguire und S. Draper. „Lessons Learned from Evaluating Eight Password Nudges in the Wild“. In: *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2017)*. USENIX Association, Okt. 2017, S. 25–37. ISBN: 978-1-931971-41-6. URL: <https://www.usenix.org/conference/laser2017/presentation/renaud>.
- [337] **P. Richter**. „Statistische Datenverarbeitung“. In: *Europäische Datenschutz-Grundverordnung: Vorrang des Unionsrechts - Anwendbarkeit des nationalen Rechts*. Hrsg. von A. Rossnagel. Nomos, 2017.
- [338] A. Rossnagel und **P. Richter**. „Aufwachsen in virtuellen und technologisierten Welten. Herausforderungen der Datensammlung, Vernetzung, Kommerzialisierung und neuen Überwachungstechnologien für Jugendliche“. In: *Sachverständigenkommission 15. Kinder- und Jugendbericht (Hrsg.) Materialien zum 15. Kinder und Jugendbericht. Zwischen Freiräumen, Familie, Ganztagschule und virtuellen Welten — Persönlichkeitsentwicklung und Bildungsanspruch im Jugendalter 15* (2017).
- [339] N. Rotenberg, **H. Shulman**, M. Waidner und B. Zeltser. „Authentication-Bypass Vulnerabilities in SOHO Routers“. In: *Proceedings of the SIGCOMM Posters and Demos*. ACM, Aug. 2017, S. 68–70. DOI: 10.1145/3123878.3131989.
- [340] **H. Shulman** und M. Waidner. „One Key to Sign Them All Considered Vulnerable: Evaluation of DNSSEC in the Internet“. In: *Proceedings of the 14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 2017)*. Hrsg. von A. Akella und J. Howell. Networked Systems Design and Implementation. USENIX Association, 2017, S. 131–144. URL: <https://www.usenix.org/system/files/conference/nsdi17/nsdi17-shulman.pdf>.
- [341] A. Singh und **H. Simo**. „Restricted Usage of Anonymous Credentials in Vehicular Ad Hoc Networks for Misbehavior Detection“. In: *International Journal of Information Security* 16.2 (Apr. 2017), S. 195–211. ISSN: 1615-5262. DOI: 10.1007/s10207-016-0328-y.
- [342] G. Traverso, C. G. Cordero, M. Nojournian, R. Azarderakhsh, D. Demirel, **S. M. Habib** und J. Buchmann. „Evidence-Based Trust Mechanism Using Clustering Algorithms for Distributed Storage Systems“. In: *Proceedings of the 15th Annual Conference on Privacy, Security and Trust (PST 2017)*. Aug. 2017. URL: <http://tubiblio.ulb.tu-darmstadt.de/98115/>.
- [343] A. Ulmer, J. Kohlhammer und **H. Shulman**. „Towards Enhancing the Visual Analysis of Interdomain Routing“. In: *Proceedings of the VISIGRAPP (3: IVAPP)*. Hrsg. von L. Linsen, A. Telea und J. Braz. Open Access. SciTePress, 2017, S. 209–216. DOI: 10.5220/0006126702090216. 
- [344] **E. Vasilomanolakis**, **S. M. Habib**, P. Milaszewicz, R. S. Malik und M. Mühlhäuser. „Towards Trust-Aware Collaborative Intrusion Detection: Challenges and Solutions“. In: *Proceedings of the 11th IFIP International Conference on Trust Management (TM)*. Hrsg. von J.-P. Steghöfer und B. Esfandiari. Bd. AICT-505. Trust Management XI. Part 3: Applications of Trust, Open Access. Gothenburg, Sweden: Springer, Juni 2017, S. 94–109. ISBN: 978-3-319-59170-4. DOI: 10.1007/978-3-319-59171-1_8. 
- [345] **V. Zimmermann** und **N. Gerber**. „If It Wasn't Secure, They Would Not Use It in the Movies"—Security Perceptions and User Acceptance of Authentication Technologies“. In: *Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings 5*. Hrsg. von T. Tryfonas. Bd. 10292. Interacción. Springer International Publishing / Springer, Juli 2017, S. 265–283. ISBN: 978-3-319-58459-1. DOI: 10.1007/978-3-319-58460-7_18.
- [346] **V. Zimmermann**, B. Henhapl, **N. Gerber** und M. Enzmann. „Promoting Secure Email Communication and Authentication“. In: *Proceedings of the Mensch Und Computer (MuC 2017)*. Hrsg. von M. Burghardt, R. Wimmer, C. Wolff und C. Womser-Hacker. Message Understanding Conference. Regensburg: Gesellschaft für Informatik e.V., Sep. 2017, S. 269. DOI: 10.18420/muc2017-ws05-0404.
- [347] **V. Zimmermann**, B. Henhapl, M. Volkamer und J. Vogt. „Ende-zu-Ende sichere E-Mail-Kommunikation“. In: *Datenschutz und Datensicherheit - DuD* 41.5 (März 2017), S. 308–313. ISSN: 1614-0702. DOI: 10.1007/s11623-017-0781-4.

- [348] **N. Alexopoulos, S. M. Habib** und M. Mühlhäuser. „Towards Secure Distributed Trust Management on a Global Scale: An Analytical Approach for Applying Distributed Ledgers for Authorization in the IoT“. In: *Proceedings of the 2018 Workshop on IoT Security and Privacy, IoT S&P@SIGCOMM 2018, Budapest, Hungary, August 20, 2018*. Bd. 99. IoT S&P@SIGCOMM. Open Access. ACM, Aug. 2018, S. 49–54. DOI: 10.1145/3229565.3229569. 
- [349] M. Bidler, J. Schumann und **T. Widjaja**. „Challenging the Cognitive Privacy Calculus: Affective Reactions in Consumers“. In: *Proceedings of the Privacy-Related Decision Making. EMAC Conference*. 2018.
- [350] M. Brandt, T. Dai, A. Klein, **H. Shulman** und M. Waidner. „Domain Validation++ for MitM-resilient PKI“. In: *Proceedings of the ACM Conference on Computer and Communications Security (CCS 2018)*. Hrsg. von D. Lie, M. Mannan, M. Backes und X. Wang. ACM, Okt. 2018, S. 2060–2076. DOI: 10.1145/3243734.3243790.
- [351] M. Brandt, **H. Shulman** und M. Waidner. „Internet as a Source of Randomness“. In: *Proceedings of the ACM Workshop on Hot Topics in Networks (HotNets)*. ACM, Nov. 2018, S. 64–70. DOI: 10.1145/3286062.3286072.
- [352] **S. Bretthauer** und I. Spiecker gen. Döhmman, Hrsg. *Dokumentation zum Datenschutz mit Informationsfreiheitsrecht*. Baden-Baden: Nomos, 2018, Loseblattsammlung, ca. 8000.
- [353] P. Buxmann und **A. Wagner**. „Datenökonomie und Privatsphäre – Ergebnisse von drei empirischen Untersuchungen“. In: *MedienWirtschaft* 15.3 (2018), S. 20–29. ISSN: 1613-0669. DOI: 10.15358/1613-0669-2018-3-20.
- [354] **J. Classen**, D. Wegemer, P. Patras, T. Spink und M. Hollick. „Anatomy of a Vulnerable Fitness Tracking System: Dissecting the Fitbit Cloud, App, and Firmware“. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)* 2.1 (2018), 5:1–5:24. DOI: 10.1145/3191737.
- [355] C. G. Cordero, G. Traverso, M. Nojournian, **S. M. Habib**, M. Mühlhäuser, J. Buchmann und **E. Vasilomanolakis**. „Sphinx: A Colluder-Resistant Trust Mechanism for Collaborative Intrusion Detection“. In: *IEEE access: practical innovations, open solutions* 6 (Nov. 2018), S. 72427–72438. ISSN: 2169-3536. DOI: 10.1109/access.2018.2880297.
- [356] **J. Daubert**, D. Boopalan, M. Mühlhäuser und **E. Vasilomanolakis**. „HoneyDrone: A Medium-Interaction Unmanned Aerial Vehicle Honeypot“. In: *2018 IEEE/IFIP Network Operations and Management Symposium, NOMS 2018, Taipei, Taiwan, April 23-27, 2018*. IEEE/IFIP Network Operations and Management Symposium. Open Access (ePrint). IEEE, Apr. 2018, S. 1–6. DOI: 10.1109/NOMS.2018.8406315. eprint: <https://download.hrz.tu-darmstadt.de/media/FB20/Dekanat/Publikationen/TK/honeyDrone.pdf>. 
- [357] **M. Fomichev**, F. Álvarez, D. Steinmetzer, P. Gardner-Stephen und M. Hollick. „Survey and Systematization of Secure Device Pairing“. In: *IEEE Communications Surveys & Tutorials* 20.1 (2018). Open Access (arXiv), S. 517–550. ISSN: 1553-877X. DOI: 10.1109/COMST.2017.2748278. arXiv: 1709.02690. 
- [358] T. Gaber, **S. Abdelwahab**, M. Elhoseny und A. E. Hassanien. „Trust-Based Secure Clustering in WSN-based Intelligent Transportation Systems“. In: *Comput. Networks* 146 (Sep. 2018). Open Access (ePrint), S. 151–158. ISSN: 1389-1286. DOI: 10.1016/J.COMNET.2018.09.015. eprint: http://usir.salford.ac.uk/id/eprint/48399/1/Tarek_Gaber_Accepted_Trust-based%20Secure%20Clustering%20in%20WSN-based%20Intelligent%20Transportation%20Systems.pdf. 
- [359] **C. Geminn**. „Das Europäische Datenschutzrecht – Zwischen Leuchtturmfunktion und Werteexport?“. In: *Deutsches Verwaltungsblatt* 133.24 (Dez. 2018), S. 1593–1599. ISSN: 2366-0651. DOI: 10.1515/dvb1-2018-1332404.
- [360] **C. Geminn**. „Rechtsschutz für Betroffene“. In: *Datenschutz im Internet – Rechtshandbuch zu DSGVO und BDSG*. Hrsg. von **S. Jandt** und R. Steidle. Nomos Praxis, 2018, S. 459–489.
- [361] **C. L. Geminn**. „Wissenschaftliche Forschung und Datenschutz“. In: *Datenschutz und Datensicherheit - DuD* 42.10 (1. Okt. 2018), S. 640–646. ISSN: 1862-2607. DOI: 10.1007/s11623-018-1016-z.
- [362] **N. Gerber, V. Zimmermann**, B. Henhapl, S. Emeröz, M. Volkamer und T. Hilt. „Nutzerwahrnehmung der Ende-zu-Ende-Verschlüsselung in WhatsApp“. In: *Datenschutz und Datensicherheit - DuD* 42.11 (Nov. 2018), S. 680–685. ISSN: 1614-0702. DOI: 10.1007/s11623-018-1024-z.
- [363] **P. Gerber**, M. Ghiglieri, B. Henhapl, **O. Kulyk, K. Marky**, P. Mayer, B. Reinheimer und M. Volkamer. „Human Factors in Security“. In: *Sicherheitskritische Mensch-Computer-Interaktion: Interaktive Technologien und Soziale Medien im Krisen- und Sicherheitsmanagement* (2018), S. 83–98. DOI: 10.1007/978-3-658-19523-6_5.

- [364] Y. Gilad, T. Hlavacek, A. Herzberg, M. Schapira und **H. Shulman**. „Perfect Is the Enemy of Good: Setting Realistic Goals for BGP Security“. In: *Proceedings of the ACM Workshop on Hot Topics in Networks (HotNets)*. ACM Workshop on Hot Topics in Networks. ACM, Nov. 2018, S. 57–63. DOI: 10.1145/3286062.3286071.
- [365] M. Gohring, **H. Shulman** und M. Waidner. „Path MTU Discovery Considered Harmful“. In: *Proceedings of the ICDCS*. IEEE Computer Society, Juli 2018, S. 866–874. DOI: 10.1109/icdcs.2018.00088.
- [366] **S. M. Habib, N. Alexopoulos**, M. M. Islam, J. Heider, S. Marsh und M. Mühlhäuser. „Trust4App: Automating Trustworthiness Assessment of Mobile Applications“. In: *Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*. IEEE, Aug. 2018, S. 124–135. DOI: 10.1109/trustcom/bigdatase.2018.00029.
- [367] T. Hlavacek, A. Herzberg, **H. Shulman** und M. Waidner. „Practical Experience: Methodologies for Measuring Route Origin Validation“. In: *Proceedings of the DSN*. Dependable Systems and Networks. IEEE Computer Society, Juni 2018, S. 634–641. DOI: 10.1109/dsn.2018.00070.
- [368] C. Husemann, **F. Pittroff** und A. D. Schulz. „Fitness-Tracking als Informationsproblem: Zu den Potenzialen und Herausforderungen rechtlicher Regulierung und pädagogischer Vermittlung“. In: *Datenschutz und Datensicherheit - DuD* 42.11 (Nov. 2018), S. 694–700. ISSN: 1862-2607. DOI: 10.1007/s11623-018-1027-9.
- [369] **S. Jandt** und R. Steidle. *Datenschutz im Internet. Rechtshandbuch zu DSGVO und BDSG*. 1. Auflage. NomosPraxis. Baden-Baden: Nomos, 2018, 532 Seiten. ISBN: 978-3-8487-4856-3 and 3-8487-4856-8.
- [370] K. Kelpen und **H. Simo**. „Privacy and Data Protection in the Domain Name System“. In: *Privatheit Und Selbstbestimmtes Leben in Der Digitalen Welt*. Springer, 2018, S. 253–302. ISBN: 978-3-658-21383-1. DOI: 10.1007/978-3-658-21384-8_8.
- [371] **J. Kropf**. „Bewertungsformen und ihre Struktur dynamiken in sozialen Feldern“. In: *Die Produktivität von Musikkulturen*. Springer, 2018, S. 185–206. ISBN: 978-3-658-19017-0. DOI: 10.1007/978-3-658-19018-7_8.
- [372] **J. Kropf**. „Übersetzung, Ungleichzeitigkeit und Konflikt: Zur Transformation sozialer Felder“. In: *Österreichische Zeitschrift für Soziologie* 43.2 (Juni 2018), S. 157–178. ISSN: 1011-0070. DOI: 10.1007/s11614-018-0304-z.
- [373] **K. Marky, O. Kulyk**, K. Renaud und M. Volkamer. „What Did I Really Vote for? On the Usability of Verifiable E-voting Schemes“. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. Hrsg. von R. L. Mandryk, M. Hancock, M. Perry und A. L. Cox. Bd. 2. Chi '18. Open Access (ePrint). New York, NY, USA: Association for Computing Machinery, Apr. 2018, S. 1–13. ISBN: 978-1-4503-5620-6. DOI: 10.1145/3173574.3173750. eprint: https://rke.abertay.ac.uk/files/14702506/Renaud_WhatDidIReallyVoteFor_Author_2018.pdf. 
- [374] **K. Marky, O. Kulyk** und M. Volkamer. „Comparative Usability Evaluation of Cast-as-Intended Verification Approaches in Internet Voting“. In: *Proceedings of the SICHERHEIT 2018*. Hrsg. von H. Langweg, M. Meier, B. C. Witt und D. Reinhardt. Bd. P-281. Sicherheit. Bonn: Gesellschaft für Informatik e.V., Apr. 2018, S. 197–208. DOI: 10.18420/sicherheit2018_15.
- [375] **K. Marky**, P. Mayer, **N. Gerber** und **V. Zimmermann**. „Assistance in Daily Password Generation Tasks“. Englisch. In: *Proceedings of the Joint ACM International Conference on Pervasive and Ubiquitous Computing (UbiComp 2018) and 2018 ACM International Symposium on Wearable Computers (ISWC 2018)*. UbiComp/ISWC Adjunct. ACM Press, New York (NY), Okt. 2018, S. 786–793. ISBN: 978-1-4503-5966-5. DOI: 10.1145/3267305.3274127.
- [376] S. Marsh, A. Diaconescu, D. Evans, T. A. Kosa, P. R. Lewis und **S. Mahbub Habib**. „Public Privacy and Brick Houses Made of Glass“. In: *Proceedings of the 12th IFIP International Conference on Trust Management (TM)*. Hrsg. von N. Gal-Oz und P. R. Lewis. Bd. AICT-528. Trust Management XII. Open Access. Toronto, ON, Canada: Springer, Juli 2018, S. 137–148. ISBN: 978-3-319-95275-8. DOI: 10.1007/978-3-319-95276-5_10. 
- [377] **C. Ochs, B. Büttner** und E. Hörster. „Das Internet als »Sauerstoff« und »Bedrohung«“. In: *Privatheit und selbstbestimmtes Leben in der digitalen Welt*. Springer, 2018, S. 33–80. ISBN: 978-3-658-21383-1. DOI: 10.1007/978-3-658-21384-8_3.
- [378] **F. Pittroff**. „Perverse Privatheiten: Die Postprivacy-Kontroverse als Labor der Transformation von Privatheit und Subjektivität“. In: *Digitale Bewertungspraktiken*. Springer Fachmedien Wiesbaden, Sep. 2018, S. 191–214. ISBN: 978-3-658-21165-3. DOI: 10.1007/978-3-658-21165-3_8.

- [379] R. Quinn, A. Baur, T. Bile, **M. Nebel**, B. Bremert, **B. Büttner**, O. Grigorjew, T. Hagendorff, J. Heesen, N. Krämer, Y. Meier, G. Neubaum, **C. Ochs**, A. Roßnagel, **H. Simo** und S. Weiler. *Forum Privatheit (hrsg.), Tracking – Beschreibung und Bewertung neuer Methoden*. Karlsruhe: Frauenhofer ISI, 2018.
- [380] K. Renaud und **V. Zimmermann**. „Ethical Guidelines for Nudging in Information Security & Privacy“. In: *International Journal of Human-Computer Studies* 120 (Dez. 2018), S. 22–35. DOI: 10.1016/j.ijhcs.2018.05.011.
- [381] K. Renaud und **V. Zimmermann**. „Guidelines for Ethical Nudging in Password Authentication“. In: *SAIEE Africa Research Journal* 109.2 (Juni 2018). Open Access, S. 102–118. ISSN: 1991-1696. DOI: 10.23919/saiee.2018.8531951. 
- [382] M. Tarafdar und **H. Wenninger**. „Effects of ‘fit’ on Email Overload“. In: *Proceedings of the 24th Americas Conference on Information Systems (AMCIS 2018)*. Americas Conference on Information Systems. Association for Information Systems, Aug. 2018. URL: <https://aisel.aisnet.org/amcis2018/OrgTrasfm/Presentations/10>.
- [383] M. Tarafdar und **H. E. Wenninger**. „How Decision-Making Culture and Email Use Norms Influence Email Overload: Toward a Demand Resource Model“. In: *Changing Nature of Work (CNoW): Bridging the Workplace of People, Data and Things* (2018).
- [384] **E. Vasilomanolakis**, **J. Daubert**, D. Boopalan und M. Mühlhäuser. „Don’t Steal My Drone: Catching Attackers with an Unmanned Aerial Vehicle HoneyPot“. In: *2018 IEEE/IFIP Network Operations and Management Symposium, NOMS 2018, Taipei, Taiwan, April 23–27, 2018*. IEEE/IFIP Network Operations and Management Symposium. Open Access (ePrint). IEEE, Apr. 2018, S. 1–2. DOI: 10.1109/NOMS.2018.8406119. eprint: <https://download.hrz.tu-darmstadt.de/media/FB20/Dekanat/Publikationen/TK/noms18honeyPotdemo.pdf>. 
- [385] M. Volkamer, A. Gutmann, K. Renaud, **P. Gerber** und P. Mayer. „Replication Study: A Cross-Country Field Observation Study of Real World PIN Usage at ATMs and in Various Electronic Payment Scenarios“. In: *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. Hrsg. von M. E. Zurko und H. R. Lipford. Open Access. USENIX Association, Aug. 2018, S. 1–11. URL: <https://www.usenix.org/conference/soups2018/presentation/volkamer>. 
- [386] **A. Wagner**, O. Abramova, H. Krasnova und P. Buxmann. „When You Share, You Should Care: Examining the Role of PerspectiveTaking on Social Networking Sites“. In: *ECIS 2018 Proceedings*. 2018, S. 174.
- [387] **A. Wagner**, L. A. Gasche u. a. *Sharenting: Making Decisions About Other’s Privacy on Social Networking Sites*. Leuphana University Lüneburg / Darmstadt Technical University, Department of Business Administration, 2018.
- [388] **A. Wagner**, H. Krasnova, O. Abramova, P. Buxmann und I. Benbasat. „From Privacy Calculus to Social Calculus: Understanding Self-Disclosure on Social Networking Sites“. In: *ICIS 2018 Proceedings*. Hrsg. von J. Pries-Heje, S. Ram und M. Rosemann. Publications of Darmstadt Technical University, Institute for Business Studies (BWL). Association for Information Systems, Dez. 2018, S. 20. URL: <https://ideas.repec.org/p/dar/wpaper/107513.html>.
- [389] **A. Wagner**, **N. Wessels**, P. Buxmann und H. Krasnova. „Putting a Price Tag on Personal Information - a Literature Review“. In: *Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS 2018)*. Proceedings of the ... Annual Hawaii International Conference on System Sciences/Proceedings of the Annual Hawaii International Conference on System Sciences. Open Access. Hawaii International Conference on System Sciences, Jan. 2018, S. 3760–3769. DOI: 10.24251/HICSS.2018.474. 
- [390] **H. Wenninger**, H. Krasnova und P. Buxmann. „Understanding the Role of Social Networking Sites in the Subjective Well-Being of Users: A Diary Study“. In: *European Journal of Information Systems* 28.2 (Aug. 2018). Open Access, S. 1–23. ISSN: 0960-085X. URL: https://eprints.lancs.ac.uk/id/eprint/126838/1/SocialActivities_EJIS_author_submitted_manuscript.pdf. 
- [391] K. Wolf, **K. Marky** und M. Funk. „We Should Start Thinking about Privacy Implications of Sonic Input in Everyday Augmented Reality!“ In: *Proceedings of the Workshop on Virtual and Augmented Reality in Everyday Context (Vareco) at Mensch Und Computer (MuC 2018)*. Hrsg. von R. Dachelt und G. Weber. Mensch & Computer Workshopband. Gesellschaft für Informatik e.V., Okt. 2018, S. 353–359. DOI: 10.18420/muc2018-ws07-0466.
- [392] **V. Zimmermann**, M. Bennighof, M. Edel, O. Hofmann, J. Jung und M. von Wick. „‘Home, Smart Home’—Exploring End Users’ Mental Models of Smart Homes“. In: *Mensch & Computer Workshopband* (2018). Hrsg. von R. Dachelt und G. Weber. DOI: 10.18420/muc2018-ws08-0539.

- [393] **V. Zimmermann**, U. Felscher-Suhr und J. Vogt. „Public Perceptions of Frankfurt Airport’s Value – a Survey Approach“. In: *Journal of Air Transport Management* 67 (März 2018), S. 46–54. ISSN: 0969-6997. DOI: 10.1016/j.jairtraman.2017.11.005.
- [394] **N. Alexopoulos**, R. Egert, **T. Grube** und M. Mühlhäuser. „Poster: Towards Automated Quantitative Analysis and Forecasting of Vulnerability Discoveries in Debian GNU/Linux“. In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, London, UK, November 11–15, 2019*. Hrsg. von L. Cavallaro, J. Kinder, X. Wang und J. Katz. Conference on Computer and Communications Security. ACM, Nov. 2019, S. 2677–2679. DOI: 10.1145/3319535.3363285.
- [395] L. Böck, **N. Alexopoulos**, E. Saracoglu, M. Mühlhäuser und **E. Vasilomanolakis**. „Assessing the Threat of Blockchain-Based Botnets“. In: *2019 APWG Symposium on Electronic Crime Research, eCrime 2019, Pittsburgh, PA, USA, November 13–15, 2019*. APWG Symposium on Electronic Crime Research. IEEE, Nov. 2019, S. 1–11. DOI: 10.1109/ECRIME47957.2019.9037600.
- [396] **S. Bretthauer**. „Verfassungsrechtliche Grundlagen des europäischen und nationalen Datenschutzrechts“. In: *Handbuch Europäisches und deutsches Datenschutzrecht*. Hrsg. von L. Specht und R. Mantz. 1. Aufl. Verlag C.H.Beck, 2019, S. 7–37. ISBN: 978-3-406-72539-5.
- [397] **M. Fomichev**, **M. Maass**, **L. Almon**, A. Molina und M. Hollick. „Perils of Zero-Interaction Security in the Internet of Things“. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3.1 (März 2019). Open Access (ePrint), S. 1–38. ISSN: 2474-9567. DOI: 10.1145/3314397. eprint: <https://tuprints.ulb.tu-darmstadt.de/8516/7/paper-ubicomp.pdf>. 
- [398] **M. Fomichev**, **M. Maass** und M. Hollick. „Zero-Interaction Security-towards Sound Experimental Validation“. In: *GetMobile: Mobile Computing and Communications* 23.2 (Nov. 2019). Open Access (arXiv), S. 16–21. ISSN: 2375-0529. DOI: 10.1145/3372300.3372304. arXiv: 1911.07486. 
- [399] M. Funk, **K. Marky**, I. Mizutani, M. Kritzler, S. Mayer und F. Michahelles. „LookUnlock: Using Spatial-Targets for User-Authentication on HMDs“. en. In: *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. CHI ’19: CHI Conference on Human Factors in Computing Systems. Open Access (ePrint). Glasgow Scotland Uk: ACM, 2. Mai 2019, S. 1–6. ISBN: 978-1-4503-5971-9. DOI: 10.1145/3290607.3312959. eprint: <http://www.makufunk.de/wp-content/papercite-data/pdf/funk2019lookunlock.pdf>. 
- [400] **N. Gerber**, **V. Zimmermann** und M. Volkamer. „Why Johnny Fails to Protect His Privacy“. In: *Proceedings of the 4th European Workshop on Usable Security (EuroUSEC 2019)*. 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). Open Access (ePrint). Stockholm, Schweden: IEEE, Juni 2019, S. 109–118. DOI: 10.1109/eurospw.2019.00019. eprint: <https://publikationen.bibliothek.kit.edu/1000096082/81665491>. 
- [401] J. Lamla und **C. Ochs**. „Selbstbestimmungspraktiken in der Datenökonomie: Gesellschaftlicher Widerspruch oder ‚Privates‘ Paradox?“ In: *Paradoxien des Verbraucherverhaltens*. Springer, 2019, S. 25–39. ISBN: 978-3-658-23840-7. DOI: 10.1007/978-3-658-23841-4_3.
- [402] S. Laser und **C. Ochs**. „Kontroversen bewertbar machen“. In: *Digitale Bewertungspraktiken*. Springer, 2019, S. 97–125. ISBN: 978-3-658-21164-6. DOI: 10.1007/978-3-658-21165-3_5.
- [403] **K. Marky**, M. Schmitz, F. Lange und M. Mühlhäuser. „Usability of Code Voting Modalities“. In: *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. Hrsg. von R. L. Mandryk, S. A. Brewster, M. Hancock, G. Fitzpatrick, A. L. Cox, V. Kostakos und M. Perry. Bd. 189. Chi Ea ’19. New York, NY, USA: Association for Computing Machinery, Mai 2019, S. 1–6. ISBN: 978-1-4503-5971-9. DOI: 10.1145/3290607.3312971.
- [404] K. Renaud und **V. Zimmermann**. „Nudging Folks towards Stronger Password Choices: Providing Certainty Is the Key“. In: *Behavioural Public Policy* 3.2 (Nov. 2019), S. 228–258. ISSN: 2398-063X. DOI: 10.1017/bpp.2018.3.
- [405] **A. Wagner** und N. Mesbah. „Too Confident to Care: Investigating Overconfidence in Privacy Decision Making“. In: *ECIS 2019 Proceedings*. Hrsg. von J. vom Brocke, S. Gregor und O. Müller. Publications of Darmstadt Technical University, Institute for Business Studies (BWL). Juni 2019, S. 42. URL: <https://ideas.repec.org/p/dar/wpaper/113206.html>.

- [406] **H. Wenninger.** „Student Assessment of Venture Creation Courses in Entrepreneurship Higher Education – an Interdisciplinary Literature Review and Practical Case Analysis“. In: *Entrepreneurship Education and Pedagogy* 2 (Jan. 2019), S. 58–81. ISSN: 2515-1274.
- [407] **N. Wessels, J. P. Gerlach und A. Wagner.** „To Sell or Not to Sell – Antecedents of Individuals' Willingness-to-Sell Personal Information on Data-Selling Platforms“. In: *ICIS 2019 Proceedings*. Hrsg. von H. Krcmar, J. Fedorowicz, W. F. Boh, J. M. Leimeister und S. Wattal. International Conference on Information Systems. Association for Information Systems, Dez. 2019, S. 34.
- [408] **V. Zimmermann und S. Dekker.** „The 1980s and Onward: Normal Accidents and High Reliability Organizations“. In: *Foundations of Safety Science*. Routledge, 2019, S. 267–304.
- [409] **V. Zimmermann, E. Dickhaut, P. Gerber und J. Vogt.** „Vision: Shining Light on Smart Homes–Supporting Informed Decision-Making of End Users“. In: *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. Bd. 4. 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). Open Access (ePrint). IEEE / IEEE, Juni 2019, S. 149–153. DOI: 10.1109/eurospw.2019.00023. eprint: http://pubs.wi-kasse1.de/wp-content/uploads/2019/10/JML_752.pdf. 
- [410] **V. Zimmermann, P. Gerber, K. Marky, L. Böck und F. Kirchbuchner.** „Assessing Users' Privacy and Security Concerns of Smart Home Technologies“. In: *i-com* 18.3 (Nov. 2019). Open Access, S. 197–216. ISSN: 1618-162X. DOI: 10.1515/icom-2019-0015. 
- [411] **V. Zimmermann und K. Renaud.** „Moving from a 'human-as-Problem' to a 'human-as-Solution' Cybersecurity Mindset“. In: *International Journal of Human-Computer Studies* 131 (Nov. 2019). Open Access (ePrint), S. 169–187. ISSN: 1071-5819. DOI: 10.1016/j.ijhcs.2019.05.005. eprint: https://rke.abertay.ac.uk/files/15927807/Renaud_Moving_from_a_Human_Accepted_2019.pdf. 
- [412] **N. Alexopoulos, S. M. Habib, S. Schulz und M. Mühlhäuser.** „The Tip of the Iceberg: On the Merits of Finding Security Bugs“. In: *ACM Trans. Priv. Secur.* 24.1 (Sep. 2020), 3:1–3:33. ISSN: 2471-2566. DOI: 10.1145/3406112.
- [413] **N. Alexopoulos, E. Vasilomanolakis, S. L. Roux, S. Rowe und M. Mühlhäuser.** „TRIDeNT: Towards a Decentralized Threat Indicator Marketplace“. In: *SAC '20: The 35th ACM/SIGAPP Symposium on Applied Computing, Online Event, [Brno, Czech Republic], March 30 - April 3, 2020*. Hrsg. von C.-C. Hung, T. Cerný, D. Shin und A. Bechini. ACM Symposium on Applied Computing. ACM, März 2020, S. 332–341. DOI: 10.1145/3341105.3374020.
- [414] **S. Bretthauer.** „A European and German Perspective on Data Protection Law in a Digitised World“. Amerikanisch. In: *Comparative Privacy and Defamation*. Hrsg. von A. Koltay und P. Wragg. Section: Comparative Privacy and Defamation. Edward Elgar Publishing, 8. Juli 2020, S. 199–215. ISBN: 978-1-78897-059-4. DOI: 10.4337/9781788970594.00020.
- [415] **S. Bretthauer.** „Die datenschutzbehördliche Informierung als neuartiges Instrument der Aufsichtsbehörden nach Art. 58 Abs. 2 DSGVO“. In: *Recht der Datenverarbeitung*. 2020, S. 245–248.
- [416] **S. Bretthauer.** „Perspektiven des europäischen Katastrophenschutzrechts – Herausforderungen eines vernachlässigten Rechtsgebiets“. In: *Beiheft - Europarecht*. 3. Nomos Verlagsgesellschaft mbH & Co. KG, 2020, S. 133–150.
- [417] **S. Bretthauer und A. A. Schmitt.** „Privatsphärengerechte intelligente Mobilitätssteuerung im Straßenverkehr“. In: *Zeitschrift für Datenschutz - ZD* 7 (2020), S. 341–347. ISSN: 2192-5593.
- [418] **S. Bretthauer und I. Spiecker gen. Döhm.** „Das Digitale-Versorgung-Gesetz als Einfallstor für eine Neujustierung von einstweiligem Rechtsschutz vor dem BVerfG und der Eingriffsqualität bei Datenverwendungen“. In: *JuristenZeitung*. Bd. 75. JuristenZeitung. Mohr Siebeck, 2020, S. 990–996. DOI: 10.1628/jz-2020-0326.
- [419] **S. Bretthauer und I. Spiecker gen. Döhm.** „Die rechtliche Zulässigkeit einer Online-Wahl zur Sozialwahl“. In: *Neue Zeitschrift für Sozialrecht*. 2020, S. 241–247.
- [420] **C. Geminn.** „Betroffenenrechte verbessern – Überarbeitungsbedarf der Datenschutz-Grundverordnung“. In: *Datenschutz und Datensicherheit - DuD* 44.5 (2020), S. 307–311. DOI: 10.1007/s11623-020-1273-5.
- [421] **C. Geminn, J. Szczuka, C. Weber und L. Artelt André / Varonina.** „Kinder als Nutzende smarter Sprachassistenten – Spezieller Gestaltungsbedarf zum Schutz von Kindern“. In: *Datenschutz und Datensicherheit - DuD* 44.9 (2020), S. 600–605. DOI: 10.1007/s11623-020-1332-y.

- [422] **J. Kropf**, „Stratifikation in der digitalen Bewertungsgesellschaft. Eine Fallanalyse der Folge ”Nosediveäus der SF-serie ”Black Mirror““. In: *Berliner Debatte Initial*. Bd. 31. 1. 2020, S. 18–31.
- [423] **O. Kulyk, N. Gerber**, A. Hilt und M. Volkamer. „Has the GDPR Hype Affected Users’ Reaction to Cookie Disclaimers?“ In: *Journal of Cybersecurity* 6.1 (Dez. 2020). Open Access, tyaa022. ISSN: 2057-2085. DOI: 10.1093/cybsec/tyaa022. eprint: <https://academic.oup.com/cybersecurity/article-pdf/6/1/tyaa022/35101886/tyaa022.pdf>. 
- [424] **K. Marky**, S. Prange, F. Krell, M. Mühlhäuser und F. Alt. „You Just Can’t Know about Everything”: Privacy Perceptions of Smart Home Visitors“. In: *Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia*. Hrsg. von J. R. Cauchard und M. Löchtefeld. Mum ’20. New York, NY, USA: Association for Computing Machinery, Nov. 2020, S. 83–95. ISBN: 978-1-4503-8870-2. DOI: 10.1145/3428361.3428464.
- [425] **K. Marky**, M. Schmitz, **V. Zimmermann**, M. Herbers, K. Kunze und M. Mühlhäuser. „3D-auth: Two-factor Authentication with Personalized 3D-printed Items“. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Hrsg. von R. Bernhaupt, F. ’. Mueller, D. Verweij, J. Andres, J. McGrenere, A. Cockburn, I. Avellino, A. Goguy, P. Bjøn, S. Zhao, B. P. Samson und R. Kocielnik. Chi ’20. Open Access. New York, NY, USA: Association for Computing Machinery, Apr. 2020, S. 1–12. ISBN: 978-1-4503-6708-0. DOI: 10.1145/3313831.3376189. 
- [426] **K. Marky**, A. Voit, **A. Stöver**, K. Kunze, S. Schröder und M. Mühlhäuser. „I Don’t Know How to Protect Myself”: Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments“. In: *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*. Hrsg. von D. Lamas, H. Sarapuu, M. Lárusdóttir, J. Stage und C. Ardito. NordiCHI ’20. New York, NY, USA: Association for Computing Machinery, Okt. 2020, S. 1–11. ISBN: 978-1-4503-7579-5. DOI: 10.1145/3419249.3420164.
- [427] **K. Marky, V. Zimmermann**, M. Funk, **J. Daubert**, K. Bleck und M. Mühlhäuser. „Improving the Usability and UX of the Swiss Internet Voting Interface“. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Hrsg. von R. Bernhaupt, F. ’. Mueller, D. Verweij, J. Andres, J. McGrenere, A. Cockburn, I. Avellino, A. Goguy, P. Bjøn, S. Zhao, B. P. Samson und R. Kocielnik. Chi ’20. New York, NY, USA: Association for Computing Machinery, Apr. 2020, S. 1–13. ISBN: 978-1-4503-6708-0. DOI: 10.1145/3313831.3376769.
- [428] **K. Marky, V. Zimmermann, A. Stöver**, P. Hoffmann, K. Kunze und M. Mühlhäuser. „All in One! User Perceptions on Centralized IoT Privacy Settings“. In: *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. Hrsg. von R. Bernhaupt, F. ’. Mueller, D. Verweij, J. Andres, J. McGrenere, A. Cockburn, I. Avellino, A. Goguy, P. Bjøn, S. Zhao, B. P. Samson und R. Kocielnik. Chi Ea ’20. New York, NY, USA: Association for Computing Machinery, Apr. 2020, S. 1–8. ISBN: 978-1-4503-6819-3. DOI: 10.1145/3334480.3383016.
- [429] **K. Marky**, M.-L. Zollinger, M. Funk, P. Y. A. Ryan und M. Mühlhäuser. „How to Assess the Usability Metrics of E-Voting Schemes“. In: *Financial Cryptography and Data Security*. Hrsg. von A. Bracciali, J. Clark, F. Pintore, P. B. Rønne und M. Sala. Bd. 11599. Open Access (ePrint). Cham: Springer International Publishing, 2020, S. 257–271. ISBN: 978-3-030-43724-4 978-3-030-43725-1. DOI: 10.1007/978-3-030-43725-1_18. eprint: <https://fc19.ifca.ai/voting/papers/MZFRM19.pdf>. 
- [430] **C. Ochs, B. Büttner** und J. Lamla. „Trading Social Visibility for Economic Amenability: Data-based Value Translation on a ”Health and Fitness Platform““. Englisch. In: *Science, Technology, & Human Values* 46.3 (24. Juni 2020), S. 480–506. ISSN: 0162-2439. DOI: 10.1177/0162243920928138.
- [431] A. Roßnagel und **C. Geminn**. *Datenschutz-Grundverordnung verbessern – Änderungsvorschläge aus Verbrauchersicht*. Der Elektronische Rechtsverkehr Bd. 43. Baden-Baden: Nomos, 2020.
- [432] **T. Schürmann, N. Gerber** und **P. Gerber**. „Benefits of Formalized Computational Modeling for Understanding User Behavior in Online Privacy Research“. In: *Journal of Intellectual Capital* 21.3 (März 2020), S. 431–458. ISSN: 1469-1930. DOI: 10.1108/jic-05-2019-0126.
- [433] **V. Zimmermann** und **N. Gerber**. „The Password Is Dead, Long Live the Password—A Laboratory Study on User Perceptions of Authentication Schemes“. In: *International Journal of Human-Computer Studies* 133 (Jan. 2020), S. 26–44. ISSN: 1071-5819. DOI: 10.1016/j.ijhcs.2019.08.006.

- [434] **N. Alexopoulos**, A. Meneely, D. Arnouts und M. Mühlhäuser. „Who Are Vulnerability Reporters?: A Large-Scale Empirical Study on FLOSS“. In: *ESEM '21: ACM / IEEE International Symposium on Empirical Software Engineering and Measurement, Bari, Italy, October 11-15, 2021*. Hrsg. von F. Lanubile, M. Kalinowski und M. T. Baldassarre. International Symposium on Empirical Software Engineering and Measurement. ACM, Okt. 2021, 25:1–25:12. DOI: 10.1145/3475716.3475783.
- [435] **T. Biselli** und C. Reuter. „On the Relationship between IT Privacy and Security Behavior: A Survey among German Private Users“. In: *Proceedings of the International Conference on Wirtschaftsinformatik (WI)*. Wirtschaftsinformatik. Open Access (ePrint). Potsdam, Germany: AIS, 2021, S. 1–17. ISBN: 978-3-030-86796-6. DOI: 10.1007/978-3-030-86797-3_26. eprint: <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1200&context=wi2021>.
- [436] **S. Bretthauer**. „Befugnisse des Staates nach dem Infektionsschutzgesetz“. In: *Religionsfreiheit in Seuchenzeiten*. Hrsg. von S. Mückl. 2021, S. 61–83. URL: <https://publikationen.bibliothek.kit.edu/1000139482>.
- [437] **S. Bretthauer**. „Herausforderungen der Digitalisierung im Gesundheitswesen – Corona-Warn-App, Forschungsdaten und Künstliche Intelligenz“. In: *Die Verwaltung*. Bd. 54. 2021, S. 411–441.
- [438] **S. Bretthauer**. „Online-Wahlen zu Parlamenten als modernes Instrument demokratischer Partizipation in Zeiten von Pandemie und Digitalisierung“. In: *Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft*. Bd. 104. Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft 1. Open Access. Nomos Verlag, 2021, S. 3–33. URL: <https://www.nomos-e-library.de/10.5771/2193-7869-2021-1-3.pdf>.
- [439] **S. Bretthauer**, A. Appenzeller und P. Birnstill. „Datensouveränität für Patienten im Gesundheitswesen – Eine Chance für die medizinische Forschung und den Datenschutz“. In: *Datenschutz und Datensicherheit - DuD* 45.3 (1. März 2021), S. 173–179. ISSN: 1862-2607. DOI: 10.1007/s11623-021-1413-6.
- [440] **S. Bretthauer**, **D. Müllmann** und I. Spiecker gen. Döhm. „Datenschutzrechtliche Aspekte neuer Mobilitätskonzepte im öffentlichen Nahverkehr“. In: *Studien zum Datenschutz*. Bd. 61. Baden-Baden: Nomos, 2021. ISBN: 978-3-7489-2638-2. DOI: 10.5771/9783748926382.
- [441] R. Egert, **J. Daubert**, S. Marsh und M. Mühlhäuser. „Exploring Energy Grid Resilience: The Impact of Data, Prosumer Awareness, and Action“. In: *Patterns* 2.6 (Juni 2021). Open Access, S. 100258. ISSN: 2666-3899. DOI: 10.1016/j.patter.2021.100258.
- [442] K. Erenli, **C. Geminn** und L. Pfeiffer. „Legal Challenges of an Open Web Index“. In: *International Cybersecurity Law Review* 2.1 (März 2021). Open Access, S. 183–194. ISSN: 2662-9720. DOI: 10.1365/s43439-021-00017-8.
- [443] **M. Fomichev**, L. F. Abanto-Leon, M. Stiegler, A. Molina, J. Link und M. Hollick. „Next2You: Robust Copresence Detection Based on Channel State Information“. In: *ACM Transactions on Internet of Things* 1.1 (Nov. 2021). Open Access (arXiv), S. 1–30. DOI: 10.1145/3491244. arXiv: 2111.05224.
- [444] **M. Fomichev**, J. Hesse, **L. Almon**, T. Lippert, J. Han und M. Hollick. „FastZIP: Faster and More Secure Zero-Interaction Pairing“. In: *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*. Hrsg. von S. Banerjee, L. Mottola und X. Zhou. ACM SIGMOBILE International Conference on Mobile Systems, Applications, and Services. Open Access (arXiv). ACM, Juni 2021, S. 440–452. DOI: 10.1145/3458864.3467883. arXiv: 2106.04907.
- [445] A. Franz, **V. Zimmermann**, G. Albrecht, K. Hartwig, C. Reuter, A. Benlian und J. Vogt. „{SoK}: Still Plenty of Phish in the Sea—a Taxonomy of {user-Oriented} Phishing Interventions and Avenues for Future Research“. In: *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. Hrsg. von S. Chiasson. Symposium On Usable Privacy and Security. USENIX Association, Aug. 2021, S. 339–358. URL: <https://www.usenix.org/system/files/soups2021-franz.pdf>.
- [446] **S. A. Gaballah**, C. Coijanovic, T. Strufe und M. Mühlhäuser. „2PPS - Publish/Subscribe with Provable Privacy“. In: *40th International Symposium on Reliable Distributed Systems, SRDS 2021, Chicago, IL, USA, September 20-23, 2021*. Bd. abs 1902 6306. IEEE International Symposium on Reliable Distributed Systems. Open Access (arXiv). IEEE, Sep. 2021, S. 198–209. DOI: 10.1109/SRDS53918.2021.00028. arXiv: 2108.08624.
- [447] **C. Geminn**. „Datenschutz bei Sprachassistenten – Herausforderungen heute und morgen“. In: *Datenschutz und Datensicherheit - DuD* 45.8 (2021), S. 509–514. DOI: 10.1007/s11623-021-1481-7.

- [448] **C. Geminn.** „Die Regulierung Künstlicher Intelligenz – Anmerkungen zum Entwurf eines Artificial Intelligence Act“. In: *Zeitschrift für Datenschutz - ZD* 45.7 (2021), S. 354–359.
- [449] **P. Gerber**, M. Heidinger, J. Stieglmayer und **N. Gerber.** „LOKI: Development of an Interface for Task-Based, Privacy-Friendly Smart Home Control through Local Information Processing: LOKI: Entwicklung eines Interfaces für die aufgaben-basierte, privatsphäre-freundliche Smart Home-Steuerung durch lokale Informationsverarbeitung“. In: *Proceedings of Mensch und Computer 2021*. 2021, S. 578–581.
- [450] **K. Marky**, M.-L. Zollinger, P. Roenne, P. Y. A. Ryan, **T. Grube** und K. Kunze. „Investigating Usability and User Experience of Individually Verifiable Internet Voting Schemes“. In: *ACM Trans. Comput.-Hum. Interact.* 28.5 (Sep. 2021), S. 1–36. ISSN: 1073-0516. DOI: 10.1145/3459604.
- [451] **C. Ochs.** „Digital Infrastructures Suck: Zur digitalen Absorption des Sozialen“. In: *Hamburger Journal für Kultur-anthropologie (HJK)* 13.13 (29. Juli 2021). Open Access, S. 127–138. ISSN: 2365-1016. URL: <https://journals.sub.uni-hamburg.de/hjk/article/view/1728> (besucht am 27. 09. 2024). 
- [452] **C. Ochs.** „Privacies in Practice“. In: *Connect & Divide: The Practice Turn in Media Studies*. Hrsg. von U. Bergermann, M. Dommann, E. Schüttpelz und J. Stölow. Zurich: Diaphanes, 2021, S. 277–294.
- [453] A. Roßnagel und **C. Geminn.** „Vertrauen in Anonymisierung – Regulierung der Anonymisierung zur Förderung Künstlicher Intelligenz“. In: *Zeitschrift für Datenschutz - ZD* 9 (2021), S. 487–490.
- [454] **C. von Wintzingerode**, **D. Müllmann** und I. Spiecker gen. Döhm. „Ein Netzwerk für Europas Cybersicherheit“. In: *Neue Zeitschrift für Verwaltungsrecht* 40.10 (2021). Open Access, S. 690–695. ISSN: 0721-880X. DOI: 10.5445/IR/1000138349. 
- [455] **A. Wagner**, **N. Wessels**, H. Brakemeier und P. Buxmann. „Why Free Does Not Mean Fair: Investigating Users’ Distributive Equity Perceptions of Data-Driven Services“. In: *International Journal of Information Management* 59 (Aug. 2021), S. 102333. ISSN: 02684012. DOI: 10.1016/j.ijinfomgt.2021.102333.
- [456] L. M. Zankel, **P. Gerber**, **V. Zimmermann** und **N. Gerber.** „Taking on Driving Tasks Yourself? That Was Yesterday! How Drivers Would like to Be Supported by Assistance Systems“. In: *13th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*. ACM, Sep. 2021, S. 71–76. DOI: 10.1145/3473682.3480267.
- [457] **V. Zimmermann** und K. Renaud. „The Nudge Puzzle: Matching Nudge Interventions to Cybersecurity Decisions“. In: *ACM Transactions on Computer-Human Interaction (TOCHI)* 28.1 (2021), S. 1–45. DOI: 10.1145/3429888.
- [458] **N. Alexopoulos**, M. Brack, J. P. Wagner, **T. Grube** und M. Mühlhäuser. „How Long Do Vulnerabilities Live in the Code? A Large-Scale Empirical Measurement Study on FOSS Vulnerability Lifetimes“. In: *31st USENIX Security Symposium, USENIX Security 2022, Boston, MA, USA, August 10-12, 2022*. Hrsg. von K. R. B. Butler und K. Thomas. USENIX Security Symposium. Open Access. USENIX Association, 2022, S. 359–376. ISBN: 978-1-939133-31-1. URL: <https://www.usenix.org/conference/usenixsecurity22/presentation/alexopoulos>. 
- [459] P. Bekaert, N. Alotaibi, F. Mathis, **N. Gerber**, A. C. Rafferty, M. Khamis und **K. Marky.** „Are Thermal Attacks a Realistic Threat? Investigating the Preconditions of Thermal Attacks in Users’ Daily Lives“. In: *Nordic Human-Computer Interaction Conference*. Nordic Conference on Human-Computer Interaction. Open Access. ACM, Okt. 2022, S. 1–9. DOI: 10.1145/3546155.3546706. 
- [460] **T. Biselli**, **E. Steinbrink**, F. Herbert, G. M. Schmidbauer-Wolf und C. Reuter. „On the Challenges of Developing a Concise Questionnaire to Identify Privacy Personas“. In: *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2022.4 (Okt. 2022). Open Access, S. 645–669. ISSN: 2299-0984. DOI: 10.56553/popets-2022-0126. 
- [461] **S. Bretthauer.** „Extended Powers for Other Supervisory Authorities Concerned in the Case of Cross-Border Data Processing: Facebook Ireland“. In: *Common Market Law Review*. Bd. 59. Common Market Law Review Issue 5. Kluwer Law International BV, Okt. 2022, S. 1543–1556. DOI: 10.54648/cm1a2022101.
- [462] **S. Bretthauer.** „Kommentierung §§ 61-68 SGB VIII - Schutz von Sozialdaten in der Kinder- und Jugendhilfe“. In: *beck.online-Großkommentar*. Hrsg. von B. Gsell, W. Krüger, S. Lorenz und C. Reymann. 2022.
- [463] M. Friedewald, A. Roßnagel, T. Bile, **C. Geminn**, M. Hansen, F. Bieker und M. Karaboga. „Zur Einführung einer Überwachungsgesamtrechnung“. In: *Datenschutz und Datensicherheit - DuD* 46.9 (2022), S. 572–577. DOI: 10.1007/s11623-022-1661-0.

- [464] **S. A. Gaballah**, L. Abdullah, M. T. Tran, **E. Zimmer** und M. Mühlhäuser. „On the Effectiveness of Intersection Attacks in Anonymous Microblogging“. In: *Secure IT Systems - 27th Nordic Conference, NordSec 2022, Reykjavic, Iceland, November 30-December 2, 2022, Proceedings*. Hrsg. von H. P. Reiser und M. Kyas. Bd. 13700. Lecture Notes in Computer Science. Springer, 2022, S. 3–19. ISBN: 978-3-031-22294-8. DOI: 10.1007/978-3-031-22295-5_1.
- [465] **N. Gerber** und **K. Marky**. „The Nerd Factor: The Potential of S&P Adepts to Serve as a Social Resource in the User's Quest for More Secure and Privacy-Preserving Behavior“. In: *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. Open Access. Boston, MA, USA: USENIX Association, Aug. 2022, S. 57–76. ISBN: 978-1-939133-30-4. URL: <https://www.usenix.org/conference/soups2022/presentation/gerber>. 
- [466] **K. Marky**, **N. Gerber**, M. G. Pelzer, M. Khamis und M. Mühlhäuser. „You Offer Privacy like You Offer Tea: Investigating Mechanisms for Improving Guest Privacy in IoT-equipped Households“. In: *Proceedings on Privacy Enhancing Technologies (PoPETs) 2022.4* (Okt. 2022). Open Access, S. 400–420. ISSN: 2299-0984. DOI: 10.56553/popets-2022-0115. 
- [467] **K. Marky**, **P. Gerber**, S. Günther, M. Khamis, M. Fries und M. Mühlhäuser. „Investigating State-of-the-Art Practices for Fostering Subjective Trust in Online Voting through Interviews“. In: *31st USENIX Security Symposium (USENIX Security 22)*. Hrsg. von K. R. B. Butler und K. Thomas. USENIX Security Symposium. Boston, MA: USENIX Association, Aug. 2022, S. 4059–4076. ISBN: 978-1-939133-31-1. URL: <https://www.usenix.org/conference/usenixsecurity22/presentation/marky>.
- [468] **K. Marky**, S. Prange, M. Mühlhäuser und F. Alt. „Roles Matter! Understanding Differences in the Privacy Mental Models of Smart Home Visitors and Residents“. In: *Proceedings of the 20th International Conference on Mobile and Ubiquitous Multimedia*. Mum '21. New York, NY, USA: Association for Computing Machinery, 2022, S. 108–122. ISBN: 978-1-4503-8643-2. DOI: 10.1145/3490632.3490664.
- [469] **K. Marky**, K. Ragozin, G. Chernyshov, A. Matviienko, M. Schmitz, M. Mühlhäuser, C. Egtebas und K. Kunze. „Nah, It's Just Annoying!“ a Deep Dive into User Perceptions of Two-Factor Authentication“. In: *ACM Trans. Comput.-Hum. Interact.* 29.5 (Okt. 2022), S. 1–32. ISSN: 1073-0516. DOI: 10.1145/3503514.
- [470] **C. Ochs**. „Be-handeln und De-aktivieren: Ein empirischer Beitrag zur Erweiterung soziomaterieller Agency-Konzeptionen am Fall einer ‚Fitness-App‘“. In: *BEHEMOTH: A Journal on Civilization* 15.1 (2022). Open Access, S. 74–90. DOI: 10.6094/behemoth.2022.15.1.1074. 
- [471] A. Roßnagel, **C. Geminn**, P. C. Johannes und J. K. M. Müller. „Auswirkungen ausländischer Gesetzgebung auf deutsche IT-Sicherheit“. In: *Datenschutz und Datensicherheit - DuD* 46.3 (2022), S. 156–163. DOI: 10.1007/s11623-022-1581-z.
- [472] **V. Zimmermann**, J. Haunschild, M. Unden, **P. Gerber** und **N. Gerber**. „Sicherheits Herausforderungen für Smart-City-Infrastrukturen“. In: *Wirtschaftsinformatik & Management* 14.2 (Apr. 2022). Open Access, S. 119–126. ISSN: 1867-5905. DOI: 10.1365/s35764-022-00396-5. 
- [473] **S. Bretthauer**. „Datenschutzrechtliche Bußgelder – Unternehmerisches Risiko und Behördliches Governance-Instrument“. In: *Computer und Recht*. Bd. 39. Computer und Recht. Verlag Dr. Otto Schmidt, Jan. 2023, S. 22–29. DOI: 10.9785/cr-2023-390111.
- [474] **S. Bretthauer**. „Kommentierung Art. 4 Nr. 16, Art. 4 Nr. 21, Art. 4 Nr. 22, Art. 4 Nr. 23“. In: *Commentary on the European General Data Protection Regulation*. Hrsg. von I. Spiecker gen. Döhmman, V. Papakonstantinou, G. Hornung und P. de Hert. 2023.
- [475] S. Dekker, **V. Zimmermann** und D. D. Woods. „High-Reliability Organizations Invest in Resilience“. In: *Human Factors in Aviation and Aerospace*. Elsevier, 2023, S. 41–57. ISBN: 978-0-12-420139-2. DOI: 10.1016/b978-0-12-420139-2.00006-x.
- [476] S. Drewes und **S. Bretthauer**. „Kommentierung Art. 4 Nr. 18, Art. 4 Nr. 19 sowie Artt. 37–39“. In: *Commentary on the European General Data Protection Regulation*. Hrsg. von I. Spiecker gen. Döhmman, V. Papakonstantinou, G. Hornung und P. de Hert. 2023.
- [477] N. Ebert, T. Schaltegger, B. Ambuehl, L. Schöni, **V. Zimmermann** und M. Knieps. „Learning from Safety Science: A Way Forward for Studying Cybersecurity Incidents in Organizations“. In: *Computers & Security* 134 (Nov. 2023). Open Access, S. 103435. ISSN: 0167-4048. DOI: 10.1016/j.cose.2023.103435. 

- [478] **M. Fomichev**. „A Path to Holistic Privacy in Stream Processing Systems“. In: *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services*. Hrsg. von P. Nurmi, P. Hui, A. A. Sani und Y. Liu. ACM SIGMOBILE International Conference on Mobile Systems, Applications, and Services. Open Access (arXiv). New York, NY, USA: Association for Computing Machinery, Juni 2023, S. 627–628. ISBN: 9798400701108. DOI: 10.1145/3581791.3597510. arXiv: 2305.11638. 
- [479] **M. Fomichev**, M. Luthra, M. Benndorf und P. Agnihotri. „No One Size (PPM) Fits All: Towards Privacy in Stream Processing Systems“. In: *Proceedings of the 17th ACM International Conference on Distributed and Event-Based Systems*. Hrsg. von V. Schiavoni, M. Pasin, B. Kemme und E. Rivière. Distributed Event-Based Systems. Open Access (ePrint). New York, NY, USA: Association for Computing Machinery, Juni 2023, S. 61–67. ISBN: 9798400701221. DOI: 10.1145/3583678.3596889. eprint: <https://www.duo.uio.no/bitstream/10852/108887/1/2305.00871.pdf>. 
- [480] **S. A. Gaballah**, T. H. L. Nguyen, L. Abdullah, **E. Zimmer** und M. Mühlhäuser. „Mitigating Intersection Attacks in Anonymous Microblogging“. In: *Proceedings of the 18th International Conference on Availability, Reliability and Security, ARES 2023, Benevento, Italy, 29 August 2023–1 September 2023*. ARES. Open Access (arXiv). ACM, Aug. 2023, 8:1–8:11. DOI: 10.1145/3600160.3600166. arXiv: 2307.09069. 
- [481] **C. Geminn**. *Deus ex machina? – Grundrechte und Digitalisierung*. Jus Publicum – Beiträge zum öffentlichen Recht Bd. 316. zugleich: Habilitationsschrift, Universität Kassel, 2021. Tübingen: Mohr Siebeck, 2023.
- [482] **C. Geminn** und T. T. H. Pham. „Das vietnamesische Datenschutzrecht – Neuerungen durch das Dekret Nr. 13/2023/ND-CP“. In: *Zeitschrift für Datenschutz – ZD* 8 (2023), S. 440–446.
- [483] **N. Gerber** und **A. Stöver**. „From the Privacy Calculus to Crossing the Rubicon: An Introduction to Theoretical Models of User Privacy Behavior“. In: *Human Factors in Privacy Research*. Open Access. Springer, 2023, S. 11–25. ISBN: 978-3-031-28642-1. DOI: 10.1007/978-3-031-28643-8_2. 
- [484] **N. Gerber**, **A. Stöver** und **K. Marky**. *Human Factors in Privacy Research*. Open Access. Springer Nature, 2023. ISBN: 978-3-031-28642-1. DOI: 10.1007/978-3-031-28643-8. 
- [485] **N. Gerber**, **A. Stöver**, J. Peschke und **V. Zimmermann**. „Don't Accept All and Continue: Exploring Nudges for More Deliberate Interaction with Tracking Consent Notices“. In: *ACM Trans. Comput.-Hum. Interact.* 31.1 (Nov. 2023), S. 1–36. ISSN: 1073-0516. DOI: 10.1145/3617363.
- [486] C. Johannes Paul C. / Geminn und **M. Nebel**. „Learning Analytics nach Satzung – Rechtssicherer Einsatz durch Hochschulen“. In: *Datenschutz und Datensicherheit – DuD* 47.11 (2023), S. 715–720. DOI: 10.1007/s11623-023-1849-y.
- [487] **K. Marky**, S. Macdonald, Y. Abdrabou und M. Khamis. „In the Quest to Protect Users from Side-Channel Attacks – a User-Centred Design Space to Mitigate Thermal Attacks on Public Payment Terminals“. In: *32nd USENIX Security Symposium (USENIX Security 23)*. Hrsg. von J. A. Calandrino und C. Troncoso. USENIX Security Symposium. Anaheim, CA: USENIX Association, Aug. 2023, S. 5235–5252. ISBN: 978-1-939133-37-3. URL: <https://www.usenix.org/conference/usenixsecurity23/presentation/marky>.
- [488] R. Panskus, M. Ninow, S. Fahl und **K. Marky**. „Privacy Mental Models of Electronic Health Records: A German Case Study“. In: *Proceedings of the Nineteenth USENIX Conference on Usable Privacy and Security*. Hrsg. von P. G. Kelley und A. Kapadia. Soups '23. USA: USENIX Association, 2023. ISBN: 978-1-939133-36-6.
- [489] C. Reuter, M.-A. Kaufhold, **T. Biselli** und H. Pleil. „Increasing Adoption Despite Perceived Limitations of Social Media in Emergencies: Representative Insights on German Citizens' Perception and Trends from 2017 to 2021“. In: *International Journal of Disaster Risk Reduction (IJDRR)* 96 (Aug. 2023), S. 103880. ISSN: 2212-4209. DOI: 10.1016/j.ijdr.2023.103880.
- [490] T. Riebe, **T. Biselli**, M.-A. Kaufhold und C. Reuter. „Privacy Concerns and Acceptance Factors of OSINT for Cybersecurity: A Representative Survey“. In: *Proceedings on Privacy Enhancing Technologies (PoPETs) 2023.1* (Jan. 2023). Open Access, S. 477–493. ISSN: 2299-0984. DOI: 10.56553/popets-2023-0028. 

- [491] E. Sapin, S. Menon, J. Ge, **S. M. Habib**, M. Heymann, Y. Li, R. Palige, G. Byman und Y. Liu. „Monitoring Automotive Software Security Health through Trustworthiness Score“. In: *Proceedings of the 7th ACM Computer Science in Cars Symposium, CSCS 2023, Darmstadt, Germany, 5 December 2023*. Hrsg. von B. Brücher, C. Krauß, M. Fritz, H.-J. Hof und O. Wasenmüller. Cscs '23. New York, NY, USA: Association for Computing Machinery, Dez. 2023, S. 1–9. ISBN: 9798400704543. DOI: 10.1145/3631204.3631859.
- [492] M. Turner, M. Schmitz, M. M. Bierey, M. Khamis und **K. Marky**. „Tangible 2FA: An in-the-Wild Investigation of User-Defined Tangibles for Two-Factor Authentication“. In: *Proceedings of the Nineteenth USENIX Conference on Usable Privacy and Security*. Hrsg. von P. G. Kelley und A. Kapadia. Soups '23. USA: USENIX Association, 2023. ISBN: 978-1-939133-36-6.
- [493] **V. Zimmermann**. „Privacy Nudges and Informed Consent? Challenges for Privacy Nudge Design“. In: *Human Factors in Privacy Research*. Open Access. Springer International Publishing Cham, 2023, S. 155–171. ISBN: 978-3-031-28642-1. DOI: 10.1007/978-3-031-28643-8_8. 
- [494] **V. Zimmermann**. „Smart Cities as a Testbed for Experimenting with Humans?—Applying Psychological Ethical Guidelines to Smart City Interventions“. In: *Ethics and Information Technology* 25.4 (Okt. 2023). Open Access, S. 54. ISSN: 1388-1957. DOI: 10.1007/s10676-023-09729-3. 
- [495] **V. Zimmermann**, **K. Marky** und K. Renaud. „Hybrid Password Meters for More Secure Passwords—a Comprehensive Study of Password Meters Including Nudges and Password Information“. In: *Behaviour & Information Technology* 42.6 (Apr. 2023), S. 700–743. ISSN: 0144-929X.
- [496] **T. Biselli**, L. Utz und C. Reuter. „Supporting Informed Choices about Browser Cookies: The Impact of Personalised Cookie Banners“. In: *Proceedings on Privacy Enhancing Technologies (PoPETs) 2024.1* (Jan. 2024). Open Access, S. 171–191. ISSN: 2299-0984. DOI: 10.56553/popets-2024-0011. 
- [497] **S. Bretthauer**. „Das Digital-Gesetz – Zentrale Neuerungen zur Beschleunigung der Digitalisierung des Gesundheitswesens“. In: *Neue Zeitschrift für Verwaltungsrecht*. 2024, S. 1047–1055.
- [498] S. Delgado Rodriguez, P. Chatterjee, A. Dao Phuong, F. Alt und **K. Marky**. „Do You Need to Touch? Exploring Correlations between Personal Attributes and Preferences for Tangible Privacy Mechanisms“. In: *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. Hrsg. von F. ' Mueller, P. Kyburz, J. R. Williamson, C. Sas, M. L. Wilson, P. O. T. Dugas und I. Shklovski. Chi '24. Open Access. New York, NY, USA: Association for Computing Machinery, Mai 2024, S. 1–23. ISBN: 9798400703300. DOI: 10.1145/3613904.3642863.
- [499] K. Demuth, S. Linsner, **T. Biselli**, M.-A. Kaufhold und C. Reuter. „Support Personas: A Concept for Tailored Support of Users of Privacy-Enhancing Technologies“. In: *Proceedings on Privacy Enhancing Technologies (PoPETs) 2024.4* (Okt. 2024). Open Access, S. 797–817. ISSN: 2299-0984. DOI: 10.56553/popets-2024-0142. 
- [500] H. Farzand, **K. Marky** und M. Khamis. „Out-of-Device Privacy Unveiled: Designing and Validating the out-of-Device Privacy Scale (ODPS)“. In: *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. Hrsg. von F. ' Mueller, P. Kyburz, J. R. Williamson, C. Sas, M. L. Wilson, P. O. T. Dugas und I. Shklovski. Chi '24. Open Access. New York, NY, USA: Association for Computing Machinery, Mai 2024, S. 1–15. ISBN: 9798400703300. DOI: 10.1145/3613904.3642623. 
- [501] **S. A. Gaballah**, L. Abdullah, M. Alishahi, T. H. L. Nguyen, **E. Zimmer**, M. Mühlhäuser und **K. Marky**. „Anonify: Decentralized Dual-Level Anonymity for Medical Data Donation“. In: *Proc. Priv. Enhancing Technol.* 2024.3 (Juli 2024). Open Access, S. 94–108. ISSN: 2299-0984. DOI: 10.56553/POPETS-2024-0069. 
- [502] **S. A. Gaballah**, L. Abdullah, M. Mühlhäuser und **K. Marky**. „Let the Users Choose: Low Latency or Strong Anonymity? Investigating Mix Nodes with Paired Mixing Techniques“. In: *Proceedings of the 19th International Conference on Availability, Reliability and Security, ARES 2024, Vienna, Austria, 30 July 2024 - 2 August 2024*. Bd. 1. ARES. ACM, Juli 2024, 2:1–2:11. DOI: 10.1145/3664476.3664516.
- [503] **N. Gerber**, **A. Stöver** und P. Mayer. „Of Mothers and Managers – the Effect of Videos Depicting Gender Stereotypes on Women and Men in the Security and Privacy Field“. In: *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. Hrsg. von P. G. Kelley und A. Kapadia. SOUPS @ USENIX Security Symposium. Open Access. Philadelphia, PA: USENIX Association, Aug. 2024, S. 547–566. ISBN: 978-1-939133-42-7. URL: <https://www.usenix.org/conference/soups2024/presentation/gerber>. 

- [504] P. Grassl, **N. Gerber** und M. von Grafenstein. „How Effectively Do Consent Notices Inform Users about the Risks to Their Fundamental Rights?“ In: *European Data Protection Law Review* 10.1 (2024), S. 96–104. ISSN: 2364-284X. DOI: 10.21552/edpl/2024/1/14.
- [505] I. Habernal, D. Faber, N. Recchia, **S. Bretthauer**, I. Gurevych, I. Spiecker gen. Döhmman und C. Burchard. „Mining Legal Arguments in Court Decisions“. Englisch. In: *Artificial Intelligence and Law* 32.3 (1. Sep. 2024). Open Access, S. 1–38. ISSN: 1572-8382. DOI: 10.1007/s10506-023-09361-y. 
- [506] K. Hartwig, **T. Biselli**, F. Schneider und C. Reuter. „From Adolescents’ Eyes: Assessing an Indicator-Based Intervention to Combat Misinformation on TikTok“. In: *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. Hrsg. von F. ’. Mueller, P. Kyburz, J. R. Williamson, C. Sas, M. L. Wilson, P. O. T. Dugas und I. Shklovski. CHI ’24. Open Access (ePrint). New York, NY, USA: Association for Computing Machinery, Mai 2024, S. 1–20. ISBN: 9798400703300. DOI: 10.1145/3613904.3642264. eprint: https://peasec.de/paper/2024/2024_HartwigBiselliSchneiderReuter_MisinfoTikTok_CHI.pdf. 
- [507] K. Hartwig, S. Schmid, **T. Biselli**, H. Pleil und C. Reuter. „Misleading Information in Crises: Exploring Content-specific Indicators on Twitter from a User Perspective“. In: *Behaviour & Information Technology (BIT)* (Juli 2024). Open Access, S. 1–34. ISSN: 0144-929X. DOI: 10.1080/0144929X.2024.2373166. 
- [508] J. Hielscher, M. Schöps, J. Opdenbusch, F. Reichmann, M. Gutfleisch, **K. Marky** und S. Parkin. „Selling Satisfaction: A Qualitative Analysis of Cybersecurity Awareness Vendors’ Promises“. en. In: *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*. CCS ’24: ACM SIGSAC Conference on Computer and Communications Security. Open Access. Salt Lake City UT USA: ACM, 2. Dez. 2024, S. 2666–2680. ISBN: 9798400706363. DOI: 10.1145/3658644.3690196. 
- [509] S. Klivan, S. Höltervennhoff, R. Panskus, **K. Marky** und S. Fahl. „Everyone for Themselves? A Qualitative Study about Individual Security Setups of Open Source Software Contributors“. In: *2024 IEEE Symposium on Security and Privacy (SP)*. Bd. 17. IEEE Symposium on Security and Privacy. Open Access (ePrint). IEEE / IEEE, Mai 2024, S. 1065–1082. DOI: 10.1109/sp54263.2024.00214. eprint: <https://saschafahl.de/static/paper/oss2024.pdf>. 
- [510] **K. Marky**, **N. Gerber**, H. J. Krumb, M. Khamis und M. Mühlhäuser. „Investigating Voter Perceptions of Printed Physical Audit Trails for Online Voting“. In: *2024 IEEE Symposium on Security and Privacy (SP)*. Bd. 2. IEEE Symposium on Security and Privacy. IEEE / IEEE Computer Society, Mai 2024, S. 136–136. DOI: 10.1109/sp54263.2024.00136.
- [511] **K. Marky**, **A. Stöver**, S. Prange, K. Bleck, **P. Gerber**, **V. Zimmermann**, F. Mueller, F. Alt und M. Mühlhäuser. „Decide Yourself or Delegate – User Preferences Regarding the Autonomy of Personal Privacy Assistants in Private IoT-equipped Environments“. In: *Proceedings of the CHI Conference on Human Factors in Computing Systems*. Hrsg. von F. ’. Mueller, P. Kyburz, J. R. Williamson, C. Sas, M. L. Wilson, P. O. T. Dugas und I. Shklovski. Bd. 9. Chi ’24. Open Access. New York, NY, USA: ACM, Mai 2024, S. 1–20. ISBN: 9798400703300. DOI: 10.1145/3613904.3642591. 
- [512] **C. Ochs**. „Deep Targeting: Zur Steigerung der Eingriffstiefe in die Erfahrungsspielräume des Sozialen“. In: *Zeitschrift für Soziologie* 53.1 (2024). Open Access, S. 73–88. ISSN: 2366-0325. DOI: 10.1515/zfsoz-2024-2007. 
- [513] **F. Pittroff**. „Die private und die verteilte Person: Studien zu Personalisierung und Privatheit in Zeiten der Digitalisierung“. In: *Digitale Soziologie*. Open Access. transcript Verlag, Jan. 2024. ISBN: 978-3-8394-7181-4. DOI: 10.14361/9783839471814. 

Weitere Publikationen und öffentlich gemachte Ergebnisse

- [514] **B. Büttner**, **C. L. Geminn**, T. Hagendorff, J. Lamla, S. Ledder, **C. Ochs** und **F. Pittroff**. *Die Reterritorialisierung des Digitalen: Zur Reaktion nationaler Demokratie auf die Krise der Privatheit nach Snowden*. Open Access. Kassel University Press, Mai 2016. DOI: 10.19211/kup9783862191079. 
- [515] **J. Daubert**. „Anonymous Publish-Subscribe Overlays“. Diss. Darmstadt University of Technology, Germany, 2016, S. 1–175. URL: <http://tuprints.ulb.tu-darmstadt.de/5473/>.
- [516] **C. Ochs**. „Local Digital Practices, Worldwide“. In: *Handbuch Soziale Praktiken und Digitale Alltagswelten*. Hrsg. von H. Friese, G. Rebane, M. Nolden und M. Schreiter. Überarbeitete Version für aktualisierte Auflage des Handbuchs, ursprünglich veröffentlicht 2016. Wiesbaden: Springer Fachmedien, 2016, S. 1–11. ISBN: 978-3-658-08460-8. DOI: 10.1007/978-3-658-08460-8_13-1.

- [517] A. Rossnagel, **C. Geminn**, **S. Jandt** und **P. Richter**. *Datenschutzrecht 2016 „smart“ genug für die Zukunft?: Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts*. Bd. 4. ITeG - Interdisciplinary Research on Information System Design. Monographie (220 S.), Open Access. Kassel University Press, 2016. DOI: 10.19211/KUP9783737601559. 
- [518] **H. E. Wenninger**. „Der Einfluss sozialer Online-Netzwerke auf ihre Mitglieder - Eine Analyse von Nutzungsarten und sozialen Mechanismen“. Diss. Federal Reserve Bank of St. Louis / Technische Universität Darmstadt, 2016. URL: <https://econpapers.repec.org/RePEc%3Aadar%3Awpaper%3A81371>.
- [519] C. Barlag, **B. Büttner**, **C. Geminn** und N. Medzianowski. „Die Auseinandersetzungen um die Zukunft des europäischen Datenschutzes“. In: *Privacy Arena. Kontroversen um Privatheit im digitalen Zeitalter*. Hrsg. von J. Baumann und J. Lamla. Kassel University Press, 2017, S. 117–193. ISBN: 978-3-7376-0307-2.
- [520] **P. Gerber**. „Privatsphäre, gibt’s da nicht’ne App für?–Verbesserung von Privatsphäre-relevantem Verhalten durch bessere Informationen“. Diss. Dissertation, Darmstadt, Technische Universität Darmstadt, 2017, 2017.
- [521] **F. Pittroff**. „Amplituden der Demokratie: Der NSA-Untersuchungsausschuss des Deutschen Bundestages als demokratische Reaktion auf Verunsicherungen nach Snowden“. In: *Privacy Arena*. Hrsg. von J. Baumann und J. Lamla. Open Access. Kassel: Kassel University Press, 2017, S. 59–95. ISBN: 978-3-7376-0306-5.
- [522] **F. Pittroff**, **C. Ochs**, J. Lamla und **B. Büttner**. „Digitale Reterritorialisierung als politische Strategie. Die Reaktionsweisen der Demokratie in den Neuverhandlungen um Privatheit“. In: *Staat, Internet und digitale Gouvernamentalität*. Open Access. Springer Fachmedien Wiesbaden, Juli 2017, S. 141–165. ISBN: 978-3-658-18271-7. DOI: 10.1007/978-3-658-18271-7_7.
- [523] **N. Alexopoulos**, **S. M. Habib**, S. Schulz und M. Mühlhäuser. „M-STAR: A Modular, Evidence-Based Software Trustworthiness Framework“. In: *CoRR abs/1801.05764* (Jan. 2018). Open Access (arXiv). ISSN: 2331-8422. arXiv: 1801.05764. 
- [524] **B. Büttner**, **C. L. Geminn**, C. Husemann und N. Miedzianowski. *Die Arena der Datenschutz-Grundverordnung*. Bd. 6. Kassel University Press GmbH, 2018. ISBN: 978-3-7376-0564-9.
- [525] C. Husemann und **F. Pittroff**. „Smarte Regulierung in Informationskollektiven - Bausteine einer Informationsregulierung im Internet der Dinge“. In: *Die Fortentwicklung des Datenschutzes*. ISSN: 2512-7004. Springer Fachmedien Wiesbaden, 2018, S. 337–359. ISBN: 978-3-658-23727-1. DOI: 10.1007/978-3-658-23727-1_19.
- [526] M. Volkamer, A. Gutmann, K. Renaud, **P. Gerber** und P. Mayer. *Do People Shield Their PINs???* Open Access. 2018. URL: <https://pureportal.strath.ac.uk/en/publications/do-people-shield-their-pins>.
- [527] **N. Alexopoulos**, **E. Vasilomanolakis**, S. L. Roux, S. Rowe und M. Mühlhäuser. „TRIDeNT: Building Decentralized Incentives for Collaborative Security“. In: *CoRR abs/1905.03571* (Mai 2019). Open Access (arXiv). ISSN: 2331-8422. DOI: 10.48550/arxiv.1905.03571. arXiv: 1905.03571. 
- [528] **M. Fomichev**, **M. Maass**, **L. Almon**, A. Molina und M. Hollick. *Audio Data from Mobile Scenario from "Perils of Zero-Interaction Security in the Internet of Things"*. Zenodo Dataset. European Organization for Nuclear Research, Jan. 2019. URL: <https://doi.org/10.5281/zenodo.2537984>.
- [529] **M. Fomichev**, **M. Maass**, **L. Almon**, A. Molina und M. Hollick. *Index of Supplementary Files from "Perils of Zero-Interaction Security in the Internet of Things"*. Zenodo Dataset. Open Access. European Organization for Nuclear Research, Jan. 2019. URL: <https://doi.org/10.5281/zenodo.2537721>. 
- [530] T. Hanika, M. Kibanov, **J. Kropf** und S. Laser. „„Ich denke, es ist wichtig zu verstehen, warum die Netzwerkanalyse jetzt populär und besonders interessant für die Forschung geworden ist.““ In: *Digitale Bewertungspraktiken: Für eine Bewertungssoziologie des Digitalen*. Hrsg. von **J. Kropf** und S. Laser. Wiesbaden: Springer Fachmedien, 2019, S. 165–188. ISBN: 978-3-658-21165-3. DOI: 10.1007/978-3-658-21165-3_7.
- [531] **J. Kropf**. „Recommender Systems in der populären Musik“. In: *Digitale Bewertungspraktiken: Für eine Bewertungssoziologie des Digitalen*. Hrsg. von **J. Kropf** und S. Laser. Wiesbaden: Springer Fachmedien, 2019, S. 127–163. ISBN: 978-3-658-21165-3. DOI: 10.1007/978-3-658-21165-3_6.
- [532] **J. Kropf** und S. Laser. *Digitale Bewertungspraktiken: Für eine Bewertungssoziologie des Digitalen*. Hrsg. von **J. Kropf** und S. Laser. Wiesbaden: Springer Fachmedien, 2019. ISBN: 978-3-658-21164-6 978-3-658-21165-3. DOI: 10.1007/978-3-658-21165-3.

- [533] **J. Kropf** und S. Laser. „Eine Bewertungssoziologie des Digitalen“. In: *Digitale Bewertungspraktiken: Für eine Bewertungssoziologie des Digitalen*. Hrsg. von **J. Kropf** und S. Laser. Wiesbaden: Springer Fachmedien, 2019, S. 1–16. ISBN: 978-3-658-21165-3. DOI: 10.1007/978-3-658-21165-3_1.
- [534] **J. Kropf** und S. Laser. „Für eine reflexive Vergleichspraxis in der Bewertungssoziologie“. In: *Digitale Bewertungspraktiken: Für eine Bewertungssoziologie des Digitalen*. Hrsg. von **J. Kropf** und S. Laser. Wiesbaden: Springer Fachmedien, 2019, S. 19–40. ISBN: 978-3-658-21165-3. DOI: 10.1007/978-3-658-21165-3_2.
- [535] **C. Ochs**, M. Friedewald, T. Hess, T. Heß und J. Lamla. „Die Zukunft der Datenökonomie: Zwischen Geschäftsmodell, Kollektivgut und Verbraucherschutz“. In: *Medienkulturen im digitalen Zeitalter*. Hrsg. von **C. Ochs**, M. Friedewald, T. Hess und J. Lamla. Medienkulturen im digitalen Zeitalter. Open Access. Wiesbaden: Springer Fachmedien Wiesbaden, 2019. ISBN: 978-3-658-27510-5 978-3-658-27511-2. DOI: 10.1007/978-3-658-27511-2.
- [536] **S. Bretthauer**. „Datenschutz versus Katastrophenschutz“. In: *Verfassungsblog: On Matters Constitutional* (27. März 2020). Open Access. ISSN: 2366-7044. DOI: 10.17176/20200328-002931-0. 
- [537] **C. Geminn**. „Der Mensch in Recht und Technik – Eine Bestandsaufnahme“. In: *Mensch – Technik – Umwelt: Verantwortung für eine sozialverträgliche Zukunft – Festschrift für Alexander Roßnagel zum 70. Geburtstag*. Hrsg. von A. Hentschel, G. Hornung und **S. Jandt**. Baden-Baden: Nomos, Nov. 2020, S. 63–80.
- [538] **C. Geminn**. „Digitalisierung und verletzte Gruppen im Recht“. In: *Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft* Bd. 103.3 (2020), S. 254–288. ISSN: 2193-7869.
- [539] **C. Geminn**. „Grenzen des Verfassungswandels?“ In: *Verwaltungsarchiv* Bd. 111.4 (2020), S. 552–577.
- [540] **C. Geminn**. „Menschenwürde und menschenähnliche Maschinen und Systeme“. In: *Die Öffentliche Verwaltung* Bd. 73.5 (2020), S. 172–181.
- [541] **D. Müllmann** und **C. von Wintzingerode**. „Ein europäisches Netzwerk für Cybersicherheit“. In: *Den Wandel begleiten – IT-rechtliche Herausforderungen der Digitalisierung*. Hrsg. von J. Traeger. OIWR Verlag für Wirtschaft, 2020, S. 475–492. ISBN: 978-3-95599-069-5.
- [542] A. Roßnagel und **C. Geminn**. „Zwei Jahre Datenschutz-Grundverordnung – Eine Bilanz aus Verbrauchersicht“. In: *Vorgänge* 231/232 Bd. 59.3–4 (2020), S. 27–39.
- [543] G. Schwegler und **J. Kropf**. „Music and Conventions: Grasping Qualities of an Elusive and Changing Object“. Englisch. In: *Handbook of Economics and Sociology of Conventions*. Hrsg. von R. Diaz-Bone und G. de Larquier. Cham: Springer International Publishing, 2020, S. 1–24. ISBN: 978-3-030-52130-1. DOI: 10.1007/978-3-030-52130-1_96-1.
- [544] I. Spiecker gen. Döhmman und **S. Bretthauer**. „Schutzlos in Karlsruhe“. In: *Verfassungsblog: On Matters Constitutional* (5. Mai 2020). Open Access. ISSN: 2366-7044. DOI: 10.17176/20200505-133427-0. 
- [545] **M. Uhlmann**. *Netzgerechte Datenschutzgestaltung: Herausforderungen, Kriterien, Alternativen*. Nomos, 2020.
- [546] **S. Bretthauer**. „Datenschutzvollzug vor Zentralisierung“. In: *Verfassungsblog: On Matters Constitutional* (15. Dez. 2021). Open Access. ISSN: 2366-7044. DOI: 10.17176/20211215-142429-0. 
- [547] **S. Bretthauer**. „Hamburg schreitet ein“. In: *Verfassungsblog: On Matters Constitutional* (14. Mai 2021). Open Access. ISSN: 2366-7044. DOI: 10.17176/20210514-211000-0. 
- [548] **M. Fomichev**, L. F. Abanto-Leon, M. Stiegler, A. Molina, J. Link und M. Hollick. *Index of Supplementary Files from "Next2You: Robust Copresence Detection Based on Channel State Information"*. Zenodo Dataset. Open Access. European Organization for Nuclear Research, Juli 2021. URL: <https://doi.org/10.5281/zenodo.5105815>. 
- [549] **C. Geminn**. „Kommentierung von § 24 (Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken) HDSIG“. In: *Hessisches Datenschutz- und Informationsfreiheitsgesetz*. Hrsg. von A. Roßnagel. Handkommentar. Baden-Baden: Nomos, 2021, S. 271–283.
- [550] **C. Geminn**. „Kommentierung von § 28a (Datenverarbeitung bei öffentlichen Auszeichnungen und Ehrungen) HDSIG“. In: *Hessisches Datenschutz- und Informationsfreiheitsgesetz*. Hrsg. von A. Roßnagel. Handkommentar. Baden-Baden: Nomos, 2021, S. 320–328.
- [551] **C. Geminn**. „Kommentierung von § 28b (Datenverarbeitung in Gnadenverfahren) und §§ 80 bis 89 (Informationsfreiheit) HDSIG“. In: *Hessisches Datenschutz- und Informationsfreiheitsgesetz*. Hrsg. von A. Roßnagel. Handkommentar. Baden-Baden: Nomos, 2021, S. 731–797.

- [552] **C. Geminn.** „Kommentierung von Art. 24 (Videoüberwachung) BayDSG“. In: *Bayerisches Datenschutzgesetz*. Hrsg. von M. Schröder. Handkommentar. Baden-Baden: Nomos, 2021, S. 302–323.
- [553] **C. Geminn.** „Kommentierung von Art. 27 (Staatliche und kommunale Auszeichnungen und Ehrungen) BayDSG“. In: *Bayerisches Datenschutzgesetz*. Hrsg. von M. Schröder. Handkommentar. Baden-Baden: Nomos, 2021, S. 354–363.
- [554] **C. Geminn.** „Rechtsfragen eines offenen Web-Index – Freiheitsfördernde Infrastrukturen für die digitale Gesellschaft“. In: *MultiMedia und Recht* 1 (2021), S. 16–19.
- [555] **C. Geminn** und P. C. Johannes. „Die Beauftragung externer Gutachter durch die medizinischen Dienste – Spielräume und Zwänge des Wirtschaftlichkeitsgebots“. In: *Neue Zeitschrift für Sozialrecht* 21 (2021), S. 835–840.
- [556] **C. Geminn** und P. C. Johannes. „Kommentierung von § 45 (Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken, archivaren oder statistischen Zwecken) HDSIG“. In: *Hessisches Datenschutz- und Informationsfreiheitsgesetz*. Hrsg. von A. Roßnagel. Handkommentar. Baden-Baden: Nomos, 2021, S. 476–484.
- [557] **C. Geminn** und J. Müller. „Mobilität und Verkehr“. In: *IT-Sicherheitsrecht*. Hrsg. von G. Hornung und M. Schallbruch. Praxishandbuch 1. Aufl. Baden-Baden: Nomos, 2021, S. 520–553.
- [558] P. C. Johannes und **C. Geminn.** „Abwägung zur Sicherheit der Datenverarbeitung durch technische und organisatorische Maßnahmen – Zur Schwierigkeit der Bestimmung des ausreichenden datenschutzrechtlichen Schutzniveaus“. In: *InTeR – Zeitschrift für Innovations- und Technikrecht* 3 (2021), S. 140–146.
- [559] **J. Kropf.** „Changing Infrastructures of Musical Taste Formation?“ In: *Popular Music and the Poetics of Self in Fiction*. Hrsg. von N. Bachleitner und J. Werner. Leiden/Boston: Brill, Nov. 2021, S. 82–96. ISBN: 978-90-04-50069-3. DOI: 10.1163/9789004500686_006.
- [560] **J. Kropf.** „Schleichender Wandel mit ambivalenten Folgen: Rezension zu "Digitale Transformation" von Jan-Felix Schrape“. In: *Soziopolis: Gesellschaft beobachten* (2021). Open Access. URL: <https://nbn-resolving.org/urn:nbn:de:0168-ssaoar-78863-0>.
- [561] **J. Kropf.** „Zurück in die Zukunft der Künstlichen Intelligenz: Elemente einer digitalen Anthropologie am Beispiel Spotifys“. In: *Theologie und Digitalität*. Hrsg. von Beck, W., Nord, I. und J. Valentin. Freiburg: Herder, 2021, S. 50–72.
- [562] **C. Ochs.** „Kode als Kultur“. In: *Kuckuck. Notizen zur Alltagskultur* 1/21: *Code* (2021), S. 57–61.
- [563] **C. Ochs.** „Lost in Transformation? Einige Hypothesen zur Systematik der Strukturtransformation informationeller Privatheit vom 18. Jh. bis heute“. In: *Abschlussmagazin des DFG-Graduiertenkollegs 1681/2 "Privatheit & Digitalisierung"*. Open Access. Passau, Nov. 2021, S. 48–54. URL: https://www.privatheit.uni-passau.de/fileadmin/dokumente/dfg_graduiertenkolleg_privatheit/Graduiertenkolleg/Magazin/Magazin_16_Abschlussausgabe_Oktober_2021.pdf.
- [564] **C. Ochs** und **B. Büttner.** „Profilierungsdynamiken: Eine ethnographische Bestandsaufnahme der datafizierten Moderne“. In: *Autonomie und verantwortung in digitalen kulturen: Privatheit im geflecht von recht, medien und gesellschaft*. Hrsg. von F. X. Berger, A. Deremetz, M. Hennig und A. Michell. 1. Aufl. Bd. 4. Philosophische Praxis. Open Access. Baden-Baden: Academia/Nomos, 2021, S. 287–316. ISBN: 978-3-89665-937-8. DOI: 10.5771/9783896659378-287.
- [565] N. Scholten, **S. Bretthauer**, K. Eilermann, A. Hagemeyer, M. Hellmich, J. Hoffmann, D. Horenkamp-Sonntag, C. Jannes, L. Kuntz, P. Mantell, L. Mause, A. Müller, A. Reimer, C. Samel, I. Spiecker gen. Döhmman, S. Wobbe-Ribinski, C. Woopen und T. Dresbach. „The Effects of Webcams on German Neonatal Intensive Care Units – Study Protocol of a Randomised Crossover Trial (Neo-CamCare)“. Englisch. In: *BMC Health Services Research* 21.1 (12. Mai 2021). Open Access, S. 1–7. ISSN: 1472-6963. DOI: 10.1186/s12913-021-06387-3.
- [566] **N. Alexopoulos.** „New Approaches to Software Security Metrics and Measurements“. Open Access. Diss. Technical University of Darmstadt, Germany, 2022. URL: <http://tuprints.ulb.tu-darmstadt.de/21520/>.
- [567] C. Draude, C. Gruhl, G. Hornung, **J. Kropf**, J. Lamla, J. M. Leimeister, B. Sick und G. Stumme. „Social Machines“. In: *Informatik Spektrum* 45.1 (1. Feb. 2022). Open Access, S. 38–42. ISSN: 1432-122X. DOI: 10.1007/s00287-021-01421-4.

- [568] **C. Geminn.** „Zahlungsdaten im europäischen Datenwirtschaftsrecht“. In: *Recht der Zahlungsdienste* 3 (2022), S. 148–155.
- [569] **C. Geminn.** „Zur Institutionalisierung einer Überwachungsgesamtrechnung“. In: *Die Öffentliche Verwaltung* Bd. 75.19 (2022), S. 789–795.
- [570] **J. Kropf.** „Kontrollierte Verbindungen: Rezension zu ”Die Macht der Plattformen. Politik in Zeiten der Internetgiganten” von Michael Seemann“. In: *Soziopolis: Gesellschaft beobachten* (15. März 2022). Open Access. URL: <https://nbn-resolving.org/urn:nbn:de:0168-ss0ar-78976-4>. 
- [571] J. Lamla, **B. Büttner**, **C. Ochs**, **F. Pittroff** und **M. Uhlmann.** „Privatheit und Digitalität: Zur soziotechnischen Transformation des selbstbestimmten Lebens“. In: *Die Zukunft von Privatheit und Selbstbestimmung*. ISSN: 2512-7004, Open Access. Springer Fachmedien Wiesbaden, 2022, S. 125–158. ISBN: 978-3-658-35263-9. DOI: 10.1007/978-3-658-35263-9_4. 
- [572] **C. Ochs.** „Datenbasierte Sichtbarkeit: Gesellschaftsstrukturelle Bedingungen zeitgenössischer Technikgestaltung“. In: *Selbstbestimmung, Privatheit und Datenschutz: Gestaltungsoptionen für einen europäischen Weg*. Hrsg. von M. Friedewald, M. Kreutzer und M. Hansen. Open Access. Wiesbaden: Springer Fachmedien, 2022, S. 35–55. ISBN: 978-3-658-33306-5. DOI: 10.1007/978-3-658-33306-5_3. 
- [573] **C. Ochs.** *Soziologie der Privatheit: Informationelle Teilhabebeschränkung vom Reputation Management bis zum Recht auf Unberechenbarkeit*. Open Access. Weilerswist: Velbrück Wissenschaft, 2022. ISBN: 978-3-7489-1487-7. DOI: 10.5771/9783748914877. 
- [574] **C. Ochs.** „The Digital Public and its Problems: Komplexität, Verfahren und Trägerschaft als rekursive Konstitutionsprobleme einer digitalen Problemöffentlichkeit“. In: *Demokratie und Öffentlichkeit im 21. Jahrhundert – Zur Macht des Digitalen*. Hrsg. von I. Spiecker gen. Döhmman, M. Westland und R. Campos. Open Access. Baden-Baden: Nomos Verlagsgesellschaft, 2022, S. 57–74. ISBN: 978-3-7489-3274-1. DOI: 10.5771/9783748932741-57. 
- [575] **F. Pittroff.** „Verteilte Erreichbarkeit: Postdigitale Personalisierung durch Selfies als Gestaltungsaufgabe“. In: *Selbstbestimmung, Privatheit und Datenschutz*. Hrsg. von M. Friedewald, M. Kreutzer und M. Hansen. ISSN: 2512-7004, Open Access. Springer Fachmedien Wiesbaden, 2022, S. 79–97. ISBN: 978-3-658-33306-5. DOI: 10.1007/978-3-658-33306-5_5. 
- [576] A. Roßnagel, T. Bile, **C. L. Geminn** und **M. Nebel.** „Neue Konzepte für den Grundrechtsschutz in der digitalen Welt“. In: *Die Zukunft von Privatheit und Selbstbestimmung: Analysen und Empfehlungen zum Schutz der Grundrechte in der digitalen Welt*. Hrsg. von A. Roßnagel und M. Friedewald. Open Access. Wiesbaden: Springer Fachmedien Wiesbaden, 2022, S. 3–48. ISBN: 978-3-658-35263-9. DOI: 10.1007/978-3-658-35263-9_1. 
- [577] **M. Uhlmann**, **J. Kropf** und J. Lamla. *Datenintermediäre als Fairness-Akteure in der Datenökonomie*. Open Access. 1. Jan. 2022. URL: <https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-15-uhlmann-kropf-lamla-datenintermediaere-als-fairness-akteure-in-der-datenoekonomie.pdf>. 
- [578] **C. von Wintzingerode.** *Vorschlag der Europäischen Kommission für eine eIDAS-Verordnung 2.0 – Stolpersteine auf dem Weg zu einer EU-weiten digitalen Identität*. CR-online.de Blog. Open Access. 2. Feb. 2022. URL: <https://www.cr-online.de/blog/2022/02/02/vorschlag-der-europaeischen-kommission-fuer-eine-eidas-verordnung-2-0-stolpersteine-auf-dem-weg-zu-einer-eu-weiten-digitalen-identitaet/> (besucht am 07. 10. 2024). 
- [579] S. Engert, **J. Kropf** und **M. Uhlmann.** „Privacy-Trade-offs: Zur Rolle technischer und regulativer Datenschutzinitiativen im Ökosystem des digitalen Journalismus“. In: *Daten-Fairness in einer globalisierten Welt*. Hrsg. von M. Friedewald, A. Roßnagel, R. Neuburger, F. Bieker und G. Hornung. Open Access. Nomos Verlagsgesellschaft mbH & Co. KG, 2023, S. 145–170. ISBN: 978-3-7489-3874-3. DOI: 10.5771/9783748938743-145. 
- [580] **C. Geminn**, T. Tatsumi und M. Terada. „Digitalisierung der Verwaltung – Ein Blick auf Deutschland und Japan“. In: *Die Öffentliche Verwaltung* Bd. 76.20 (2023), S. 847–859.
- [581] P. C. Johannes und **C. L. Geminn.** „Anonymisierung von Patientendaten durch Fremdlabore für Dritte: Zur anonymisierenden Wirkung der Pseudonymisierung: datenschutzrechtliche Darstellung anhand eines Fallbeispiels“. In: *Medizinrecht* 41.5 (Mai 2023). Open Access, S. 368–372. ISSN: 0723-8886, 1433-8629. DOI: 10.1007/s00350-023-6458-0. 

- [582] **C. Ochs.** „Polarisierung durch Targeting? Anmerkungen zur datenbasierten Schließung sozialer Erfahrungsspielräume“. In: *Polarisierte Welten. Verhandlungen des 41. Kongresses der Deutschen Gesellschaft für Soziologie in Bielefeld 2022* 41 (29. Sep. 2023). Hrsg. von P.-I. Villa. Open Access. ISSN: 2367-4504. URL: https://publikationen.sozioLOGIE.de/index.php/kongressband_2022/article/view/1701 (besucht am 27. 09. 2024). 
- [583] I. Spiecker gen. Döhmman, **S. Bretthauer** und **D. Müllmann.** *Rechtliche Studie zum Cypher Social Contracts Konzept "Fides"*. Open Access. European Organization for Nuclear Research / Zenodo, 27. Jan. 2023. DOI: 10.5281/zenodo.7680213. 
- [584] M. Burkhardt, **J. Kropf**, **C. Ochs** und T. Seitz, Hrsg. *Frictions: Conflicts, Controversies and Design Alternatives in Digital Valuation*. Vol. 9, Issue 2/2023. Digital Culture & Society (DCS). Bielefeld: transcript Verlag, 2024.
- [585] C. Draude, D. Dürschnabel, J. Hirth, V. Horn, **J. Kropf**, J. Lamla, G. Stumme und **M. Uhlmann.** „Conceptual Mapping of Controversies“. Englisch. In: *Conceptual Knowledge Structures*. Hrsg. von I. P. Cabrera, S. Ferré und S. Obiedkov. Bd. 14914. Lecture Notes in Computer Science. Open Access (arXiv). Cham: Springer Nature Switzerland, Apr. 2024, S. 201–216. ISBN: 978-3-031-67868-4. DOI: 10.1007/978-3-031-67868-4_14. arXiv: 2404.18940. 
- [586] C. Draude, S. Engert, T. Hess, J. Hirth, V. Horn, **J. Kropf**, J. Lamla, G. Stumme, **M. Uhlmann** und N. Zwingmann. „Verrechnung - Design - Kultivierung: Instrumentenkasten für die Gestaltung fairer Geschäftsmodelle durch Ko-Valuation“. In: *Forschungsbericht Plattform Privatheit*. Hrsg. von M. Friedewald, A. Roßnagel, **C. Geminn** und M. Karaboga. Open Access. Fraunhofer ISI, 2024. DOI: 10.24406/publica-2497. 
- [587] **C. Geminn**, M. Terada und T. Tatsumi. „Die Verwaltung in der Pandemie – Bewältigungsstrategien in Japan und Deutschland“. In: *Die Öffentliche Verwaltung* Bd. 77.11 (2024), S. 464–473.
- [588] K. Hartwig, **T. Biselli**, F. Schneider und C. Reuter. „NEBULA: Nutzerzentrierte KI-basierte Erkennung von Fake News und Fehlinformationen“. In: *Aktuelle Themen und Herausforderungen behördlicher Risikokommunikation - Tagungsband*. München: Bundesamt für Strahlenschutz, 2024.
- [589] **J. Kropf.** „Werten und Bewerten“. In: *KZfSS Kölner Zeitschrift für Soziologie und Sozialpsychologie* 76.2 (1. Juni 2024). Open Access, S. 233–236. ISSN: 1861-891X. DOI: 10.1007/s11577-024-00959-x. 
- [590] **J. Kropf** und T. Frisch. „Valuation and Digital Platforms“. In: *The Routledge International Handbook of Valuation and Society*. Hrsg. von A. Krüger, T. Peetz und H. Schaefer. London: Routledge, Aug. 2024, S. 267–278. ISBN: 978-1-00-322935-3. DOI: 10.4324/9781003229353-32.
- [591] **C. Ochs.** „Privacy, the Private Sphere, and Digitization“. Englisch. In: *Handbuch Soziale Praktiken Und Digitale Alltagswelten*. Hrsg. von H. Friese, G. Rebane, M. Nolden und M. Schreiter. München: Springer, 2024. URL: <https://link.springer.com/book/9783658445201> (besucht am 27. 09. 2024).
- [592] **C. Ochs.** „The DataEconomy@Home: The Private Sphere, Privacy, and the Embedding of Artificial Intelligence Systems into Everyday Life as an Expansion of Economic Data Grabbing“. In: *Voice Assistants in Private Homes: Media, Data and Language in Interaction and Discourse*. Hrsg. von S. Habscheid, T. Hector, D. Hoffmann und D. Waldecker. Open Access. Bielefeld: transcript Verlag, 2024. URL: <https://www.transcript-verlag.de/978-3-8376-7200-8/voice-assistants-in-private-homes/?number=978-3-8394-7200-2>. 
- [593] C. Reuter, J. Franken, T. Reinhold, P. Kuehn, M.-A. Kaufhold, T. Riebe, K. Hartwig, **T. Biselli**, S. Schmid, L. Guntrum und S. Haesler. „Informatik für den Frieden: Perspektive von PEASEC zu 40 Jahren FlfF“. In: *FlfF-Kommunikation* (2024).
- [594] A. Roßnagel und **C. Geminn.** „The GDPR Five Years on – A Retrospective from the Viewpoint of Consumers“. In: *Revue européenne de droit de la consommation / European Journal of Consumer Law* 1 (2024), S. 109–129.
- [595] RUSTlab, K. Amelang, R. Asai, L. Çelik, R. Eggel, O. Galanova, S. Laser, M. Ojala, **F. Pittroff**, E. Sørensen und L. Werner. „Please Go Away... We're Reading“. en. In: *On_Culture* (Mai 2024), No 16 (2024): Ways of Reading. DOI: 10.22029/OC.2024.1415.

5.2. Projektergebnisse des Graduiertenkollegs

Die nachfolgenden 20 ausgewählten Projektergebnisse der gesamten Förderdauer des Graduiertenkollegs sind nicht sortiert, sondern erscheinen in der Reihenfolge, in der sie in Abschnitt 3.2 zitiert werden. Alle am Graduiertenkolleg beteiligten

(Post-)Doktorandinnen und (Post-)Doktoranden sind hervorgehoben. Open-Access-Publikationen sind mit einem Symbol  am Seitenrand markiert.

Publikationen mit wissenschaftlicher Qualitätssicherung

- [T1] **N. Büscher**, D. Demmler, S. Katzenbeisser, D. Kretzmer und T. Schneider. „HyCC: Compilation of Hybrid Protocols for Practical Secure Computation“. In: 25. *ACM Conference on Computer and Communications Security (CCS'18)*. Hrsg. von D. Lie, M. Mannan, M. Backes und X. Wang. Conference on Computer and Communications Security. Code: <https://gitlab.com/securityengineering/HyCC>, Open Access (ePrint). Toronto, Canada: ACM, 19. Okt. 2018, S. 847–861. DOI: 10.1145/3243734.3243786. eprint: <https://crypto.de/papers/BDKKS18.pdf>. 
- [T2] **A. Brüggemann**, O. Schick, T. Schneider, A. Suresh und H. Yalame. „Don't Eject the Impostor: Fast Three-Party Computation with a Known Cheater“. In: 45. *IEEE Symposium on Security and Privacy (IEEE S&P'24)*. Bd. abs/2112.13338. IEEE Symposium on Security and Privacy. Open Access. San Francisco, CA, USA: IEEE, 23. Mai 2024, S. 503–522. DOI: 10.1109/SP54263.2024.00164. eprint: <https://ia.cr/2023/1744>. 
- [T3] **A. Treiber**, **D. Müllmann**, T. Schneider und I. Spiecker gen. Döhmman. „Data Protection Law and Multi-Party Computation: Applications to Information Exchange between Law Enforcement Agencies“. In: 21. *Workshop on Privacy in the Electronic Society (WPES'22)*. Hrsg. von Y. Hong und L. Wang. Bd. 202. IACR Cryptology ePrint Archive. Open Access (ePrint). Los Angeles, CA, USA: ACM, 7. Nov. 2022, S. 69–82. DOI: 10.1145/3559613.3563192. eprint: <https://ia.cr/2022/1242>. 
- [T4] J. P. Gerlach, **N. Eling**, **N. Wessels** und P. Buxmann. „Flamingos on a Slackline: Companies' Challenges of Balancing the Competing Demands of Handling Customer Information and Privacy“. In: *Information Systems Journal* 29.2 (Aug. 2018), S. 548–575. ISSN: 1350-1917. DOI: 10.1111/isj.12222.
- [T5] **D. Müllmann**. „Brauchen wir ein Recht auf „digitalen Herdenschutz“? – Die Gefahren kommerziellen Profilings für die pluralistische Demokratie und gesellschaftliche Minderheiten“. In: *Der digitalisierte Staat - Chancen und Herausforderungen für den modernen Staat*. Hrsg. von R. Greve, B. Gwiasda, T. Kemper, J. Moir, S. Müller, A. Schönberger, S. Stöcker, J. Wagner und L. Wolff. Open Access. Nomos Verlagsgesellschaft mbH & Co. KG, 2020, S. 129–152. ISBN: 978-3-7489-0749-7. DOI: 10.5771/9783748907497-129. 
- [T6] **A. Wainakh**, F. Ventola, T. Müßig, J. Keim, C. G. Cordero, **E. Zimmer**, **T. Grube**, K. Kersting und M. Mühlhäuser. „User-Level Label Leakage from Gradients in Federated Learning“. Englisch. In: *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2022.2 (1. Apr. 2022). Open Access, S. 227–244. ISSN: 2299-0984. DOI: 10.2478/popets-2022-0043. 
- [T7] **H. Jöntgen**, N. V. Lingnau, O. Hinz und R. Holten. „This Is Why We Pay—Motivational Factors for Supporting Subscription-Based Crowdfunding Campaigns“. In: *Electronic Markets* 34.1 (Apr. 2024). Open Access, S. 1–21. ISSN: 1019-6781. DOI: 10.1007/s12525-024-00710-6. 
- [T8] **E. Steinbrink**, L. Reichert, M. Mende und C. Reuter. „Digital Privacy Perceptions of Asylum Seekers in Germany - An Empirical Study about Smartphone Usage during the Flight“. In: *Proceedings of the ACM: Human Computer Interaction (PACM): Computer-Supported Cooperative Work and Social Computing* 5 (CSCW2 Okt. 2021), S. 1–24. ISSN: 2573-0142. DOI: 10.1145/3479526.
- [T9] **N. Gerber**, **A. Stöver** und **K. Marky**. *Human Factors in Privacy Research*. Open Access. Springer Nature, 2023. ISBN: 978-3-031-28642-1. DOI: 10.1007/978-3-031-28643-8. 
- [T10] **M. Gazzari**, A. Mattmann, **M. Maass** und M. Hollick. „My(o) Armband Leaks Passwords: An EMG and IMU Based Keylogging Side-Channel Attack“. Englisch. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5.4 (27. Dez. 2021). Open Access (arXiv), S. 1–24. ISSN: 2474-9567. DOI: 10.1145/3494986. arXiv: 2112.02382. 
- [T11] **H. Lurtz** und G. Hornung. „Cyber-physische Systeme zwischen rechtlichen Anforderungen und rechtskonformer Gestaltung“. In: *Handbuch Industrie 4.0 und Digitale Transformation. Betriebswirtschaftliche, technische und rechtliche Herausforderungen* (2019). Hrsg. von R. Obermaier, S. 113–136. DOI: 10.1007/978-3-658-24576-4_5.
- [T12] **F. Hapsari**, R. I. Stemler und S. Pieschl. „Trust Resilience in Pedagogical Agents: Will Anthropomorphism Help Against Trust Decline?“ In: *Proceedings of the Annual Meeting of the Cognitive Science Society* 46.0 (2024). Open Access. URL: <https://escholarship.org/uc/item/3bz0w09k> (besucht am 10. 01. 2025). 

- [T13] **T. Schürmann** und P. Beckerle. „Personalizing Human-Agent Interaction through Cognitive Models“. In: *Frontiers in Psychology* 11 (Sep. 2020). Open Access, S. 561510. ISSN: 1664-1078. DOI: 10.3389/fpsyg.2020.561510. 
- [T14] **P. Gerber**, M. Volkamer und K. Renaud. „The Simpler, the Better? Presenting the COPING Android Permission-Granting Interface for Better Privacy-Related Decisions“. In: *Journal of Information Security and Applications* 34 (Juni 2017). Open Access (ePrint), S. 8–26. ISSN: 2214-2126. DOI: 10.1016/j.jisa.2016.10.003. eprint: <https://eprints.gla.ac.uk/137741/7/137741.pdf>. 
- [T15] **J. Brendel**, M. Fischlin, F. Günther und C. Janson. „PRF-ODH: Relations, Instantiations, and Impossibility Results“. en. In: *Advances in Cryptology – CRYPTO 2017*. Hrsg. von J. Katz und H. Shacham. Bd. 10403. Cham: Springer International Publishing, Aug. 2017, S. 651–681. ISBN: 978-3-319-63696-2 978-3-319-63697-9. DOI: 10.1007/978-3-319-63697-9_22.
- [T16] **K. Shrishak** und **H. Shulman**. „Privacy Preserving and Resilient RPKI“. In: *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*. IEEE Conference on Computer Communications. Open Access (arXiv). IEEE, Mai 2021, S. 1–10. DOI: 10.1109/INFOCOM42981.2021.9488759. arXiv: 2102.02456. 
- [T17] **A. Wainakh**, **T. Grube**, **J. Daubert** und M. Mühlhäuser. „Efficient Privacy-Preserving Recommendations Based on Social Graphs“. In: *Proceedings of the 13th ACM Conference on Recommender Systems, RecSys*. Hrsg. von T. Bogers, A. Said, P. Brusilovsky und D. Tikk. Bd. 1215. Copenhagen, Denmark: ACM, Sep. 2019, S. 78–86. DOI: 10.1145/3298689.3347013.
- [T18] **K. Marky**, **A. Stöver**, S. Prange, K. Bleck, **P. Gerber**, **V. Zimmermann**, F. Mueller, F. Alt und M. Mühlhäuser. „Decide Yourself or Delegate-User Preferences Regarding the Autonomy of Personal Privacy Assistants in Private IoT-equipped Environments“. In: *Proceedings of the CHI Conference on Human Factors in Computing Systems*. Hrsg. von F. ' Mueller, P. Kyburz, J. R. Williamson, C. Sas, M. L. Wilson, P. O. T. Dugas und I. Shklovski. Bd. 9. International Conference on Human Factors in Computing Systems. Open Access. ACM, Mai 2024, S. 1–20. ISBN: 9798400703300. DOI: 10.1145/3613904.3642591. 
- [T19] **M. Maass**, **A. Stöver**, H. Pridöhl, **S. Bretthauer**, D. Herrmann, M. Hollick und I. Spiecker gen. Döhmman. „Effective Notification Campaigns on the Web: A Matter of Trust, Framing, and Support“. In: *30th USENIX Security Symposium (USENIX Security 21)*. Hrsg. von M. Bailey und R. Greenstadt. USENIX Security Symposium. Open Access. USENIX Association, Aug. 2021, S. 2489–2506. ISBN: 978-1-939133-24-3. URL: <https://www.usenix.org/system/files/sec21-maass.pdf>. 
- [T20] N. Bindel, **J. Brendel**, M. Fischlin, B. Goncalves und D. Stebila. „Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange“. en. In: *Post-Quantum Cryptography*. Hrsg. von J. Ding und R. Steinwandt. Bd. 11505. Lecture Notes in Computer Science. Open Access (ePrint: longer version in iacr.org). Cham: Springer International Publishing, 2019, S. 206–226. ISBN: 978-3-030-25509-1 978-3-030-25510-7. DOI: 10.1007/978-3-030-25510-7_12. eprint: <https://eprint.iacr.org/2018/903.pdf>. 