TECHNISCHE UNIVERSITÄT DARMSTADT

Untersuchung des Beitrags von Webseitenbetreibenden zur Entstehung und Behebung von Privatsphärerisiken

Fachbereich Humanwissenschaften
der Technischen Universität Darmstadt

zur Erlangung des Grades
Doctor rerum naturalium
(Dr. rer. nat.)

Dissertation
von Alina Christina Stöver

Erstgutachter: Prof. Dr. Joachim Vogt
Zweitgutachterin: Prof. Dr. Karola Marky

Darmstadt 2023

Stöver, Alina: Untersuchung des Beitrags von Webseitenbetreibenden zur Entstehung und Behebung von Privatsphärerisiken
Darmstadt, Technische Universität Darmstadt,
Jahr der Veröffentlichung der Dissertation auf TUprints: 2023
Tag der mündlichen Prüfung: 27.03.2023

Erklärungen laut Promotionsordnung

Erklärung gemäß §9 der Allgemeinen Bestimmungen der Promotionsordnung der Technischen Universität Darmstadt.

Die Dissertation ist von mir mit einem Verzeichnis aller benutzten Quellen versehen. Ich erkläre, dass ich die Arbeit – abgesehen von den in ihr ausdrücklich genannten Hilfen – selbstständig verfasst habe. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen. Ich erkläre, dass die elektronische Version mit der schriftlichen Version übereinstimmt.

Darmstadt, den ……

……
Alina Stöver

Danksagung

An erster Stelle möchte ich meinem Doktorvater Herrn Prof. Dr. Joachim Vogt danken, der mich während der gesamten Promotionszeit unterstützt und mir große akademische Freiheit gewährt hat. Frau Prof. Dr. Karola Marky danke ich dafür, dass sie mir die Türen in die Welt der Usable Privacy Forschung geöffnet hat, mich immer gefördert hat und mich auf meinem Forschungsweg mit ihren Ideen und konstruktiven Feedback begleitet hat.

Ein besonderer Dank gilt allen Mitgliedern der fai. Besonders bedanken möchte ich bei Dr. Nina Gerber, Dr. Paul Gerber und Prof. Dr. Verena Zimmermann für die wunderbare Zusammenarbeit und den fachlichen Austausch. Dr. Nina Gerber und Angela Menig danke ich für ihre hilfreichen Kommentare zu dieser Arbeit. Annemarie Krebs-Nold und Angela Dressler danke ich von Herzen für die vielen kleinen Momente der Unterstützung. Ganz außerordentlichen möchte ich auch meinen wissenschaftlichen Hilfskräften Felix Kretschmer und Christin Cornel für ihre tatkräftige Unterstützung danken.

Ein weiterer besonderer Dank gilt den Mitgliedern des Graduiertenkollegs 2050 Privacy and Trust for Mobile Users für zahlreiche inspirierende Einblicke in andere Forschungsfelder, den spannenden Austausch und die Unterstützung auf allen Ebenen. Prof. Dr. Max Mühlhäuser danke ich für seine Unterstützung als Tandem-PI und seine zahlreichen Impulse im PAT-Seminar. Jana Vogel und Dr. Ephraim Zimmer danke ich für alles, was sie mit größtem persönlichem Engagement ermöglicht haben – ihr habt das GRK zu einem wunderbaren Ort zum Promovieren gemacht!
Mein großer Dank gilt meinen interdisziplinären Kollaborationspartnern Dr. Max Maass, Henning Pridöhl, Prof. Dr. Dominik, Prof. Dr. Matthias Hollick, Prof. Dr. Indra Spiecker gen. Döhmann sowie Dr. Sebastian Bretthauer. Danke für die vielen Gespräche und die interdisziplinäre Zusammenarbeit, in der ich unglaublich viel lernen durfte.

Großer Dank gilt auch Prof. Dr. Karola Marky und Prof. Dr. Mohamed Khamis, die mich im Rahmen eines (virtuellen) Forschungsaufenthalts an der University of Glasgow in ihre Forschungsgruppe aufgenommen und mir spannende Einblicke gegeben haben.

Danken möchte ich auch Prof. Dr. Verena Zimmermann und ihrem Team für die große Gastfreundschaft und den fachlichen Austausch während meines Forschungsaufenthalts an der ETH Zürich.

Ein weiterer Dank gebührt Dr. Vanessa Geuen und Dr. Ute Henning vom SchreibCenter der TU Darmstadt, deren Schreibchoachings sehr dazu beigetragen haben, die Ausrichtung dieser Arbeit zu schärfen.

Danke an meine Freund:innen, die mich während dieser Zeit begleitet und bestärkt haben.

Größter Dank gilt meiner Familie, die das ganze Projekt mitgetragen hat und immer für mich da war – ohne euch wäre diese Arbeit niemals möglich gewesen!

Zusammenfassung

Privatsphärerisiken auf Webseiten sind weitverbreitet und führen zu Einschränkungen der Privatsphäre von Nutzenden. Die bisherige Forschung hat sich überwiegend mit der Perspektive der Nutzenden beschäftigt und Lösungen entwickelt, um diese zu unterstützen. Hinter jeder Webseite stehen jedoch Webseitenbetreibende, die mit ihren Entscheidungen potenziell Einfluss auf das Entstehen bzw. Bestehen von Privatsphärerisiken nehmen können. In der vorliegenden Arbeit wird die Perspektive von Webseitenbetreibenden untersucht, um besser zu verstehen, wie diese zur Entstehung und zum Bestehen von Privatsphärerisiken auf Webseiten beitragen.

Der erste Teil der Arbeit ist der Herausforderung von Webseitenbetreibenden gewidmet, bestehende Privatsphärerisiken auf ihrer Webseite zu beheben. Diese Herausforderung wird beispielhaft an der Behebung einer bestehenden Fehlkonfiguration (fehlende IP-Anonymisierung) eines auf der Webseite eingebundenen Analysetools (Google Analytics) durch die Webseitenbetreibenden untersucht. Dazu wurde eine mehrteilige Studie durchgeführt. Zunächst wurden 4594 Webseitenbetreibende im Rahmen eines Feldexperiments mit Briefen und E-Mails über die fehlende IP-Anonymisierung auf ihrer Webseite benachrichtigt. Um die Hintergründe besser zu verstehen, wurden 477 Webseitenbetreibende im Anschluss mittels Fragebogen befragt. Insgesamt 1043 Rückmeldungen von Webseitenbetreibenden auf die vorausgegangenen Benachrichtigungen dienten als Datengrundlage für eine quantitative sowie eine qualitative Analyse. Die Ergebnisse zeigen, dass zu den Ursachen für bestehende Privatsphärerisiken auf Webseiten neben fehlendem Bewusstsein der Webseitenbetreibenden auch unklare Zuständigkeiten, fehlerhafte technische Umsetzung und mangelnde Wartung der Webseite zählen. Webseitenbetreibende unterscheiden sich von anderen Personengruppen, die Systeme entwickeln und betreiben (z. B. Entwickler:innen), u. a. dahingehend, dass sie teilweise nur über geringes technisches Wissen verfügen. Webseitenbetreibende haben verschiedene Hintergründe und Rahmenbedingungen. Sie reichen von Privatpersonen, die mit der Webseite einer Freizeitbeschäftigung nachgehen, über Selbständige, die ihre Produkte vertreiben wollen, bis zu Vollzeitangestellten, die ein großes Unternehmen repräsentieren. Entsprechend ihrer Rahmenbedingungen variieren die Hürden, die Webseitenbetreibende beim Beheben von Privatsphärerisiken überwinden müssen. Diese Hürden reichen von fehlendem technischen Wissen bis zu zähen Organisationsprozessen. Es besteht ein großer Unterstützungsbedarf bei der Behebung von Privatsphärerisiken. Maßnahmen müssen auf die unterschiedlichen Bedürfnisse und Rahmenbedingungen verschiedener Webseitenbetreibenden angepasst sein, um effektiv zu sein. Durch die Arbeit wird aufgezeigt, wie eine Unterstützungsmaßnahme in Form einer Benachrichtigung gestaltet sein sollte, die bei Webseitenbetreibenden sowohl Bewusstsein schafft als auch beim Beheben von Privatsphärerisiken unterstützt. Der erste Teil der Arbeit impliziert, dass es sinnvoll sein kann, Webseitenbetreibende nicht nur bei der Behebung von Privatsphärerisiken zu unterstützen, sondern auch bei der Entstehung von Privatsphärerisiken anzusetzen, um diese zu vermeiden.

Der zweite Teil der Arbeit befasst sich mit der Herausforderung der Vermeidung von Privatsphärerisiken aus Sicht der Webseitenbetreibenden, die am Beispiel der Erstellung von Cookie-Einwilligungsklärungen untersucht wird. Dazu wurde in zwei aufeinanderfolgenden Studien u. a. sowohl die Präferenz von 376 Nutzenden als auch die von 195 Webseitenbetreibenden hinsichtlich verschiedener Gestaltungsvarianten von Cookie-Einwilligungserklärungen untersucht. Die Ergebnisse zeigen, dass Nutzende

Gestaltungsvarianten von Cookie-Einwilligungserklärungen präferieren, die privatsphärefreundliche Entscheidungen fördern und keine Design-Elemente enthalten, die sie zur Zustimmung verleiten (sog. *Deceptive Designs*; dt. irreführende Gestaltung). Webseitenbetreibende schätzen die Nutzendenpräferenz größtenteils korrekt ein, orientieren sich bei der Auswahl einer Gestaltungsvariante jedoch nur zum Teil daran. Webseitenbetreibende, die mit den durch Cookies gespeicherten Daten Einnahmen generieren, wählen häufiger eine Gestaltungsvariante, die *Deceptive Designs* enthält und die Privatsphäre der Nutzenden einschränkt. Dabei scheint die Popularität der Webseite eine untergeordnete Rolle zu spielen. Ein Großteil der Webseitenbetreibenden in der untersuchten Stichprobe präferiert jedoch privatsphärefreundliche Gestaltungvarianten.

Immer häufiger greifen Webseitenbetreibende bei der Erstellung von Einwilligungserklärungen auf die Vorlagen von Consent Management Platforms (CMPs) zurück. Um zu untersuchen, inwiefern sie mit diesen Vorlagen Einwilligungserklärungen ohne *Deceptive Designs* generieren und damit Privatsphärerisiken vermeiden können, wurden im Rahmen einer weiteren Studie die Vorlagen von 15 populären CMPs analysiert. Die Ergebnisse zeigen, dass es für Webseitenbetreibende nur eingeschränkt möglich ist, mit den Vorlagen der CMPs Einwilligungserklärungen ohne *Deceptive Designs* zu erstellen. Die Vorlagen der CMPs erschweren es also Webseitenbetreibenden, Privatpshärerisiken zu vermeiden, und sind ein möglicher Erklärungsansatz für die weite Verbreitung von *Deceptive Designs* in Cookie-Einwilligungserklärungen.

Die Erkenntnisse der vorliegenden Arbeit helfen dabei, die Gruppe der Webseitenbetreibenden mit ihren Herausforderungen beim Beheben bzw. Vermeiden von Privatsphärerisiken besser zu verstehen. Dieses Verständnis kann als Grundlage für die Entwicklung gezielter und wirkungsvoller Maßnahmen zur Unterstützung von Webseitenbetreibenden dienen. Webseitenbetreibende dabei zu unterstützen, die Privatsphäre der Nutzenden besser zu schützen, entlastet zugleich die Nutzenden. Damit soll die Arbeit auch einen Beitrag zur Verbesserung der Privatsphäre von Nutzenden leisten.

Abstract

Privacy risks on websites are widespread and affect the privacy of users. Previous research has mainly focused on the perspective of users and developed solutions to support them. However, behind every website is a website operator whose decisions can potentially influence the emergence or existence of privacy risks. This dissertation focuses on the perspective of website operators and helps to better understand how they contribute to the emergence and existence of privacy risks on websites.

The first part of the dissertation is dedicated to the challenge of website operators in addressing existing privacy risks on their websites. This challenge is investigated using the example of website operators' remediation of an existing misconfiguration (lack of IP anonymization) of an analytics tool (Google Analytics) embedded on the website. For this purpose, a multi-part study was conducted. First, 4,594 website operators were notified by letter and email about the missing IP anonymization on their website as part of a field experiment. To better understand the background, 477 website operators were subsequently surveyed via questionnaire. A total of 1,043 responses from website operators to the previous notifications served as the data basis for a quantitative and a qualitative analysis. The results show that the reasons for existing privacy risks on websites include a lack of awareness on the part of website operators, unclear responsibilities, faulty technical implementation, and a lack of website maintenance. Website operators differ from other groups of people who develop and operate systems (e.g., developers) insofar as they sometimes have only limited technical knowledge. Website operators have different backgrounds and circumstances. These range from private individuals who pursue a leisure activity with their website, to self-employed individuals who want to sell their products, to full-time employees who represent a large company. According to their backgrounds, the hurdles website operators face in addressing privacy risks vary. These hurdles range from a lack of technical knowledge to tough organizational processes. There is a great need for support in remediating privacy risks. Measures need to be adapted to the different needs and frameworks of different website operators to be effective. This work shows how a support measure in the form of a notification should be designed to both raise awareness and assist website operators in remediating privacy risks. The first part of the thesis implies that it may be useful to support website operators not only in remedying privacy risks but also in preventing privacy risks from arising in the first place.

The second part of the dissertation focuses on the challenge of avoiding privacy risks from the perspective of website operators, which was investigated using the example of the creation of cookie consent notices. In two subsequent studies, the preferences of 376 users as well as those of 195 website operators were investigated with regard to different design variants of cookie consent notices. The results show that users prefer cookie consent notices that promote privacy-friendly choices and do not contain design elements that would induce them to consent (so-called *Deceptive Designs*). Most website operators correctly assess user preferences but only partially follow them when selecting a design variant. Website operators who generate revenue with the data stored by cookies are more likely to choose a design variant that contains *Deceptive Designs* and thus restricts the privacy of users. The popularity of the website seems to play a subordinate role. However, a large proportion of the website operators studied in the sample prefer privacy-friendly design variants.

Website operators are making increasing use of the templates of consent management platforms (CMPs) when creating consent notices. To investigate the extent to which they can use these templates to generate consent notices without deceptive designs and thus avoid privacy risks, a further study analyzed the templates of 15 popular CMPs. The results show that it is only possible to a limited extent for website operators to generate consent notices without *deceptive designs* using the templates of the CMPs. Thus, the CMPs' templates make it difficult for website operators to avoid privacy risks and are a possible explanation for the widespread use of deceptive designs in cookie consent notices.

The findings of this dissertation help to better understand website operators and their challenges in remediating or avoiding privacy risks. This understanding can serve as the basis for developing purposeful and effective interventions to support website operators. Supporting website operators in better protecting the privacy of users also relieves the burden placed on users. Ultimately, this work also aims to contribute to improving the privacy of users.

Inhaltsverzeichnis

1 Einleitung

1.1 Relevanz und Motivation der Arbeit

Im August 1991 veröffentlichte der britische Forscher Tim Berners-Lee die erste Webseite überhaupt. Berners-Lees ursprüngliche Idee war es, mithilfe von Webseiten einen automatisierten Informationsaustausch zwischen Forschenden an Universitäten und Instituten in aller Welt zu ermöglichen (CERN, 2023). Rund 30 Jahre später existieren schätzungsweise 1.88 Mrd. Webseiten weltweit (Armstrong, 2021). Für viele Menschen sind Webseiten nicht mehr aus ihrem Alltag wegzudenken. Sie nutzen diese, um Online-Einkäufe zu tätigen, Nachrichten oder Unterhaltung zu konsumieren und sich mit anderen zu vernetzen. Damit bieten Webseiten den Nutzenden zahlreiche Vorteile und Möglichkeiten.

Öffentliche Webseiten werden aus dem Internet geladen, das wiederum auf dem Datenaustausch zwischen Computern über Telekommunikationsnetze basiert – ohne Datenaustausch an sich gäbe es also kein Internet (Metzger et al., 2018). Das bedeutet auch, dass prinzipiell Daten der Nutzenden gesammelt, gespeichert, verarbeitet und weitergegeben werden können, womit Risiken für deren Privatsphäre[1] einhergehen.

Ein besonderes Risiko für die Privatsphäre stellt das sogenannte Tracking[2] (dt. Nutzendenverfolgung) dar. Untersuchungen zufolge enthalten 90 % der Webseiten mindestens ein Tracking-Skript (Englehardt & Narayanan, 2016). Damit können nicht nur die Webseitenbetreibenden das Verhalten der Nutzenden analysieren, sondern auch Anbieter von Trackern (Third-Party-Provider) können Nutzende mithilfe verschiedener Technologien wie Cookies über Webseiten hinweg verfolgen (Third-Party-Tracking) und so deren Standorte, Gewohnheiten und Interessen erfassen. Google, Facebook und Amazon zählen aktuell zu den Anbietern, deren Tracker die größte Reichweite haben (Binns, Lyngs, et al., 2018; Karaj et al., 2019). Durch Analysen wird belegt, dass große Tracker im Durchschnitt etwa die Hälfte des Browserverlaufs fast aller Nutzenden kennen (Dambra et al., 2022). Das Wissen, das diese Unternehmen auf diese Weise sammeln, ermöglicht es ihnen, aussagekräftige Profile zu erstellen, die immer weiter verfeinert werden und für viele kaufwillige Akteure verfügbar sind. Infolgedessen riskieren die Nutzenden, die Kontrolle über ihre privaten Daten zu verlieren, und müssen mit potenziell schwerwiegenden Konsequenzen rechnen. Zum Beispiel kann Tracking genutzt werden, um Produktpreise entsprechend dem geografischen Standort und der finanziellen Situation der Nutzenden anzupassen (Shiller, 2020).

Viele Webseiten enthalten eine Reihe spezifischer Privatsphärerisiken für Nutzende, die dazu beitragen können, das Trackingausmaß zu erhöhen (Utz et al., 2022). Zum Beispiel sind eingebundene Analysetools häufig so konfiguriert, dass sie mehr Daten der Nutzenden sammeln als nötig und als rechtlich zulässig (Maass et al., 2021). Ein weiteres Beispiel ist die Gestaltung von Einwilligungserklärungen, bei denen Nutzende dazu verleitet werden, dem Tracking eher zuzustimmen (Utz et al., 2019).

[1] Unter Privatsphäre wird in dieser Arbeit „der Anspruch der Einzelnen [...], selbst zu bestimmen, wann, wie und in welchem Umfang Informationen über sie oder ihn an andere weitergegeben werden verstanden.“ (Westin, 1968, S. 7). Eine ausführlichere Definitionsbeschreibung befindet sich in Kapitel 2.3.

[2] Webseite-Tracking bezeichnet die Methode der Erfassung, Speicherung und Analyse der Browseraktivitäten von Nutzenden (Ghostery, Inc., 2022).

Hinter jeder Webseite stehen Betreibende, die verantwortlich sind und prinzipiell über das Ausmaß eingesetzter Tracker mitentscheiden können. Damit haben sie einen großen Einfluss auf die Privatsphäre der Nutzenden. Häufig greifen Webseitenbetreibende auf die Dienste von Drittanbietern zurück, um Funktionalitäten auf ihren Webseiten zu ermöglichen. Diese Funktionalitäten sind vielfältig und reichen von der Einbindung von Werbenetzwerken (z. B. Google Ads[3]) mit dem Ziel der Monetarisierung der Webseite durch Werbeeinnahmen bis zur optischen Aufwertung beispielsweise durch die Einbindung von Schriften (z. B. Google Fonts[4]). Die Einbettung dieser externen Ressourcen erlaubt es häufig nicht nur den Webseitenbetreibenden, sondern auch den Drittanbietern, die Nutzenden der Webseite zu tracken (Libert & Nielsen, 2018). Zum Beispiel bietet Google mit Google Fonts Schriften an, die webkompatibel und optisch ansprechend sind. Standardmäßig können Webseitenbetreibende diese Schriftarten so einbinden, dass sie beim Aufrufen der Webseite über einen Google-Server nachgeladen werden. Dabei werden jedoch automatisch Daten der Nutzenden (in dem Fall ihre IP-Adresse) an den Google-Server übertragen (Lenz et al., 2022).

Gleichzeitig haben Webseitenbetreibende mehrere Möglichkeiten, Tracking einzudämmen, und sind teilweise sogar rechtlich dazu verpflichtet. Zum einen können sie die auf ihrer Webseite eingebundenen Dienste häufig so konfigurieren, dass sie weniger Daten der Nutzenden sammeln. Zum anderen sind sie verpflichtet, den Nutzenden die freiwillige und informierte Entscheidung zu überlassen, ob sie dem Tracking zustimmen. Das wird von den Webseitenbetreibenden meist in Form von sogenannten Cookie-Einwilligungserklärungen (umgangssprachlich: Cookie-Banner) umgesetzt.

Besuchen Nutzende also eine Webseite, müssen sie sich zum einen darauf verlassen, dass die Webseitenbetreibenden eingebundene Dienste so konfiguriert haben, dass ihre Privatsphäre geschützt ist. Zum anderen sind sie darauf angewiesen, dass die Webseitenbetreibenden ihnen die Möglichkeit einer transparenten, freiwilligen und informierten Entscheidung für oder gegen Tracking geben. Die bisherige Forschung bietet eine Reihe an Lösungen für Nutzende, um ihre Privatsphäre zu schützen. Damit wird ihnen jedoch zugleich eine große Last übertragen und sie fühlen sich häufig machtlos und überfordert, wenn sie versuchen, die Kontrolle über ihre Daten zu behalten (Pew Research Center, 2019). Zur Eindämmung von Privatsphärerisiken sind auch die entsprechenden rechtlichen Rahmenbedingungen relevant. Diese können jedoch nur wirksam werden, wenn die Anforderungen von den Webseitenbetreibenden auch umgesetzt werden, die somit eine große Verantwortung bezüglich des Schutzes der Privatsphäre tragen.

1.2 Problemstellung und Ziele der Arbeit

Aus der bisherigen Forschung geht hervor, dass Webseitenbetreibende nicht immer ihrer Verantwortung nachkommen, die Privatsphäre der Nutzenden bestmöglich zu schützen. So sind sowohl Fehlkonfigurationen als auch Einwilligungserklärungen verbreitet, die so gestaltet sind, dass sie die Privatsphäre der Nutzenden gefährden. Diese Risiken zu beheben bzw. erst gar nicht entstehen zu lassen, liegt in der Verantwortung der Webseitenbetreibenden. Gleichzeitig deutet die weite Verbreitung von Privatsphärerisiken darauf hin, dass der Schutz der Privatsphäre der Nutzenden auch für Webseitenbetreibende mit Herausforderungen einhergeht. Herausforderungen können darin bestehen,

[3] Google Ads stellt ein Onlinewerbeprogramm von Google dar (Google, 2023).
[4] Google Fonts ist ein Verzeichnis mit Schriftarten von Google (Google, o. J.).

Privatsphärerisiken auf ihren Webseiten zu beheben oder die Entstehung von neuen Privatsphärerisiken zu vermeiden. Das **übergeordnete Ziel** dieser Arbeit ist es, diese Herausforderungen aus der Perspektive von Webseitenbetreibenden zu beleuchten, um so besser zu verstehen, wie diese zur Entstehung und zum Bestehen von Privatsphärerisiken auf Webseiten beitragen. Dazu wurden die Herausforderungen an je einem beispielhaften Privatsphärerisiko analysiert. In Abbildung 1 wird ein Überblick über die Herausforderungen gegeben, die in dieser Arbeit betrachtet werden, und die damit verbundenen Ziele sowie die dazugehörigen Studien und Forschungsfragen werden genannt. In den folgenden Unterkapiteln werden die Herausforderungen beschrieben sowie die jeweiligen Forschungsziele aufgezeigt. Die zu den Studien gehörenden Forschungsfragen werden in den späteren Kapiteln hergeleitet.

Abbildung 1. Überblick über die in dieser Arbeit behandelten Herausforderungen, die daraus abgeleiteten Ziele sowie die durchgeführten Studien mit den entsprechenden Forschungsfragen.

1.2.1 Herausforderung 1: Behebung bestehender Privatsphärerisiken

Analysetools gehören zu den häufigsten Drittanbieterdiensten, die Webseitenbetreibende auf ihren Webseiten einbinden. Sie ermöglichen es beispielsweise, das Verhalten der Nutzenden oder die Webseitenleistung zu messen (Utz et al., 2022). Das Tool mit der größten Reichweite ist Google Analytics (Karaj et al., 2019). Analysetools können die Privatsphäre der Nutzenden gefährden, indem sie umfangreiche Daten sammeln, die sie zudem häufig mit anderen (z. B. Werbenetzwerken) teilen (Dambra et al., 2022). Webseitenbetreibende haben jedoch die Möglichkeit, diese Tools so zu konfigurieren, dass sie weniger Daten sammeln. Teilweise sind sie sogar dazu verpflichtet, Konfigurationen anzupassen, damit ihre Webseite datenschutzrechtliche Anforderungen erfüllt. Zur Vermeidung, dass Google die IP-Adresse der Nutzenden zusammen mit den Analysedaten speichert,

mussten Webseitenbetreibende beispielsweise in der Vergangenheit die IP-Anonymisierung von Google Analytics aktivieren. Diese Konfiguration war laut eines Urteils des Landesgerichts Dresden notwendig, um mit den Anforderungen der Datenschutz-Grundverordnung (DSGVO) konform zu sein (Landgericht Dresden, 2019). Die Aktivierung der IP-Anonymisierung kann in den meisten Fällen durch eine einfache Anpassung einer JavaScript-Zeile im Code der Webseite vorgenommen werden (Maass et al., 2021). Eine Nichtumsetzung kann potenziell empfindliche Strafen für die Webseitenbetreibenden zur Folge haben. Es können Geldbußen von bis zu 20 Mio. € oder im Fall eines Unternehmens von bis zu 4 % des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden, je nachdem, welcher Betrag höher ist (Art. 83 Abs. 5 DSGVO). Eine Analyse von 1.3 Mio. deutschen Webseiten von Maass et al. (2021) ergab jedoch, dass bei 12.7 % der gescannten Webseiten die IP-Anonymisierung von Google Analytics nicht oder inkorrekt umgesetzt ist. Damit Datenschutzgesetze effektiv werden und die Privatsphäre der Nutzenden gewährleistet werden kann, müssen die geforderten Maßnahmen auch umgesetzt werden. Obwohl nur kleine Änderungen im Code vorgenommen werden müssen, schaffen es Webseitenbetreibende nicht, das Privatsphärerisiko zu beheben. Deshalb soll zunächst ein Verständnis für diese Herausforderung entwickelt werden. Dies soll dabei helfen, zu begreifen, was die Ursachen für die bestehenden Privatsphärerisiken sind, wie Webseitenbetreibende diese beheben können und welche Hürden sie dabei überwinden müssen. Das erste Ziel dieser Arbeit lautet demnach wie folgt:

Ziel 1: Entwicklung eines besseren Verständnisses für die Herausforderung für Webseitenbetreibende, bestehende Privatsphärerisiken auf ihren Webseiten zu beheben. Untersucht am Beispiel der Behebung einer Fehlkonfiguration von Google Analytics.

Die weite Verbreitung von Privatsphärerisiken deutet darauf hin, dass Webseitenbetreibende Unterstützung bei der Behebung benötigen. In anderen Kontexten wurde in der Forschung bereits gezeigt, dass es nützlich sein kann, zunächst ein Bewusstsein für das bestehende Problem zu schaffen (z.B. Durumeric et al., 2014). Dazu wurden in der Vergangenheit bereits Benachrichtigungen an Verantwortliche versandt, in denen auf solche Probleme hingewiesen wurde (Canali et al., 2013; Çetin et al., 2017; Durumeric et al., 2014; Stock et al., 2016, 2018; Vasek & Moore, 2012; Zeng, Li, & Stark, 2019).
Mit Ziel 2 soll eine entsprechende Maßnahme auch für Privatsphärerisiken auf Webseiten untersucht werden:

Ziel 2: Erarbeitung von Maßnahmen, wie Webseitenbetreibende bei der Behebung von Privatsphärerisiken auf ihren Webseiten unterstützt werden können. Untersucht am Beispiel von Benachrichtigungen zum Hinweis auf die Fehlkonfiguration von Google Analytics.

Das Beispiel der Behebung einer Fehlkonfiguration (der fehlenden IP-Anonymisierung) von Google Analytics, das zur Beleuchtung der Herausforderung 1 gewählt wurde, zeichnet sich durch eine Reihe an Merkmalen aus: Es stellt ein Privatsphärerisiko dar, (1) das aus rechtlicher Sicht ein Handeln der Webseitenbetreibenden erforderlich macht, (2) das bereits auf vielen Webseiten besteht und (3) das für Nutzende beim Besuch nicht direkt erkennbar ist. Für die Betrachtung der Herausforderung 2 – das

Vermeiden der Entstehung von Privatsphärerisiken – wurde ein weiteres Risiko als Beispiel ausgewählt. Dabei geht es um Cookie-Einwilligungserklärungen, die Gestaltungselemente enthalten, die Nutzende dazu verleiten, ihre Zustimmung zu erteilen – sogenannte *Deceptive Designs* (dt. irreführende Gestaltung). Dieses Privatsphärerisiko unterscheidet sich vom vorherigen Beispiel (fehlende IP-Anonymisierung von Google Analytics) dahingehend, dass (1) aus rechtlicher Perspektive nicht immer ein eindeutiges Handeln der Webseitenbetreibenden erforderlich ist, (2) das Risiko auch auf neu erstellten Webseiten oder beim Einbinden neuer Dienste entstehen kann und (3) es für die Nutzenden beim Besuch der Webseite erkennbar ist sowie deren *User Experience* (dt. Nutzungserleben) beeinflussen kann.

1.2.2 Herausforderung 2: Vermeidung der Entstehung von Privatsphärerisiken

Webseitenbetreibende sind gesetzlich dazu verpflichtet, eine Einwilligung der Nutzenden einzuholen, wenn sie (1) personenbezogene Daten verarbeiten oder (2) Cookies setzen (HmbBfDI, 2021). Dazu greifen sie in der Regel auf sogenannte Cookie-Einwilligungserklärungen zurück. Während das Ziel darin besteht, die Nutzenden in die Lage zu versetzen, eine informierte Entscheidung über die gemeinsame Nutzung von Daten zu treffen, sind Cookie-Einwilligungserklärungen in Wirklichkeit oft so gestaltet, dass sie die Nutzenden dazu ermutigen, ihre Einwilligung zu geben, wie in Abbildung 2 durch Hervorhebung des Zustimmungs-Buttons. In früheren Forschungen wurde gezeigt, dass solche *Deceptive Designs* zu einer erhöhten Zustimmung führen, was die Privatsphäre beeinträchtigen kann. *Deceptive Designs* in Cookie-Einwilligungserklärungen sind weit verbreitet (Kampanos & Shahandashti, 2021; Krisam et al., 2021; Soe et al., 2020). Analysen ergaben, dass bei 85 % der top 500 deutschen Webseiten, die eine Cookie-Einwilligungserklärung enthalten, die Nutzenden durch visuelle Hervorhebung dazu verleitet werden, Cookies zu akzeptieren (Krisam et al., 2021). Diese Art der Gestaltung spiegelt häufig nicht das Interesse der Nutzenden wider (Singh et al., 2022).

Abbildung 2. Aktuelle Cookie-Einwilligungserklärung der offiziellen Seite des Nationalen Cyber-Sicherheitsrats – Stand 12.01.2023 (Bundesministerium der Verteidigung, 2023).

Auf den ersten Blick kann es für Webseitenbetreibende vorteilhaft sein, die Nutzenden durch die Verwendung eines *Deceptive Designs* dazu zu bewegen, alle Cookies zu akzeptieren, da die Sammlung von Statistiken und Werbedaten unter Umständen Teil des Geschäftsmodells ist. Andererseits könnte es jedoch auch von Interesse sein, Vertrauen aufzubauen und positives Feedback auf der Webseite zu erhalten, indem die Verwendung von Cookies transparent dargestellt und eine informierte Entscheidung ermöglicht wird. Folglich liegt es an den Webseitenbetreibenden, das Privatsphärerisiko für Nutzende, das durch solche *Deceptive Designs* in Cookie-Einwilligungserklärungen entsteht, durch bewusste Gestaltung zu vermeiden. Bisher ist jedoch noch ungeklärt, welche Aspekte Webseitenbetreibende bei der Gestaltung bzw. Erstellung von Cookie-Einwilligungserklärungen berücksichtigen und inwiefern es

in ihrem Interesse ist, an dieser Stelle Privatsphärerisiken für Nutzende zu vermeiden. Daraus ergibt sich das nächste Ziel:

Ziel 3: Entwicklung eines besseren Verständnisses für die Herausforderung für Webseitenbetreibende, die Entstehung von Privatsphärerisiken auf ihren Webseiten zu vermeiden. Untersucht am Beispiel der Gestaltung von Cookie-Einwilligungserklärungen.

Auch bei dieser Herausforderung stellt sich die Frage, wie Webseitenbetreibende dabei unterstützt werden können. Anhand der bisherigen Forschung konnte bereits gezeigt werden, dass Entwickler:innen von Apps durch die Bereitstellung von Informationen über Privatsphäreimplikationen in ihren Entscheidungen beeinflusst werden können. Eine weitere Möglichkeit besteht darin, direkt bei den Vorlagen anzusetzen, die Webseitenbetreibenden von sogenannten *Consent Mangement Platforms* (CMPs, dt. Plattformen für die Verwaltung von Zustimmungen) zur Verfügung gestellt werden. Das nächste Ziel lautet wie folgt:

Ziel 4: Erarbeitung von Maßnahmen zur Unterstützung von Webseitenbetreibenden bei der Vermeidung von Privatsphärerisiken auf ihren Webseiten. Untersucht an den Beispielen (a) der Bereitstellung von Informationen bei der Auswahl von Einwilligungserklärungen sowie (b) der Gestaltungsmöglichkeiten von Einwilligungserklärungen mithilfe von CMP-Vorlagen.

1.3 Aufbau, Inhalt und Beitrag der Arbeit

Die vorliegende Arbeit umfasst insgesamt fünf Kapitel, wie in Abbildung 3 dargestellt wird. Nach der Einleitung (**Kapitel 1**) folgt in **Kapitel 2** ein Überblick über die für diese Arbeit relevanten theoretischen Grundlagen. Dazu zählen neben der Definition des Privatsphäre-Begriffs ein Überblick über die rechtlichen Grundlagen und der Stand der Forschung zu Privatsphärerisiken auf Webseiten. Des Weiteren wird das Forschungsfeld Usable Privacy and Security (S&P, dt. Nutzbare Privatsphäre und Sicherheit), in dem die Arbeit verankert wird, vorgestellt. Das Kapitel wird mit der aktuellen Forschung zur Sicht der Nutzenden, der Entwickler:innen und der Webseitenbetreibenden auf Privatsphäre abgeschlossen.

Kapitel 3 ist Herausforderung 1 gewidmet, dem Beheben bestehender Privatsphärerisiken durch Webseitenbetreibende – untersucht am Beispiel der Behebung einer Fehlkonfiguration (fehlende IP-Anonymisierung) von Google Analytics. Dabei werden die Forschungsziele 1 und 2 adressiert. Im Rahmen der Studie 1a (Feldexperiment) wurden Webseitenbetreibende ($N = 4594$) mit Briefen und E-Mails über die fehlende IP-Anonymisierung auf ihrer Webseite informiert. Um die Hintergründe besser zu verstehen, wurde ein Teil dieser Webseitenbetreibenden ($N = 477$) im Rahmen von Studie 1b (Umfrage) befragt. Viele meldeten sich auf die Benachrichtigungen zurück, die sie im Rahmen des Experiments erhalten hatten. Diese Rückmeldungen ($N = 1043$) dienten als Datengrundlage für Studie 1c (Auswertung der Rückmeldungen), in der eine quantitative sowie eine qualitative Analyse weiteren Aufschluss über die Hintergründe geben sollte.

Die Ergebnisse der Untersuchungen liefern Erkenntnisse darüber, was die Ursachen für bestehende datenschutzrechtlich relevante Privatsphärerisiken auf Webseiten sind, wie Webseitenbetreibende beim Beheben vorgehen, welche Herausforderungen sie dabei überwinden müssen und wie sie effektiv

unterstützt werden können. Die Ergebnisse sowie der Beitrag aus Kapitel 3 lassen sich wie folgt zusammenfassen:

- Durch die Auswertung der Umfrage sowie der Rückmeldungen wird gezeigt, dass die Ursachen für bestehende Privatsphärerisiken auf Webseiten neben fehlendem Bewusstsein der Webseitenbetreibenden auch unklare Zuständigkeiten, fehlerhafte technische Umsetzung und mangelnde Wartung der Webseite sein können.
- Webseitenbetreibende unterscheiden sich von anderen Personengruppen, die Systeme entwickeln und betreiben (z. B. Entwickler:innen), u. a. dahingehend, dass sie teilweise nur über geringes technisches Wissen verfügen. Auch sind ihre Rahmenbedingungen und Motivationen verschieden. Webseitenbetreibende reichen von Privatpersonen, die mit der Webseite einer Freizeitbeschäftigung nachgehen, über Selbständige, die ihre Produkte vertreiben wollen, bis zu Vollzeitangestellten, die ein großes Unternehmen repräsentieren.
- Entsprechend ihrer Rahmenbedingungen variieren die Hürden, die Webseitenbetreibende beim Beheben von Privatsphärerisiken überwinden müssen. Diese Hürden reichen von fehlendem technischen Wissen bis zu zähen Organisationsprozessen.
- Es besteht ein großer Unterstützungsbedarf bei der Behebung von Privatsphärerisiken. Damit dies effektiv ist, müssen Maßnahmen auf die unterschiedlichen Bedürfnisse und Rahmenbedingungen verschiedener Webseitenbetreibenden angepasst sein.
- Durch die Arbeit wird aufgezeigt, wie eine Unterstützungsmaßnahme in Form einer Benachrichtigung gestaltet sein sollte, die bei Webseitenbetreibenden sowohl Bewusstsein schafft als auch beim Beheben von Privatsphärerisiken unterstützt.

In **Kapitel 4** werden die Forschungsziele 3 und 4 adressiert und die Herausforderung aus Sicht von Webseitenbetreibenden beim Vermeiden von Privatsphärerisiken wird beleuchtet – untersucht am Beispiel der Erstellung von Cookie-Einwilligungsklärungen. Dazu wurden zunächst mit den Studien 2a und 2b zwei aufeinanderfolgende Umfragen durchgeführt, die jeweils ein Online-Experiment inkludierten. Untersucht wurde die Perspektive der Nutzenden ($N = 376$), wobei diese mit einem fiktiven Online-Shop interagierten, der für die unterschiedlichen Experimentalgruppen verschiedene Cookie-Einwilligungserklärungen enthielt. Im Anschluss wurden Nutzende u. a. zu ihren Beurteilungen und Präferenzen hinsichtlich der Einwilligungserklärungen befragt. In Studie 2b gaben Webseitenbetreibende ($N = 195$) u. a. Auskunft zu ihren Präferenzen bezüglich der Gestaltung der Einwilligungserklärungen. Außerdem wurden sie gebeten, eine von vier möglichen Einwilligungserklärungen auszuwählen, wobei die Experimentalgruppe zusätzlich Informationen über die Nutzendenpräferenz sowie die Cookie-Zustimmungsrate (Ergebnisse aus Studie 2a) erhielt. Immer häufiger greifen Webseitenbetreibende bei der Erstellung von Einwilligungserklärungen auf die Vorlagen von CMPs zurück. Um zu untersuchen, inwiefern sie mit diesen Vorlagen Einwilligungserklärungen ohne *Deceptive Designs* generieren und damit Privatsphärerisiken vermeiden können, wurden im Rahmen der Studie 3 die Vorlagen von 15 populären CMPs analysiert. Die Ergebnisse und der Beitrag aus Kapitel 4 lassen sich wie folgt zusammenfassen:

- Aus den Ergebnissen des Online-Experiments mit Nutzenden geht hervor, dass die Gestaltung von Einwilligungserklärungen einen Einfluss auf die Zustimmungsrate hat. Sind *Deceptive Designs*

enthalten, akzeptieren mehr Nutzende alle Cookies. Nutzende präferieren jedoch Gestaltungsvarianten, die keine *Deceptive Designs* aufweisen.

- Webseitenbetreibende sind sich der Präferenzen der Nutzenden bezüglich der Gestaltung bewusst und schätzen diese korrekt ein, wählen jedoch nur zum Teil entsprechende Einwilligungserklärungen aus.
- Einwilligungserklärungen mit *Deceptive Designs* werden häufiger von Webseitenbetreibenden ausgesucht, die mit den durch Cookies gespeicherten Daten Einnahmen generieren. Dabei scheint jedoch die Popularität der Webseite eine untergeordnete Rolle zu spielen. Zentraler ist, ob das Geschäftsmodell bzw. die Werte der Organisationen hinter der Webseite die Privatsphäre von Nutzenden bestärken oder nicht.
- Es konnte nicht gezeigt werden, dass die Bereitstellung von Informationen über die Präferenz bzw. das Verhalten der Nutzenden eine wirkungsvolle Maßnahme ist, um Webseitenbetreibende dazu zu veranlassen, Privatsphärerisiken zu vermeiden – sprich Einwilligungserklärungen ohne *Deceptive Designs* zu wählen.
- Aus der Analyse der CMPs-Vorlagen ergibt sich, dass es für Webseitenbetreibende nur eingeschränkt möglich ist, damit Einwilligungserklärungen ohne *Deceptive Designs* zu erstellen, und CMPs möglicherweise einen wesentlichen Beitrag zur Entstehung von Privatsphärerisiken leisten.

In **Kapitel 5** werden die Erkenntnisse aus den vorangegangenen Kapiteln in Bezug auf die Forschungsziele diskutiert sowie die Implikationen für die Praxis herausgestellt. Es folgt eine Reflexion der Limitationen und der ethischen Aspekte. Das Kapitel wird mit einem Ausblick auf zukünftige Forschung und einer Schlussfolgerung abgeschlossen.
In dieser Arbeit wird die Perspektive der zentralen, bisher aber wenig berücksichtigten Gruppe der Webseitenbetreibenden beleuchtet. Die Erkenntnisse können helfen, die Herausforderungen beim Beheben bzw. Vermeiden von Privatsphärerisiken auf ihren Webseiten besser zu verstehen. Dieses Verständnis kann als Grundlage für die Entwicklung gezielter und wirkungsvoller Maßnahmen zur Unterstützung von Webseitenbetreibenden dienen. Webseitenbetreibende dabei zu unterstützen, die Privatsphäre der Nutzenden besser zu schützen, entlastet zugleich die Nutzenden. Somit soll durch die vorliegende Arbeit aufzeigt werden, wie Webseiten, die einst dem Austausch von Forschenden dienen sollten, zu einem privatsphärefreundlicheren Ort für alle gemacht werden können.

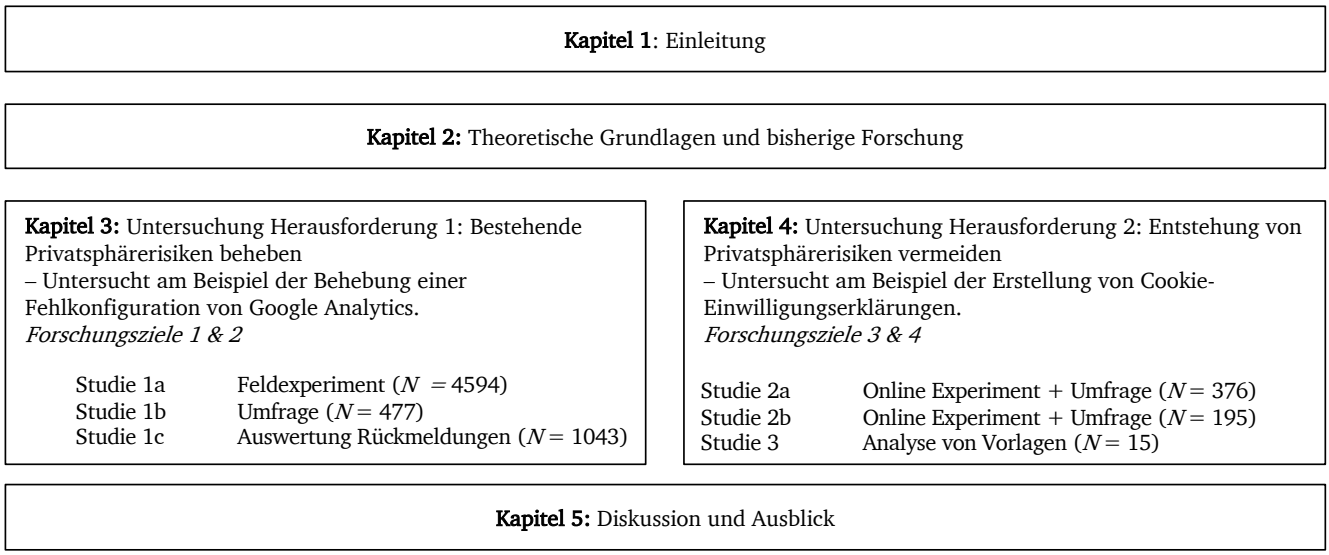


Abbildung 3. Überblick über den Aufbau der vorliegenden Arbeit.

1.4 Dahinterliegende Veröffentlichungen und Beitrag der Autorin

Die vorliegende Arbeit baut auf teils veröffentlichten Publikationen auf, die in Zusammenarbeit mit anderen Autor:innen entstanden sind. In diesem Unterkapitel wird der Beitrag der Autor:innen zu den einzelnen Publikationen dargestellt:

Paper 1 (Teil von Kapitel 3): Maass, M., **Stöver, A.**, Pridöhl, H., Bretthauer, S., Herrmann, D., Hollick, M., & Spiecker, I. (2021). Effective Notification Campaigns on the Web: A Matter of Trust, Framing, and Support. In 30th *USENIX Security Symposium (USENIX Security 21)* (pp. 2489-2506).

Konferenz Metrik: Computing Research & Education (CORE) Ranking CORE21: A* (7.32 % of 792 ranked venues). Zugegriffen am 06. Dezember 2022.

Paper 2 (Teil von Kapitel 3): **Stöver, A.**, Gerber, N., Pridöhl, H., Maass, M., Bretthauer, S., Spiecker, N., Hollick, M., & Herrmann, D. (accepted). 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)* (Vol. 2023).

Journal Metrik: Computing Research & Education (CORE) Ranking CORE21: A (16.29 % of 792 ranked venues). Zugegriffen am 06. Dezember 2022.

Paper 3 (Teil von Kapitel 4): **Stöver, A.**, Zimmermann, V., Gerber, N., Marky, K., & Khamis, M. (submission in preparation). Working Title: Website Owners Perspective on the Design of Cookie Consent Notices.

Paper 4 (Teil von Kapitel 4): **Stöver, A.**, Gerber, N., Cornel, C., Henz, M., Marky, K., Zimmermann, V. & Vogt, J. (2022). Website Operators are not the Enemy either – Analyzing Options for Creating Cookie Consent Notices Without Dark Patterns. *Mensch und Computer 2022 – Workshopband*.

Konferenz Metrik: n. A.

Kapitel 3 basiert auf einer Zusammenarbeit mit Max Maass, Matthias Hollick, Henning Pridöhl, Dominik Herrmann, Sebastian Bretthauer, Indra Spiecker und Nina Gerber. Die Grundidee für Paper 1 (Feldexperiment) stammt primär von Max Maass, Henning Pridöhl und Dominik Herrmann. Diese Forschenden haben zusammen mit der Autorin dieser Arbeit alle Entscheidungen bezüglich des Studiendesigns und der Auswertung getroffen sowie die Ergebnisse diskutiert. Max Maass bereitete die Benachrichtigungen vor, verschickte diese und reagierte auf Rückfragen der Webseitenbetreibenden. Er führte außerdem die Survival Analysis durch. Die Autorin dieser Arbeit entwickelte die Umfrage, führte diese durch und wertete die Antworten aus. Gemeinsam mit Max Maass führte sie die quantitative Analyse der Rückmeldungen durch. Sebastian Bretthauer und Indra Spiecker gen. Döhmann stellten ihr juristisches Fachwissen zur Verfügung und beantworteten Rückfragen der benachrichtigten Webseitenbetreibenden. Das Paper wurde gemeinsam verfasst, wobei jede:r die Teile schrieb, die in sein oder ihr Fachgebiet fielen. Matthias Hollick gab hilfreiches Feedback zum Paper.
Die Idee für Paper 2 (Analyse der Rückmeldungen) stammt von der Autorin dieser Arbeit. Diese führte auch die qualitative Analyse der Rückmeldungen durch. Die zweite Codierung wurde von Carlos Böhm durchgeführt. Die Autorin diskutierte mit Nina Gerber die Studienidee sowie die Ergebnisse der qualitativen Analyse. Gemeinsam mit Nina Gerber führte die Autorin den Workshop zur Entwicklung der Personas durch. Gemeinsam mit Nina Gerber, Henning Pridöhl und Dominik Herrmann diskutierte und verfasste die Autorin das Paper. Matthias Hollick und Sebastian Bretthauer gaben hilfreiches Feedback zum Paper.
Kapitel 4 beinhaltet zwei Studien. Die Idee zu Studie 2 (Paper 3) stammt von der Autorin dieser Arbeit. Diese bereitete die Studie vor, wobei die technische Umsetzung des Onlineshops auf der Arbeit von Justin Peschke basiert und von Thorsten Schumacher angepasst wurde. Die Autorin führte die Studie durch und wertete die Daten aus. Hilfreiches Feedback zur Studienidee, zur Auswertung sowie zur Interpretation der Ergebnisse steuerten Verena Zimmermann, Nina Gerber, Karola Marky und Mohamed Khamis bei.
Die Idee zu Studie 3 stammt von der Autorin dieser Arbeit. Diese bereitete die Studie vor. Die Erstellung der Cookie-Einwilligungserklärungen mithilfe der Vorlagen übernahmen Christin Cornel und Mona Henz. Nina Gerber, Verena Zimmermann und Karola Marky gaben hilfreiches Feedback während aller Schritte der Studie und übernahmen die Bewertung der zuvor erstellten Einwilligungserklärungen. Nina Gerber und Verena Zimmermann unterstützten die Autorin beim Schreiben des Papers.

2 Theoretische Grundlagen und bisherige Forschung

In diesem Kapitel werden die Konzepte und Definitionen eingeführt, die für die vorliegende Arbeit grundlegend sind, sowie bisherige Forschungsarbeiten zusammengefasst, die für diese Arbeit relevant sind. Zunächst wird das Forschungsfeld Usable Privacy and Security, in dem diese Arbeit angesiedelt ist, vorgestellt. Anschließend wird die untersuchte Technologie beschrieben. Es folgen die Definition des Privatsphäre-Begriffs sowie entsprechende rechtliche Grundlagen. Anschließend werden bisherige Forschungsarbeiten zur Perspektive verschiedener Gruppen (Nutzende, Entwickler:innen und Webseitenbetreibende) auf Privatsphäre zusammengefasst.

2.1 Forschungsfeld Usable Privacy and Security

In dem Forschungsfeld Usable Security and Privacy, in dem diese Arbeit angesiedelt ist, wird das Thema der digitalen Privatsphäre in unterschiedlichen Anwendungskontexten wie Internet of Things, Mobile Apps, Smart Home oder Web behandelt (z. B. Marky, Voit, et al., 2020; Marky, Zimmermann, et al., 2020; Stöver et al., 2020, 2021). Dabei beschäftigt sich das Forschungsfeld unter anderem damit, „*Konzepte und Tools* [zu gestalten]*, die Nutzende dabei unterstützen ihr Verhalten in Bezug auf den Schutz von Privatsphäre und Sicherheit zu verbessern*“ (Reuter et al., 2022, S. 2035). Die S&P-Forschung hat sich in der Vergangenheit primär auf die Perspektive der Personen konzentriert, die Systeme nutzen (*End Users*) (Kaur et al., 2021). Seit einiger Zeit gibt es eine wachsende Nachfrage, auch die Perspektive derjenigen zu berücksichtigen, die Systeme entwickeln und betreiben (*Expert Users*) (Kaur et al., 2021). Laut Kaur (2021) gehören zu dieser Gruppe unter anderem Entwickler:innen und Systemadministrator:innen. Inwiefern Webseitenbetreibende einer dieser Gruppen zugeordnet werden können, ist fraglich. Zum einen sind sie verantwortlich für Webseiten, haben diese gegebenenfalls auch aufgebaut und betreiben diese. Damit könnten sie den *Expert Users* zugeordnet werden. Zum anderen deuten erste Studienergebnisse darauf hin, dass Webseitenbetreibende von *Expert Users* dahingehend zu unterscheiden sind, dass viele von ihnen zwar einen technischen Hintergrund haben, die Webseiten aber nicht unbedingt als Vollzeitbeschäftigung betreiben (Utz et al., 2022).

Das Grundverständnis, dem auch diese Arbeit folgt, ist ähnlich wie das der arbeits- und ingenieurpsychologischen Forschung, in der die Menschen bzw. die Nutzenden nicht als problematischer Faktor gesehen werden, sondern ihr Potenzial als Teil der Lösung erkannt wird (Adams & Sasse, 1999; Zimmermann & Renaud, 2019). Folglich sollen auch die Personen, die Systeme entwickeln und betreiben, wie in dieser Arbeit die Webseitenbetreibenden, nicht als Feind für die Privatsphäre, sondern als Teil der Lösung betrachtet werden (Chowdhury et al., 2021).

Zusammenfassend lässt sich sagen, dass in der S&P-Forschung das Thema der digitalen Privatsphäre in unterschiedlichen Anwendungskontexten wie Internet of Things, Mobile Apps, Smart Home oder Web und aus verschiedenen menschlichen Perspektiven (z. B. *End Users* und *Expert Users*) behandelt wird. Diese Arbeit beschäftig sich mit der Privatsphäre von Webseiten aus Sicht der Webseitenbetreibenden. Da diese potenziell mit ihren Entscheidungen bzw. mit ihrem Verhalten Einfluss auf das Entstehen bzw. Bestehen von Privatsphärerisiken für Nutzende nehmen können, werden diese in den folgenden Unterkapiteln behandelt.

2.2 Privatsphärerisiken auf Webseiten

In diesem Unterkapitel werden die Privatsphärerisiken für Nutzende von Webseiten aufgezeigt. Dazu werden zunächst für diese Arbeit wichtige Definitionen wie Internet, Web und Webseiten beschrieben und im Anschluss auf das Privatsphärerisiko des Trackings sowie spezifische Privatsphärerisiken durch Drittanbieter eingegangen.

2.2.1 Definition Internet, Web und Webseiten

Das Internet lässt sich „*als ein dezentral organisiertes, globales Rechnernetz charakterisieren, das aus einer Vielzahl miteinander verbundener Einzelnetze gebildet wird und in dem die Kommunikation zwischen den einzelnen Rechnern auf der Grundlage des Transmission Control Protocol/Internet Protocol (TCP/IP)* [stattfindet]“ (Metzger et al., 2018 o. S.). Ursprünglich für militärische Zwecke entwickelt, reichen die Ursprünge des Internets in die 1950er Jahre zurück (Abbate, 2010; Metzger et al., 2018). Heutzutage werden zahlreiche Dienste wie E-Mail oder das World Wide Web (WWW, Web) über das Internet angeboten (Metzger et al., 2018). Mit der Einführung des Web war das Internet auch für die breite Bevölkerung zugänglich. Das Web ist ein „*interaktives Informationssystem, das den weltweiten Austausch digitaler Dokumente ermöglicht*“ (Lackes et al., 2018, o. S.). Es besteht dabei aus sog. Hypertext-Systemen, wobei ein Hypertext-System Webseite genannt wird (Lackes et al., 2018).

2.2.2 Tracking als Privatsphärerisiko

Ein zentrales Risiko für die Privatsphäre von Nutzenden von Webseiten stellt das User Tracking dar. Tracking beschreibt dabei „*die Methode zum Sammeln, Speichern und Analysieren von Benutzer-Browsing-Aktivitäten im Internet*“ (Ghostery, Inc., 2022). Das ursprüngliche Ziel des Trackings war es, Nutzenden ein personalisiertes Erlebnis durch gezieltes Marketing oder benutzerdefinierte Newsfeeds zu bieten (Kant, 2021). Eine Form des Trackings ist das sogenannte Third-Party-Tracking, bei dem Daten der Nutzenden von einem Onlineservice (z. B. einer Webseite) zu einer anderen Einheit, die nicht den Provider dieses Services darstellt, übertragen werden (Leon et al., 2010). Dies geschieht häufig, wenn Webseitenbetreibende Dienste von Drittanbietern mit einem entsprechenden Code auf ihren Webseiten einbinden. Zum Beispiel können Webseitenbetreibende Google Analytics von Google (Third-Party) auf ihren Webseiten integrieren, um Nutzungskennzahlen zu sammeln. Wenn Nutzende dann die Webseite besuchen, kann der Third-Party-Code z. B. Cookies im Browser der Nutzenden setzen, sodass, wenn diese andere Webseiten besuchen, die denselben Third-Party-Tracker-Code beinhalten, die Aktivitäten zwischen den Webseiten verlinkt werden können.

Diese eben beschriebene Form des Trackings wird auch als Cookie-Tracking bezeichnet, wobei Tracking-Cookies *„Textdateien* [sind]*, die kleine Mengen an Informationen aus einer Webbrowser-Sitzung auf einer Webseite speichern“* (Ghostery, Inc., 2022, o. S.). Zu den Informationen, die durch Cookies gespeichert werden können, zählen Such- und Browserverläufe, aber auch Verhalten wie die Scrollgeschwindigkeit. Eine weitere Form des Trackings stellt das sogenannte Browser-Fingerprinting dar, bei dem ‚Fingerprints‘ der Nutzenden durch die Aufzeichnung eines eindeutig zu identifizierenden Attributs oder einer Kombination von Attributen, z. B. der Browsereinstellungen oder der installierten Plugins, erstellt werden (Binns, Zhao, et al., 2018). Diese Art des Trackings wird als noch privatsphäreinvasiver

eingestuft, weil es ihr Ziel ist, möglichst viele Informationen über Nutzende zu sammeln, um so einzigartige Profile zu erstellen (Ghostery, Inc., 2022).
Tracking ist ein weit verbreitetes Phänomen. So belegen Analysen, dass 90 % der Webseiten mindestens ein Tracker-Skript enthalten, wobei Tracker von Google auf 73 % der von Dambra et al. (2022) analysierten Webseiten gefunden wurden. Nutzenden begegnen beim Besuch auf Webseiten im Laufe einer Woche durchschnittlich 177 Tracker (Dambra et al., 2022). Die Analysen von Dambra et al. (2022) belegen auch, dass große Tracker im Durchschnitt fast die Hälfte des Browserverlaufs fast aller Nutzenden kennen.

2.2.3 Spezifische Privatsphärerisiken auf Webseiten durch Drittanbieter

Viele Webseitenbetreibende verlassen sich auf die Dienste von Drittanbietern, um z. B. Nutzendenanalysen, Werbung und Einwilligungserklärungen zu implementieren. Utz et al. (2022) zeigen in ihrer Arbeit auf, dass diese Dienste jedoch häufig mit einer Reihe spezifischer Risiken einhergehen, die die Privatsphäre der Nutzenden gefährden bzw. einschränken. Dazu gehören auch zwei Risiken, die Gegenstand dieser Arbeit sind:
(1) Fehlkonfiguration von Analysetools: Um das Verhalten der Nutzenden sowie die Leistung der Webseite zu analysieren, greifen Webseitenbetreibende in der Regel auf Analysetools von Drittanbietern zurück. Eine beliebte und häufig eingesetzte Lösung ist Google Analytics, ein Dienst, der für die Verfolgung des Surfverhaltens über Webseiten hinweg kritisiert wird (Utz et al., 2022). Wenn Google Analytics fehlkonfiguriert ist, können Webseitenbetreibende zusätzlich die Privatsphäre ihrer Nutzenden verletzen (Utz et al., 2022). Um zu verhindern, dass Google die IP-Adresse der Nutzenden zusammen mit den Analysedaten speichert, müssen Webseitenbetreibende die IP-Anonymisierung von Google Analytics aktivieren (Google, 2020). Allerdings wird später in dieser Arbeit gezeigt werden, dass nicht alle Webseitenbetreibenden dieser datenschutzrechtlichen Anforderung nachkommen und die Fehlkonfiguration dieses Analysetools ein weitverbreitetes Privatsphärerisiko darstellt.
(2*) Deceptive Designs* in Einwilligungserklärungen: Webseitenbetreibende greifen zur Erstellung von Einwilligungserklärungen zunehmend auf die Vorlagen von Drittanbietern zurück. Diese stehen jedoch in der Kritik, sogenannte *Deceptive Designs* zu enthalten, sprich Gestaltungselemente, die die Nutzenden dazu verleiten, eher ihre Einwilligung zu erteilen (Utz et al., 2019).
Weitere spezifische Privatsphärerisiken, die auf die Dienste von Drittanbietern zurückgehen, sind z. B. auf Webseiten eingebundene Zahlungsanbieter (z. B. PayPal[5]), die sensible Daten von Nutzenden sammeln, oder Werbenetzwerke (z. B. Amazon Ads), die Nutzendenprofile aus den gesammelten Daten erstellen (Utz et al., 2022).

2.3 Definition von Privatsphäre

Privatsphäre ist ein Konzept, das Beachtung in verschiedenen Disziplinen wie der Philosophie, der Psychologie, der Soziologie und den Rechtswissenschaften findet und seit 100 Jahren in fast allen Bereichen der Sozialwissenschaften erforscht wird (Smith, Jeff et al., 2011). Dennoch ist weithin anerkannt, dass das Konzept der Privatsphäre unklar ist (Smith, Jeff et al., 2011). Es gibt kein einheitliches Konzept für den Schutz der Privatsphäre, das sich über alle Disziplinen erstreckt und von

[5] Paypal ist ein Online-Bezahldienst (Bocksch, 2022)

allen Beobachtern akzeptiert wird (Smith, Jeff et al., 2011). Smith et al. (2011) geben in ihrer Arbeit „Information Privacy Research: An ‚Interdisciplinary Review'" einen umfassenden Überblick über verschiedene Definitionsansätze der Privatsphäre. Sie unterscheiden dabei zwischen wertbasierten und kognitionsbasierten Definitionsansätzen (Smith, Jeff et al., 2011). Nach Smith et al. (2011) wird die allgemeine Privatsphäre in wertorientierten Definitionen als ein Menschrecht betrachtet, das ein integraler Bestandteil des moralischen Wertesystems der Gesellschaft ist. Weitere Ausführungen und Definitionen zur Privatsphäre als Menschenrecht aus rechtlicher Perspektive finden sich in Abschnitt 2.4.1. Als einen weiteren Definitionsstrang, den Smith et al. (2011) zu den wertbasierten Ansätzen zählen, ist das Verständnis von Privatsphäre als ein wirtschaftliches Gut. Zu den kognitionsbasierten Definitionsansätzen gehören die Sicht der Privatsphäre als Zustand sowie als Kontrolle (Smith, Jeff et al., 2011). Dazu zählt z. B. Altmans (1977) Definition von allgemeiner Privatsphäre als *„the selective control of access to the self"*, was übersetzt *„die selektive Kontrolle des Zugangs zum Selbst"* bedeutet (Altman, 1977, S. 67). Ein weitere und populäre Definition, die den Kontrollaspekt beinhaltet, stammt von Alan Westin (1968). Er definiert Privatsphäre in Bezug auf Informationen als

> *„the claim of individuals [...] to determine for themselves when, how, and to what extent information about them is communicated to others"*

Übersetzt beschreibt Privatsphäre demnach *„den Anspruch des Einzelnen* [...], *selbst zu bestimmen, wann, wie und in welchem Umfang Informationen über ihn* [oder sie] *an andere weitergegeben werden"* (Westin, 1968, S. 7).

Eine weitere begriffliche Unterscheidung kann zwischen der informationellen Privatsphäre und der physischen Privatsphäre vorgenommen werden. Während erstere den Zugang zu individuell identifizierbaren persönlichen Informationen meint, betrifft letztere den physischen Zugang zu einer Person und/oder ihrer Umgebung (Smith, Jeff et al., 2011). Auch wenn die Definition von Westin aus einer Zeit stammt, in der der Austausch von Daten über das Internet für die breite Bevölkerung noch nicht möglich war, kann diese auch auf digitale Informationen bzw. Daten übertragen werden und somit als eine Definition für digitale Privatsphäre dienen.

In dieser Arbeit wird der Begriff Privatsphäre verwendet, wobei dieser sich auf Privatsphäre im Kontext digitaler Informationen bezieht. Auch wenn es an einigen Stellen konkret um Datenschutz geht, wird der Konsistenz halber der Privatsphärebegriff verwendet, weil Datenschutz als Teil von Privatsphäre verstanden wird, in dem Sinne, dass fehlender Datenschutz zur Einschränkung der Privatsphäre führen kann. Ferner wird in dieser Arbeit anerkannt, dass der Begriff der Privatsphäre nicht abschließend definiert ist. Für diese Arbeit soll Westins Definition als Ausgangspunkt, jedoch nicht als endgültige Definition dienen, denn auch dieser Definitionsansatz hat seine Grenzen. Wie Laufer und Wolfe (1977) bemerken, ist eine „*situation* [...] *not necessarily a privacy situation simply because the individual perceives, experiences, or exercises control/choice*" (Laufer & Wolfe, 1977, S. 26), was übersetzt heißt, dass eine „*Situation* [...] *nicht notwendigerweise eine Situation der Privatsphäre* [ist]*, nur weil die Person Kontrolle/Wahlmöglichkeit wahrnimmt, erlebt oder ausübt*" (Laufer & Wolfe, 1977, S. 26).

2.4 Relevante rechtliche Grundlagen für diese Arbeit

Im Folgenden werden die für diese Arbeit relevanten rechtlichen Grundlagen beschrieben. Zunächst wird auf die rechtlichen Aspekte der Begriffe der Privatsphäre und des Datenschutzes eingegangen. Anschließend wird ein kurzer Einblick in die DSGVO sowie das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) gegeben. Daraus leitet sich auch das Erfordernis einer informierten Einwilligung ab, wie sie am Ende des Unterkapitels beschrieben wird.

2.4.1 Privatsphäre und Datenschutz aus rechtlicher Perspektive

Für diese Arbeit ist die Unterscheidung zwischen Privatsphäre und Datenschutz relevant. Diese Unterscheidung wird auch vom Europäischen Datenschutzbeauftragten (EDSB) vorgenommen, der die unabhängige Datenschutzbehörde der Europäischen Union (EU) ist (European Data Protection Supervisor, 2022b). Dieser merkt an, dass es sich beim Schutz der Privatsphäre und des Datenschutzes um verschiedene Rechte handelt (European Data Protection Supervisor, 2022a). „*Beim Datenschutz geht es darum, alle Informationen, die sich auf eine bestimmte oder bestimmbare (lebende) natürliche Person beziehen, zu schützen – unter anderem Namen, Geburtsdaten, Fotos, Videoaufnahmen, E-Mail-Adressen und Telefonnummern*“ (European Data Protection Supervisor, 2022a, o. S.). Darüber hinaus gelten auch weitere Angaben, z. B. IP-Adressen, als personenbezogene Daten (European Data Protection Supervisor, 2022a). Das Recht auf Datenschutz ist mit Artikel 8, Schutz personenbezogener Daten, in der Charta der Grundrechte der EU verankert. Dort ist unter anderem vermerkt, dass „[j]*ede Person* […] *das Recht auf Schutz der sie betreffenden personenbezogenen Daten*“ hat. Der Begriff des Datenschutzes ist eng mit dem Recht auf Privatsphäre verbunden. Laut dem EDSB hat „*der Begriff des Datenschutzes* […] *seinen Ursprung im Recht auf Privatsphäre*“ (European Data Protection Supervisor, 2022a, o. S.). Privatsphäre wiederum ist mit Artikel 12, Recht auf Privatsphäre und auf ein Privatleben, in der Allgemeinen Erklärung der Menschenrechte verankert (European Data Protection Supervisor, 2022a). Der Begriff findet sich außerdem in Artikel 8 der Europäischen Menschenrechtskonvention sowie in Artikel 7 der Europäischen Charta der Menschenrechte wieder. So ist in Artikel 8 Absatz 1 der Europäischen Menschenrechtskonvention festgehalten, dass „[j]*ede Person* […] *das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz*“ hat. In Artikel 7, Achtung des Privat- und Familienlebens, der Charta der Grundrechte der EU steht: „*Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.*“

2.4.2 Datenschutz-Grundverordnung

Den Rechtsrahmen für den Datenschutz in der EU bildet die DSGVO, die im April 2016 von der EU verabschiedet wurde und seit Mai 2018 in der EU uneingeschränkt gilt (European Data Protection Supervisor, 2022a). In Artikel 1 Absatz 1 und 2 der DSGVO steht, dass „[d]*iese Verordnung* […] *Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten* [enthält]. *Sie schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten*“ (DSGVO, 2016). In Artikel 5 Absatz 1 der DSGVO sind unter anderem sieben Grundsätze für die Verarbeitung personenbezogener Daten enthalten. Drei für diese Arbeit besonders relevante Grundsätze sollen an dieser Stelle zitiert werden:

- Der Grundsatz der Datenminimierung besagt, dass die Verarbeitung personenbezogener Daten „*dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein*“ (Art. 5 Abs. 1 lit. c DSGVO) muss.
- Der Grundsatz der Speicherbegrenzung schreibt vor, dass „*personenbezogene Daten* […] *länger gespeichert werden* [dürfen], *soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden*“ (Art. 5 Abs. 1 lit. e DSGVO).
- Der Grundsatz der Integrität und Vertraulichkeit besagt, dass personenbezogene Daten „*in einer Weise verarbeitet werden* [müssen], *die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen*“ (Art. 5 Abs. 1 lit. f DSGVO).

In der DSGVO ist außerdem festgehalten, dass bei der Verarbeitung personenbezogener Daten diese nur rechtmäßig ist, wenn eine Einwilligung der betroffenen Person vorliegt (BfDI, o. J.).

2.4.3 Telekommunikation-Telemedien-Datenschutz-Gesetz

Ein weiteres für diese Arbeit relevantes Gesetz ist das TTDSG. Es handelt sich dabei um eine spezialgesetzliche Regelung für den Bereich der elektronischen Kommunikation, die neben die DSGVO tritt und am 1. Dezember 2021 in Deutschland in Kraft getreten ist. Zu den Telemedien werden in diesem Gesetz unter anderem Webseiten gezählt. Das Gesetz soll unerwünschte Zugriffe auf Informationen verhindern, die auf Computern, Tablets oder Mobiltelefonen gespeichert sind (HmbBfDI, 2021). Das TTDSG besagt außerdem Folgendes: „*Die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, sind nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat. Die Information des Endnutzers und die Einwilligung haben gemäß der Verordnung (EU) 2016/679 zu erfolgen*“ (§ 25 Abs. 1 TTDSG).

2.4.4 Einwilligungserklärungen

Wie bereits im vorangegangenen Unterkapitel beschrieben, müssen Webseitenbetreibende sowohl nach DSGVO, wenn sie personenbezogene Daten verarbeiten, als auch nach TTSDG, wenn sie Technologien wie Cookies oder Fingerprinting einsetzen, vorher die Einwilligung der Nutzenden einholen. Diese Einwilligungen können auch gleichzeitig eingeholt werden (HmbBfDI, 2021). Eine solche Einwilligung muss nach Artikel 4 Absatz 11 und Artikel 7 der DSGVO eine Reihe an Voraussetzungen erfüllen, die auf der Webseite der Bundesbeauftragten für Datenschutz und die Informationsfreiheit im Detail nachzulesen sind (BfDI, o. J.). Zusammenfassend lässt sich sagen, dass eine solche Einwilligung eine unmissverständlich abgegebene Willensbekundung der betroffenen Person ist, die in informierter Weise und freiwillig abgegeben werden muss.

2.5 Privatsphäre auf Webseiten aus Sicht von Nutzenden

In der bisherigen Forschung konnte zum einen gezeigt werden, dass Nutzende zu einem gewissen Grad ein Bewusstsein über Tracking-Praktiken von Drittanbietern haben und sich dadurch in ihrer Privatsphäre eingeschränkt fühlen (Samat et al., 2017; Weinshel et al., 2019). Andererseits wurde auch berichtet, dass die Teilnehmenden überrascht sind, wenn sie mit detaillierten Informationen über das Ausmaß und die Häufigkeit des Trackings konfrontiert werden (Samat et al., 2017; Weinshel et al., 2019). Sobald sich die Nutzenden der tatsächlichen Auswirkungen bewusst waren, sprachen sie sich gegen solche Praktiken aus und sie hatten verstärkt die Absicht, Maßnahmen zum Schutz der Privatsphäre zu ergreifen (Purcell et al., 2023) bzw. die Nutzenden fühlten sich mit der Datenerhebung deutlich weniger wohl und waren eher bereit, Schutzmaßnahmen zu ergreifen (Arias-Cabarcos et al., 2022). Jedoch scheint nur ein kleiner Anteil der Nutzenden aktiv Maßnahmen zu ergreifen, um ihre Privatsphäre beim Besuch von Webseiten zu schützen. In einer Untersuchung von Weinshel et al. (2019) gaben nur 8.5 % der befragten Teilnehmenden an, dass sie Tools zum Blockieren von Trackern verwenden, und nur 0.59 % von ihnen nutzen Suchmaschinen, die die Privatsphäre schützen (Weinshel et al., 2019). Häufig sind sich Nutzende nicht bewusst, dass es Tools zum Schutz ihrer Privatsphäre gibt, z. B. den Tor Browser (Story et al., 2021). Wenn sie davon gehört haben, nutzen sie diese nicht (Story et al., 2021). Nur ungefähr 50 % der 500 befragten Personen von Story et al. (2021) hat schon einmal ein *Virtual Private Network* (dt. virtuelles privates Netzwerk, kurz: VPN) bewusst genutzt. Diese Maßnahmen, die direkt bei den Nutzenden ansetzen, sind ein essenzieller Bestandteil für den Schutz ihrer Privatsphäre. Gleichzeitig wird damit jedoch auch eine große Last auf die Nutzenden übertragen, die sich häufig machtlos und überfordert fühlen, wenn sie versuchen, die Kontrolle über ihre Daten zu behalten (Pew Research Center, 2019).

2.6 Privatsphäre aus Sicht von Entwickler:innen

Wie bereits in Unterkapitel 2.1 dargestellt, wird in der S&P-Forschung zunehmend die Perspektive der Personen untersucht, die Systeme entwickeln und betreiben (*Expert Users*) (Kaur et al., 2021). Ob Webseitenbetreibende zu den *Expert Users* gezählt werden können, ist noch ungeklärt. Es ist dennoch anzunehmen, dass Webseitenbetreibende ähnlich wie Entwickler:innen und Systemadministrator:innen mit ihren Entscheidungen bei der Gestaltung der Systeme einen Einfluss auf die Privatsphäre der Nutzenden nehmen können. Daher soll an dieser Stelle die Perspektive von *Expert Users* auf Privatsphäre zusammengefasst werden, um später Gemeinsamkeiten und Unterschiede zwischen Webseitenbetreibenden und *Expert Users* zu diskutieren.

In der bisherigen Forschung zu *Expert Users* und Privatsphäre wurde die Perspektive von Entwickler:innen mobiler Apps (Alomar & Egelman, 2022; Balebako et al., 2014; Mhaidli et al., 2019) und anderer Software (Hadar et al., 2018; Nurgalieva et al., 2021) analysiert. Durch diese Studien werden erste Erkenntnisse zu deren Einstellung zu Privatsphäre, zu Faktoren, die die Umsetzung von Privatsphäremaßnahmen beeinflussen, und zu Herausforderungen bei der Umsetzung vermittelt. Eine der Hauptmotivationen für *Expert Users*, Privatsphäre in ihren Systemen oder Produkten zu berücksichtigen, stellt der Wunsch dar, datenschutzrechtliche Anforderungen einzuhalten, (Agrawal et al., 2021) sowie, im Falle von mobilen Apps, deren Akzeptanz durch die App-Stores (Alomar & Egelman, 2022). *Expert Users* müssen die Vorteile von Privatsphäre für Nutzende gegen die Funktionalität, aber auch gegen die Notwendigkeit, ihr Produkt zu monetarisieren, und gegen die zusätzlichen Kosten, die

sich aus der Umsetzung von Privatsphäremaßnahmen ergeben, abwägen (Balebako et al., 2014). In einigen Fällen schränken sie die Privatsphäre ihrer Nutzenden bewusst ein, um Einnahmen aus deren Daten zu generieren. Auch finden sie nicht immer alle Privatsphärerichtlinien nützlich. Bei der Nutzung von Drittanbieterdiensten greifen *Expert Users* in der Regel auf den Marktstandard zurück und verwenden die Standardeinstellungen (Mhaidli et al., 2019). Damit hoffen sie, die rechtlichen Standards zu erfüllen. *Expert Users*, die Apps entwickeln, verlassen sich hauptsächlich auf das Feedback, das sie von den App-Stores erhalten, um festzustellen, ob ihre Apps ausreichend datenschutzrechtskonform sind. Im Allgemeinen scheinen sie sich der Datenpraktiken ihrer Produkte und der Praktiken der in ihren Produkten verwendeten Drittanbieterdienste nicht bewusst zu sein (Alomar & Egelman, 2022; Balebako et al., 2014; Hadar et al., 2018). Darüber hinaus fühlen sie sich oft nicht für den Schutz der Privatsphäre der Nutzenden verantwortlich, sondern sehen dies eher als Aufgabe der Drittanbieter oder der Nutzenden selbst an (Mhaidli et al., 2019; Nurgalieva et al., 2021; Tahaei, Li, et al., 2022).
Es gibt mehrere Faktoren, die die Umsetzung von Privatsphäremaßnahmen beeinflussen. Entscheidend ist z. B. die persönliche Einstellung der *Expert Users* und ihr Wissen über Privatsphäre. Auch organisatorische Faktoren spielen eine Rolle: Reifere Unternehmen priorisieren Privatsphäremaßnahmen eher und finanziell gut aufgestellte App-Entwickler:innen lagern die meisten Privatsphäre-Entscheidungen an externe Prüfstellen aus. Bei kleineren Unternehmen ist es weniger wahrscheinlich, dass sie ein positives Privatsphäreverhalten zeigen, und für diese ist es schwieriger, die datenschutzrechtlichen Anforderungen zu erfüllen (Alomar & Egelman, 2022). Bei der Integration von Drittanbieterdiensten müssen *Expert Users* damit umgehen, dass Privatsphäreinformationen versteckt oder unverständlich sind (Tahaei, Ramokapane, et al., 2022). Mehrere Forschende betonen einen hohen Bedarf an nutzbaren Tools, die *Expert Users* dabei helfen, Privatsphärerisiken zu erkennen und zu beheben sowie die Einhaltung der datenschutzrechtlichen Anforderungen zu überprüfen (Alomar & Egelman, 2022; Balebako et al., 2014; Nurgalieva et al., 2021). In Vorstudien wurden Unterstützungsansätze für *Expert Users* in der Praxis bewertet, z. B. das Versenden von Benachrichtigungen, um das Bewusstsein für Privatsphäre- und Sicherheitsprobleme auf ihrer Webseite zu stärken (Canali et al., 2013; Çetin et al., 2017; Durumeric et al., 2014; Stock et al., 2016, 2018; Vasek & Moore, 2012; Zeng, Li, & Stark, 2019).

2.7 Privatsphäre aus Sicht von Webseitenbetreibenden

In diesem Unterkapitel wird die Sicht von Webseitenbetreibenden auf Privatsphäre beleuchtet. Dazu wird zunächst der Begriff ‚Webseitenbetreibende' näher beschrieben, bevor auf die bisherige Forschung zu ihrer Perspektive eingegangen wird.

2.7.1 Definition Webseitenbetreibende

Hinter jeder (aktiven) Webseite steht auch mindestens ein Webseitenbetreibender bzw. eine Webseitenbetreibende (Fachverband deutscher Webseiten-Betreiber, 2017). Laut dem Fachverband deutscher Webseiten-Betreiber (2017, o. S.) ist ein „*Webseitenbetreiber* […] *Urheber einer Webseite*" (Fachverband deutscher Webseiten-Betreiber, 2017, o. S.). In den meisten Fällen müssen die Betreibenden einer Webseite Angaben über ihre Identität im Impressum bereitstellen (Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV),

2022). Sowohl in der bisherigen Forschung als auch im Recht werden unterschiedliche Begriffe für Webseitenbetreibende verwendet, wobei diese nicht immer eindeutig definiert und oder voneinander abzugrenzen sind. So finden sich im englischen Sprachgebrauch sowohl der Begriff *Website Owner* (dt. Webseiteninhaber:in) als auch *Website Operator* (dt. Webseitenbetreibende:r) und äquivalent existieren im Deutschen die Begriffe ‚Webseiteninhabende' sowie ‚Webseitenbetreibende'. In dieser Arbeit wird der Begriff ‚Webseitenbetreibende' verwendet. Damit ist in erster Linie die Person gemeint, die für die Webseite verantwortlich und im Impressum vermerkt ist. Jedoch sind gerade in größeren Unternehmen häufig mehrere natürliche Personen bei der Erstellung und der Wartung von Webseiten involviert, weshalb nicht immer mit Sicherheit gesagt werden kann, wer genau der oder die Webseitenbetreibende ist. Dies muss genaugenommen in jedem Einzelfall geprüft werden. Das kann z. B. der Fall sein, wenn Daten im Impressum nicht korrekt oder veraltet sind. In dieser Arbeit werden zunächst diejenigen als Webseitenbetreibende definiert, die im Impressum stehen und für die Webseite verantwortlich sind.
Schätzungen zufolge gibt es allein in Deutschland 5.6 Mio. Webseitenbetreibende (Fachverband deutscher Webseiten-Betreiber, 2017). Diese Zahl verdeutlicht, dass Webseitenbetreibende kein Randphänomen sind, sondern viele Menschen in Deutschland potenziell zu dieser Gruppe gehören. Das ist auch nicht verwunderlich, wenn bedacht wird, dass auch viele Vereine oder lokale Einzelhändler:innen eine Webseite betreiben. Das gibt einen ersten Hinweis darauf, dass Webseitenbetreibende sich möglicherweise von anderen *Expert Users* unterscheiden, die meist einen technischen Hintergrund haben und dem Entwickeln oder Betreiben digitaler Systeme im Rahmen einer Vollzeitbeschäftigung nachgehen.

2.7.2 Bisherige Forschung zur Perspektive von Webseitenbetreibenden auf Privatsphäre

Obwohl bereits gefordert, wurde der Perspektive von Webseitenbetreibenden auf die Privatsphäre bisher wenig Aufmerksamkeit geschenkt (Acar et al., 2016; Ginosar & Ariel, 2017; Kaur et al., 2021). Utz et al. (2022) haben E-Mail-Adressen aus GitHub-Repositorien gesammelt und Personen, die an der Erstellung und Pflege von Webseiten beteiligt sind, zu einer Umfrage eingeladen (N = 395). Für zehn gängige Webseiten-Funktionen untersuchten Utz et al. (2022), ob die Privatsphäre ein Faktor war, der bei der Integration einer Funktion berücksichtigt wurde, ob die Umfrageteilnehmenden besondere Anstrengungen unternahmen, um die Privatsphäre der Nutzenden zu schützen, und inwieweit sich die Teilnehmenden der Datenerfassung durch Dritte bewusst waren (Utz et al., 2022, S. 202) . Sie fanden heraus, dass eine einfache Integration die Akzeptanz von Drittanbietern begünstigt und der Schutz der Privatsphäre der Nutzenden berücksichtigt wird, wenn es rechtliche Anforderungen oder entsprechende Richtlinien gibt. Das Bewusstsein für die Datenerfassung und Privatsphärerisiken ist höher, wenn die Erfassung direkt mit dem Zweck des Drittanbieterdienstes zusammenhängt. Die meisten Teilnehmenden hatten einen technischen Abschluss, wobei ein Drittel im Rahmen einer unbezahlten Tätigkeit (als Hobby) an einer Webseite beteiligt war. Auch diese Beobachtung deutet darauf hin, dass sich Webseitenbetreibende von anderen *Expert Users* unterscheiden, die oft hauptberuflich Systeme entwickeln und betreiben (Alomar & Egelman, 2022). Eine weitere verwandte Arbeit über Privatsphäreaspekte und Webseitenbetreibende wurde von Hennig et al. (2022) veröffentlicht. Die Forschenden zielten darauf ab, zu verstehen, wie Webseiten die Verwendung von Cookie-Einwilligungserklärungen rechtfertigen, die nicht den gesetzlichen Anforderungen entsprechen (z. B.

indem sie es schwieriger machen, Tracking abzulehnen als diesem zuzustimmen). Im Gegensatz zu den Untersuchungen in dieser Arbeit kontaktierten Hennig et al. (2022) die Datenschutzbeauftragten der entsprechenden Webseiten. Sie erhielten nur wenige Antworten. Die Antworten deuteten darauf hin, dass ein Grund für nicht konforme Cookie-Einwilligungserklärungen darin liegen könnte, dass Webseitenbetreibende keinen Einfluss auf die Gestaltung der Einwilligungserklärungen nehmen können, weil sie von Dritten (Einwilligungsmanagement-Anbietern) bereitgestellt werden (Hennig, Dietmann, et al., 2022).

3 Herausforderung 1: Behebung bestehender Privatsphärerisiken – Untersucht am Beispiel der Behebung einer Fehlkonfiguration von Google Analytics

Im vorherigen Kapitel wurden die theoretischen Grundlagen für diese Arbeit vorgestellt. In diesem Kapitel wird die erste Herausforderung untersucht, der sich die Webseitenbetreibenden gegenübergestellt sehen, wenn sie die Privatsphäre ihrer Nutzenden schützen wollen: der Behebung von bestehenden Privatsphärerisiken auf ihren Webseiten – untersucht am Beispiel der fehlenden IP-Anonymisierung von Google Analytics.

3.1 Motivation und Überblick

Ist eine Webseite online, muss sie von den Webseitenbetreibenden auch gewartet werden. Geschieht das nicht, kann das Konsequenzen für die Sicherheit und die Privatsphäre der Nutzenden haben. Außerdem müssen die Webseitenbetreibenden unter Umständen mit empfindlichen Strafen rechnen, wenn sie ihre Webseiten nicht auf dem aktuellen Stand halten und damit etwa datenschutzrechtliche Anforderungen nicht erfüllen. Ein bereits vorgestelltes Beispiel ist die fehlende IP-Anonymisierung von Google Analytics. Wie im vorherigen Unterkapitel dargestellt, greifen viele Webseitenbetreibende auf Analysetools zurück, um z. B. das Verhalten der Nutzenden oder die Webseitenleistung zu messen (Utz et al., 2022). Am häufigsten wird hier Google Analytics eingesetzt. Um die Privatsphäre der Nutzenden zu schützen, müssen Webseitenbetreibende jedoch manuell Konfigurationen vornehmen und z. B. die IP-Anonymisierung implementieren. Dass dies nicht immer geschieht, zeigt die Analyse von 1.3 Mio. deutschen Webseiten von Maass et al. (2021). Bei 12.7 % der gescannten Webseiten wurde die IP-Anonymisierung von Google Analytics nicht oder inkorrekt umgesetzt. Damit Datenschutzgesetze effektiv werden und die Privatsphäre der Nutzenden geschützt werden kann, müssen die geforderten Maßnahmen auch umgesetzt werden. Obwohl nur kleine Änderungen im Code vorgenommen werden müssen und die potenziellen Strafen für viele Webseitenbetreibende spürbar sein dürften, schaffen es nicht alle, die gesetzlichen Datenschutzanforderungen umzusetzen. Die Gründe dafür sind noch ungeklärt. Daraus ergeben sich die folgenden Ziele für dieses Kapitel:

Ziel 1: Entwicklung eines besseren Verständnisses für die Herausforderung für Webseitenbetreibende, bestehende Privatsphärerisiken auf ihren Webseiten zu beheben. Untersucht am Beispiel der Behebung einer Fehlkonfiguration von Google Analytics.

Ziel 2: Erarbeitung von Maßnahmen, wie Webseitenbetreibende bei der Behebung von Privatsphärerisiken auf ihren Webseiten unterstützt werden können. Untersucht am Beispiel von Benachrichtigungen zum Hinweis auf die Fehlkonfiguration von Google Analytics.

Um die beiden Forschungsziele zu adressieren, wurden drei Untersuchungen durchgeführt: (1) Feldexperiment: Im Rahmen eines Feldexperiments wurden Webseitenbetreibende ($N = 4594$) mit Briefen und E-Mails über die fehlende IP-Anonymisierung von Google Analytics auf ihrer Webseite

informiert.[6] (2) Umfrage: Um die Hintergründe besser zu verstehen, wurde ein Teil dieser Webseitenbetreibenden ($N = 477$) mittels Fragebogen im Nachgang befragt. (3) Auswertung Rückmeldungen: Viele Webseitenbetreibende meldeten sich auf die Benachrichtigung zurück, die sie im Rahmen des Experiments erhalten hatten. Diese Rückmeldungen ($N = 1043$) dienten als Datengrundlage für eine quantitative und qualitative Analyse, die weiteren Aufschluss über die Hintergründe der betroffenen Webseitenbetreibenden geben soll.

Die Erkenntnisse aus den Untersuchungen können dabei helfen, besser zu verstehen, warum Webseitenbetreibende es nicht schaffen, datenschutzrechtliche Anforderungen auf ihren Webseiten umzusetzen, welche Hürden sie bei der Bewältigung dieser Herausforderung überwinden müssen und wie effektive Unterstützungsangebote aussehen können. In Abbildung 4 wird ein Überblick über Kapitel 3 gegeben. Zunächst werden die für dieses Kapitel relevanten theoretischen Grundlagen sowie der Stand der Forschung, auf dem das Kapitel aufbaut, beschrieben. Einleitend wird eine kurze Einführung zu Analysetools auf Webseiten und den damit einhergehenden Privatsphärerisiken gegeben. Es folgt eine Beschreibung der Rechtslage zur fehlenden IP-Anonymisierung des Analysetools Google Analytics. Schließlich wird die bisherige Forschung zu Unterstützungsmaßnahmen von Webseitenbetreibenden zusammengefasst. Aufbauend auf den theoretischen Grundlagen und der bisherigen Forschung werden im folgenden Unterkapitel die Forschungsfragen dieses Kapitels beschrieben. In den weiteren Unterkapiteln werden die Methoden des durchgeführten Feldexperiments, der Umfrage sowie der Auswertung der Rückmeldungen beschrieben. Ethische Überlegungen werden angegeben und darauffolgend werden die Ergebnisse vorgestellt und diskutiert.

Kapitel 3: Untersuchung Herausforderung 1: Bestehende Privatsphärerisiken beheben
– Untersucht am Beispiel der Behebung einer Fehlkonfiguration von Google Analytics.
Forschungsziele 1 & 2

Studie 1a	Feldexperiment ($N = 4594$)
Studie 1b	Umfrage ($N = 477$)
Studie 1c	Auswertung Rückmeldungen ($N = 1043$)

Abbildung 4. Überblick über Kapitel 3.

[6] Hinweis: Das Feldexperiment ist Gegenstand der Dissertation von Max Maaß und wird hier der Vollständigkeit halber, auch damit die folgenden Arbeiten besser einzuordnen sind, zusammengefasst. Eine detaillierte Beschreibung des Experiments inkl. technischer Details findet sich in Maass et al. (2021).

3.2 Theoretische Grundlagen und bisherige Forschung

In diesem Unterkapitel werden die theoretischen Grundlagen sowie die bisherige Forschung, die für dieses Kapitel relevant ist, vorgestellt.

3.2.1 Analysetools und Privatsphärerisiken

Webseitenbetreibende greifen häufig auf die Dienste von Drittanbietern zurück, um Funktionalitäten auf ihren Webseiten zu ermöglichen. Dazu gehören auch Analysetools wie Google Analytics. Diese erlauben die Messung des Nutzendenverhaltens sowie die Bewertung der Webseitenleistung und des Marketingerfolgs (Utz et al., 2022). Analysen deuten darauf hin, dass Google Analytics der Drittanbieterdienst mit der höchsten Reichweite ist (Karaj et al., 2019). Karaj et al. (Karaj et al., 2019) analysierten über zwölf Monate hinweg 1.5 Mrd. Seitenaufrufe und zeigten, dass bei rund 46 % Google Analytics präsent ist. Aufgrund ihrer weiten Verbreitung stehen Analysetools wie Google Analytics in der Kritik, das Verhalten von Nutzenden über Webseiten hinweg zu verfolgen sowie umfangreiche Daten zu erfassen und diese mit anderen zu teilen (z. B. mit Werbenetzwerken) (Utz et al., 2022).

3.2.2 Fehlende IP-Anonymisierung von Google Analytics

Am 01.11.2019 entschied das Landgericht Dresden, dass Webseitenbetreibende, die Google Analytics auf ihrer Webseite eingebunden haben, eine Anonymisierung der IP-Adresse vornehmen müssen. In den meisten Fällen bedeutet das, dass Webseitenbetreibende eine Zeile Java-Code im Webseitenskript manuell anpassen müssen. Die detaillierte Beschreibung des technischen Hintergrunds zur IP-Anonymisierung von Google Analytics findet sich in Maass et al. (2021). Die Anforderung, eine IP-Anonymisierung zu implementieren, ergibt sich aus der DSGVO. Das Landgericht Dresden entschied, dass das Unterlassen der IP-Anonymisierung gegen die Datenschutzgrundsätze der Datenminimierung und der Speicherbegrenzung sowie gegen die Nichtverwendung von Pseudonymisierungs- und Anonymisierungstechniken verstößt. Die entsprechenden rechtlichen Grundlagen sind in Unterkapitel 2.4.2 beschrieben. Eine Nichtumsetzung der IP-Anonymisierung kann potenziell empfindliche Strafen für die Webseitenbetreibenden zur Folge haben. Die Geldbußen können bis zu 20 Mio. € oder im Fall eines Unternehmens bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres betragen, je nachdem, welcher der Beträge höher ist (Art. 83 Abs. 5 DSGVO). Eine Analyse von 1.3 Mio. deutschen Webseiten von Maass et al. (Maass et al., 2021) ergab, dass bei 12.7 % der gescannten Webseiten die IP-Anonymisierung von Google Analytics nicht oder inkorrekt umgesetzt wird.

3.2.3 Unterstützungsmaßnahmen für Webseitenbetreibende

Es stellt sich also die Frage, wie Webseitenbetreibende dabei unterstützt werden können, solche Fehlkonfigurationen wie die fehlende IP-Anonymisierung von Google Analytics zu beheben. Ein Ansatz, der bereits in anderen Kontexten, z. B. bezüglich Sicherheitslücken auf Webseiten, erforscht wurde, stellen Benachrichtigungen von Webseitenbetreibenden dar. Diese zielen darauf ab, zunächst ein Bewusstsein für das Problem zu schaffen. Die Wirksamkeit von Benachrichtigungen wurde in verschiedenen Bereichen untersucht, von der Sicherheit von Webseiten (Canali et al., 2013; Çetin et al., 2017; Durumeric et al., 2014; Stock et al., 2016, 2018; Vasek & Moore, 2012; Zeng, Li, & Stark, 2019)

oder Malware-Infektionen von Endnutzenden (Çetin et al., 2018). In den Studien wurde in der Regel eine Verbesserung im Vergleich zur Kontrollgruppe festgestellt.
Nachdem bei den Betroffenen ein Bewusstsein für das Problem geschaffen wurde, kann es sinnvoll sein, eine konkrete Unterstützung zur Lösung des Problems bereitzustellen. Hier wurden in der bisherigen Forschung Tools zur Überprüfung der Richtigkeit bereitgestellt. Obwohl solche Tools als hilfreich angesehen werden, sind die Forschungsergebnisse zur tatsächlichen Wirkung solcher Unterstützungstools gemischt (Li, Ho, et al., 2016; Zeng, Li, Stark, et al., 2019).

3.3 Studie 1 – Untersuchung der Behebung der Fehlkonfiguration von Google Analytics durch Webseitenbetreibende

3.3.1 Forschungsfragen

In Abschnitt 3.2.2, wurde gezeigt, dass die fehlende IP-Anonymisierung von Google Analytics viele Webseiten betrifft (12 %). Eine mögliche Erklärung könnte darin liegen, dass Webseitenbetreibenden nicht bewusst ist, dass dieses Privatsphärerisiko auf ihrer Webseite besteht. Bisher wurden in der Forschung nur Erkenntnisse zum Bewusstsein von Webseitenbetreibenden über Sicherheitslücken durch Fehlkonfigurationen auf ihren Webseiten berichtet und die Forschenden kommen zu unterschiedlichen Ergebnissen. Während in der Studie von Li et al. (2016) 46 % der Teilnehmenden angaben, dass sie sich der Schwachstelle auf ihrer Webseite bewusst sind, berichteten Durumeric et al. (2014), dass im Fall einer anderen Sicherheitslücke alle 17 Teilnehmenden sich des Problems bereits bewusst waren. Inwiefern sich Webseitenbetreibende über bestehende Privatsphärerisiken auf ihren Webseiten bewusst sind, ist noch nicht geklärt. Mit der Einführung der DSGVO wurde das Thema Datenschutz auf Webseiten auch medial häufig aufgegriffen. Deshalb stellt sich die Frage, ob fehlendes Bewusstsein hier auch eine Ursache ist und welche weiteren Ursachen es gibt, die ggf. auch das fehlende Bewusstsein erklären können. Deshalb soll mit der ersten Forschungsfrage Folgendes untersucht werden:

Forschungsfrage 1: Was sind aus Sicht der Webseitenbetreibenden die Ursachen für die fehlende IP-Anonymisierung von Google Analytics auf ihren Webseiten?

Forschungsfrage 2: (a) Wie gehen Webseitenbetreibende bei der Behebung der fehlenden IP-Anonymisierung von Google Analytics auf ihren Webseiten vor und (b) welche Hürden müssen sie dabei bewältigen?

Wie bereits im vorherigen Unterkapitel dargestellt, kann eine Maßnahme darin bestehen, die Webseitenbetreibenden über entsprechende Lücken zu benachrichtigen. Bisher wurde diese Maßnahme im Kontext von Sicherheitslücken erforscht, was zu gemischten Ergebnissen geführt hat. Unklar ist, wie diese Maßnahme im Kontext von Privatsphärerisiken angepasst werden kann, um effektiv zu sein. Deshalb stellt sich die folgende Frage:

Forschungsfrage 3: Wie sollten Benachrichtigungen gestaltet sein, die Webseitenbetreibende effektiv dabei unterstützen, die fehlende IP-Anonymisierung von Google Analytics zu beheben?

Zur Beantwortung der beschriebenen Forschungsfragen wurden drei Untersuchungen durchgeführt. (1) Feldexperiment: Im ersten Schritt wurden Webseitenbetreibende, deren Webseite keine IP-Anonymisierung von Google Analytics aufwies, im Rahmen eines Feldexperiments über das Privatsphärerisiko informiert. (2) Umfrage: Anschließend wurden die Teilnehmenden des Feldexperiments dazu eingeladen, an einer Umfrage teilzunehmen. (3) Rückmeldungen: Die Teilnehmenden des Feldexperiments hatten die Möglichkeit, auf die Benachrichtigung zu reagieren. Diese Rückmeldungen wurden quantitativ und qualitativ analysiert. Im Folgenden werden die Methoden der drei Untersuchungen beschrieben.

3.3.2 Methode der Studie 1a – Feldexperiment

Um einen ersten Kontakt zu Webseitenbetreibenden herzustellen, wurden Webseitenbetreibende, deren Webseiten eine fehlende IP-Anonymisierung aufwies, von den Studienorganisator:innen darüber informiert. Dies geschah im Rahmen eines Feldexperiments, in dem die Webseitenbetreibenden (Teilnehmenden) je nach Gruppenzugehörigkeit eine E-Mail oder einen Brief erhielten, bei denen der Absender sowie der Inhalt variiert wurden.

Sammlung der Kontaktdaten und Identifikation der fehlerhaften Webseiten

Wie ausführlich nachzulesen bei (Maass et al., 2021), wurden zunächst 1.3 Mio. Webseiten mit der Endung *.de* auf ein Fehlen der IP-Anonymisierung von Google Analytics überprüft. Dazu wurde ein zuvor entwickeltes Prüftool eingesetzt, das automatisch den Code der 1.3 Mio. Webseiten dahingehend prüfte, ob die IP-Anonymisierung von Google Analytics implementiert war. Diese Analysen ergaben, dass bei 12.8 % der geprüften Webseiten die IP-Anonymisierung nicht oder nicht korrekt implementiert war. Von den nicht konformen Toplisten-Seiten wurden 5000 Webseiten zufällig ausgewählt. Jede Webseite wurde von drei Forschenden besucht, die jeweils unabhängig voneinander die Post- und E-Mail-Adressen aus dem Impressum der Webseite erfassten. Nach der Zusammenlegung von Webseiten, die sich im gemeinsamen Besitz eines Webseitenbetreibenden befanden, enthielt der finale Datensatz 4754 Webseiten, die zu 4594 verschiedenen Webseitenbetreibenden gehörten. Diese Webseiten wurden während des Untersuchungszeitraums viermal täglich automatisch mithilfe des Prüftools gescannt.

Experimentelles Design

Bei dieser Studie handelt es sich um ein Feldexperiment mit einem Drei-Faktor-Zwischen-Subjekt-Design. Die Faktoren waren das Kontaktmedium (zwei Bedingungen: Brief vs. E-Mail), der Absender (drei Bedingungen: Privatperson vs. Forschungsgruppe Informatik vs. Forschungsgruppe Rechtswissenschaften) und das inhaltliche Argument (drei Bedingungen: Schadet der Privatsphäre vs. GDPR-Verstoß vs. GDPR-Verstoß + potenzielle Strafe). Als abhängige Variable wurde gemessen, ob die Webseitenbetreibenden die IP-Anonymisierung implementiert hatten.

Faktoren. Insgesamt wurden drei Faktoren variiert. Beim Faktor *Kontaktmedium* wurde zwischen E-Mail und Brief variiert. Beim Faktor *Absender* wurde zwischen drei verschiedenen Absendern variiert: eine Privatperson, eine Forschungsgruppe der Informatik der TU Darmstadt sowie eine Forschungsgruppe

aus den Rechtwissenschaften der Goethe-Universität Frankfurt. Der dritte variierte Faktor war der Inhalt bzw. das *Argument*, das in der Benachrichtigung verwendet wurde. Hier gab es drei Varianten: Beim Argument ‚Privatsphäre' wurde argumentiert, dass die Fehlkonfiguration die Privatsphäre der Nutzenden beeinträchtigt, ohne rechtlichen Konsequenzen zu erwähnen. Beim Argument ‚DSGVO' wurde den Teilnehmenden mitgeteilt, dass die Fehlkonfiguration gegen die DSGVO verstößt. Bei dem Argument ‚DSGVO + Strafe' wurde ebenfalls auf den DSGVO-Verstoß verwiesen und zusätzlich erwähnt, dass damit eine Geldbuße von bis zu 4 % des Jahresumsatzes einhergehen kann.

Erneute Benachrichtigungen. Es wurden bis zu drei Benachrichtigungen an alle Teilnehmenden verschickt: eine erste Benachrichtigung, gefolgt von einer Erinnerung einen Monat später (falls das Problem noch nicht behoben war) und eine abschließende Aufklärung an alle Teilnehmende einen Monat später, um sie darüber zu informieren, dass sie an einer Studie teilgenommen hatten, und sie aufzufordern, an einer Umfrage teilzunehmen, sowie ihnen die Möglichkeit zum Opt-out zu geben. Alle Benachrichtigungen wurden in deutscher Sprache verfasst und enthielten einen Verweis auf das Prüftool.

Prüftool. In den Benachrichtigungen wurden die Teilnehmenden auch auf ein online zur Verfügung gestelltes Prüftool hingewiesen. Damit hatten sie die Möglichkeit, selbst zu prüfen, ob die IP-Anonymisierung von Google Analytics korrekt auf ihrer Webseite umgesetzt war.

Sammlung und Auswertung der Daten

Die Analysen wurden auf Basis der Daten, die mithilfe des automatischen Prüftools im Juli und August 2019 gesammelt wurden, durchgeführt. Das Prüftool hatte jede Webseite viermal pro Tag besucht und mit einem Scan geprüft, ob die IP-Anonymisierung korrekt durchgeführt wurde. Für detaillierte Informationen zur Datensammlung und -auswertung siehe Maas et al. (Maass et al., 2021).

3.3.3 Methode der Studie 1b – Umfrage

Um die Perspektive der Webseitenbetreibenden zu untersuchen, wurden alle zuvor im Feldexperiment kontaktieren Webseitenbetreibenden im Rahmen der Aufklärung zur Teilnahme an einer Umfrage eingeladen.

Ablauf

Die Umfrage wurde auf der Plattform Soscisurvey gehostet (Leiner, 2014). Nachdem die Teilnehmenden der Datenschutzerklärung zugestimmt hatten, wurden sie zu ihrer Beurteilung der Benachrichtigung befragt, die sie im Rahmen des Feldexperiments erhalten hatten. Weiterhin erhielten sie Fragen zum Umgang mit dem Problem und zum Prüftool. Zuletzt wurden die Teilnehmenden gefragt, ob und in welcher Form sie zukünftig über Privatsphärerisiken auf ihrer Webseite informiert werden möchten. Die Fragen waren auf die Gruppe der Teilnehmenden zugeschnitten (Medium, Absender, Framing sowie Problemstatus). Die Umfrage umfasste zwischen 17 und 21 Fragen, je nach Gruppenzugehörigkeit der Teilnehmenden im Feldexperiment und deren Antworten. Eine Version des Fragebogens findet sich in Anhang A.

Teilnehmende

Insgesamt nahmen 561 Personen an der Umfrage teil. Davon wurden 84 aus der Auswertung ausgeschlossen, da diese entweder der informierten Zustimmung nicht zugestimmt hatten (N = 19) oder weniger als 50 % der Fragen beantwortet hatten (N = 65). 226 der 477 Teilnehmenden füllten den Fragebogen vollständig aus. Es nahmen mehr Personen an der Umfrage teil, die zuvor einen Brief (67.9 %) erhalten hatten, als solche, die eine E-Mail empfangen hatten. Die Gruppenzugehörigkeiten ‚Argument' und ‚Absender' waren etwa gleich verteilt. Die Unternehmen/Organisationen der Befragten hatten zwischen 0 und 1 1500 Mitarbeitende (MD = 5; M = 146.34; SD = 748.02). 28.5 % der Befragten gaben an, dass ihr Unternehmen/ihre Organisation keine oder einen Mitarbeitenden hat (22.9 %). Die Teilnehmendenzahl bei den verschiedenen Fragen kann variieren, da die Umfrage außer der informierten Zustimmung keine obligatorischen Fragen enthielt und einige Fragen nur für bestimmte Gruppen oder Folgefragen bestimmt waren.

Auswertung

Die Antworten wurden mit Analysesoftware SPSS (IBM, 2020) ausgewertet. Offene Antworten wurden mit thematischer Inhaltsanalyse nach Braun und Clarke (2006) analysiert. Zur Unterstützung wurde die Software MAXQDA (VERBI Software, Berlin, Germany, 2020) verwendet.

3.3.4 Methode der Studie 1c – Analyse der Rückmeldungen

Die Benachrichtigungen aus dem Feldexperiment enthielten Kontaktdaten der Studienorganisator:innen, die es den Webseitenbetreibenden ermöglichte, Kontakt aufzunehmen. Von dieser Möglichkeit machten eine Reihe der Teilnehmenden Gebrauch. Diese Kommunikation wurde von den Studienorganisator:innen dokumentiert und im Rahmen einer quantitativen sowie qualitativen Analyse ausgewertet.

Daten

Insgesamt enthält der Datensatz 1882 Dokumente. Davon sind 452 Bounces oder Auto-Replies und 387 ausgehende Nachrichten der Studienorganisator:innen. Die verbleibenden 1043 Dokumente des Datensatzes sind Rückmeldungen der Webseitenbetreibenden, die in die Analyse einbezogen wurden. Diese Antworten unterteilen sich in 41 Briefe, 946 E-Mails und 56 Telefonprotokolle.

Auswertung

Die Rückmeldungen der Webseitenbetreibenden wurden im ersten Schritt quantitativ und im zweiten Schritt qualitativ ausgewertet. Das genaue Vorgehen wird im Folgenden beschrieben.

Quantitative Analyse der Rückmeldungen. Um einen ersten Überblick über die Rückmeldungen der Webseitenbetreibenden zu bekommen, wurde zunächst eine quantitative Inhaltsanalyse durchgeführt, die sich an dem Verfahren orientiert, das von Döring und Bortz (2016) vorgeschlagen wurde. Dazu wurde zunächst induktiv ein Kategoriensystem sowie ein Codebook entwickelt. Dazu machten sich zunächst zwei Forschende durch mehrfaches Lesen mit den Daten vertraut und entwickelten unabhängig voneinander Kategorien, die sie im Anschluss diskutierten und anpassten. Ein Teil des Materials wurde

von einem weiteren Forschenden unabhängig kodiert und das Kategoriensystem anschließend angepasst. Im weiteren Verlauf wurde das gesamte Material von zwei Forschenden unabhängig voneinander codiert. Die Codierung wurde im Anschluss verglichen, Unterschiede wurden diskutiert und Codierungen angepasst. Ziel der quantitativen Analyse war es primär, einen Überblick über die Daten zu gewinnen. Die Themen geben einen Überblick darüber, welche Themen in den Daten enthalten sind. Diese erste Analyse erlaubt jedoch keine tiefgehenden Einblicke über die Gründe, Wahrnehmungen und die Motivation der Webseitenbetreibenden. Einige Kategorien sind selbsterklärend (Dankeschön), andere werfen tiefergehende Fragen auf (z. B. Beschreibung des Problems). Um hier ein besseres Verständnis zu entwickeln, wurde weiterhin eine qualitative Inhaltsanalyse durchgeführt.

Qualitative Analyse der Rückmeldungen. Für die qualitative Analyse der Rückmeldungen der Webseitenbetreibenden wurde eine thematische Analyse durchgeführt, die es erlaubt, Muster und Themen in qualitativen Daten zu erkennen (Braun & Clarke, 2006). Es wurde den von Braun und Clarke (2006) vorgeschlagenen Schritten gefolgt und MAXQDA als Softwareunterstützung verwendet (VERBI Software, Berlin, Germany, 2020). Dazu machte sich die Autorin dieser Arbeit zunächst durch mehrfaches Lesen der Dokumente mit den Daten vertraut. Im zweiten Schritt entwickelte sie ein Codebuch, indem sie die Dokumente auf Satzebene kodierte. Anschließend traf sich die Autorin mit einem zweiten Autor, um das Codebuch zu besprechen und zu verfeinern. Beide Autoren benutzten dieses Codebuch, um alle Dokumente unabhängig voneinander zu kodieren. In Anlehnung an Clarke und Brauns (Braun & Clarke, 2006) Verständnis der thematischen Analyse wurde keine Inter-Rater-Reliabilität berechnet. Um eine hohe Qualität der Analyse zu gewährleisten, kamen die Autoren im nächsten Schritt zusammen, um Unklarheiten zu diskutieren und sich auf eine endgültige Kodierung zu einigen. Danach gruppierten die Autoren die Daten in vier Themen: (1) Hintergründe zu den Webseitenbetreibenden, (2) Gründe für die fehlende IP-Anonymisierung, (3) Vorgehen der Webseitenbetreibenden bei der Behebung der fehlenden IP-Anonymisierung und (4) Hürden bei der Umsetzung der IP-Anonymisierung. Für Ergebnisse zu diesen Themen siehe Unterkapitel 3.3.9 sowie Abbildung 5.

Ableitung von Personas. Die Ergebnisse der thematischen Analyse deuten darauf hin, dass Webseitenbetreibende Webseiten in unterschiedlichen Kontexten und unter verschiedensten Umständen betreiben. Daraus ergeben sich spezifische Herausforderungen und Bedürfnisse für die Webseitenbetreibenden. Um diese Diversität abzubilden, wurde auf Grundlage der Ergebnisse der thematischen Analyse Beispiel-Personas entwickelt, die verschiedene Webseitenbetreibende aus den Daten repräsentieren. Personas, wie sie in dieser Arbeit verwendet werden, sind abstrakte Repräsentationen von Nutzenden (in diesem Fall von Webseitenbetreibenden) (Pruitt & Grudin, 2003). Sie sind eine weitverbreitete Technik des Interaktionsdesigns, um die Entwicklung von Produkten zu unterstützen (Guo et al., 2011; Pruitt & Grudin, 2003). Für die Entwicklung der Personas für die vorliegende Arbeit wurde der Ansatz von Pruitt und Grudin (2003) gewählt. In einem Workshop wurden die Themen und Kategorien der thematischen Analyse auf Post-its notiert, die dann von zwei Forschenden geclustert wurden. Ziel des Clusterings war es, Personas zu finden, die die Vielfalt der Hintergründe von Webseitenbetreibenden und ihre spezifischen Herausforderungen repräsentieren.

Einerseits sollten die Personas so unterschiedlich wie möglich sein, andererseits sollten sie die Bandbreite der in den Daten vertretenen Fälle so gut wie möglich abdecken. Pruitt und Grudin (2003) empfehlen, drei bis sechs Personas zu entwickeln, um die Anzahl der Charaktere überschaubar zu halten. In dem vorliegenden Clustering-Prozess kamen die Forschenden zu dem Schluss, dass drei Personas die in den Daten repräsentierten Webseitenbetreibenden am besten widerspiegeln. Diese drei Beispiel-Personas entsprechen genau einigen der Webseitenbetreibenden aus dem Datensatz; auf andere Webseitenbetreibende aus dem Datensatz treffen nur einzelne Aspekte einer der Personas zu. Bei der Entwicklung der Personas war es den Forschenden wichtig, zu beachten, dass die Datengrundlage kein vollständiges Bild der Realität darstellt, da vermutlich nur einige Webseitenbetreibende bestimmte Detailfragen beantworten. Es ist beispielsweise anzunehmen, dass Webseitenbetreibende, die in großen Unternehmen arbeiten, tendenziell weniger Informationen preisgeben. Dies bedeutet jedoch nicht, dass es diese Fälle nicht gibt. Um zu vermeiden, dass durch scheinbare Objektivität ein verzerrtes Bild entsteht, wurde bewusst auf die Quantifizierung von Clustereigenschaften verzichtet.

3.3.5 Ethische Überlegungen

Die Benachrichtigung der Webseitenbetreibenden über die Fehlkonfiguration auf ihrer Webseite hatte auch zum Ziel, diese vor eventuell kostspieligen Abmahnungen zu schützen. Trotzdem ist zu beachten, dass die Bearbeitung der Benachrichtigung die meisten Webseitenbetreibenden Zeit und in einigen Fällen auch Geld kosten konnte. Insbesondere bei Teilnehmenden, die die Benachrichtigung mit dem Verweis auf mögliche Geldstrafen erhalten hatten, konnte diese potenziell Stress auslösen. Dennoch wurde das Risiko von den Studienorganisator:innen für vertretbar eingeschätzt, da die Benachrichtigung keine Forderungen oder Drohungen enthielt und die vorgeschlagenen Änderungen die Webseitenbetreibenden vor einer Haftung schützen. Die Kontaktadressen wurden aus dem für diesen Zweck vorgesehenen Impressum der Webseite erhoben. Während aus den ersten beiden Benachrichtigungen nicht hervorging, dass sie als Teil einer Studie verschickt wurden, um Priming-Effekte zu vermeiden, wurden alle kontaktierten Webseitenbetreibenden in einer weiteren Benachrichtigung darüber informiert, dass sie Teil einer Studie waren, zusammen mit der Einladung, an der Umfrage teilzunehmen. Im Rahmen der Aufklärung wurden alle ausdrücklich darauf hingewiesen, dass die Kommunikation zu Forschungszwecken analysiert werden kann und dass die Antworten der Webseitenbetreibenden in Publikationen zitiert werden können, ohne die Identität der Organisation, des Unternehmens oder der Person preiszugeben. In diesem Zuge wurde allen Webseitenbetreibenden angeboten, aus der Studie herausgenommen zu werden, was vier Webseitenbetreibende in Anspruch nahmen. Die Mitglieder der Kontrollgruppe wurden vor der Veröffentlichung dieser Arbeit informiert.
Ein positives Votum von der Ethikkommission der TU Darmstadt liegt vor. Im Ethikantrag wird neben anderen für die Studie relevanten Details erwähnt, dass alle während der Studie erhaltenen Rückmeldungen der Webseitenbetreibenden gespeichert und analysiert werden. Darüber hinaus ist festgelegt, dass der Datensatz nur von bestimmten Forschenden eingesehen werden darf und nicht öffentlich zugänglich ist. Um das Risiko einer unbeabsichtigten Offenlegung der Identität zu minimieren, wurde darauf verzichtet, Hintergrundinformationen über einzelne Webseitenbetreibende zu geben. Außerdem werden Rückmeldungen nur auszugsweise zitiert, sodass keine Rückschlüsse auf den Absender oder die Organisation gezogen werden können.

3.3.6 Ergebnisse der Studie 1a – Feldexperiment

An dieser Stelle soll nur kurz auf die Ergebnisse des Feldexperiments eingegangen werden, die ausführlich bei Maass et al. (2021) nachzulesen sind. Die Ergebnisse zeigen, dass das Problem der fehlenden IP-Anonymisierung besonders häufig gelöst wurde, wenn dieses als Rechtsverstoß formuliert wurde, vor allem dann, wenn die Benachrichtigung in Form eines Schreibens einer juristischen Forschungsgruppe versandt wurde. Dabei wurde das Problem in 76.3 % der Fälle gelöst, verglichen mit 33.9 % bei Benachrichtigungen per E-Mail, die von Informatikforschenden versandt wurden und die vor einem Datenschutzproblem warnten. Über alle Gruppen hinweg behoben 56.6 % der benachrichtigten Webseitenbetreibenden das Problem, verglichen mit 9.2 % in der Kontrollgruppe.

3.3.7 Ergebnisse der Studie 1b – Umfrage

Um die Perspektive der teilnehmenden Webseitenbetreibenden auf die Benachrichtigung sowie ihr Vorgehen beim Beheben der Fehlkonfiguration zu erfassen, wurde eine Umfrage durchgeführt. Der entsprechende Fragebogen findet sich in Anhang A. Insgesamt wurden die Antworten von 477 teilnehmenden Webseitenbetreibenden in die Auswertung aufgenommen. Die Teilnehmendenanzahl kann bei den verschiedenen Fragen variieren, da die Umfrage keine obligatorischen Fragen enthielt und einige Fragen Folgefragen waren oder nur für bestimmte Gruppen angezeigt wurden.

Problembewusstsein der Webseitenbetreibenden

Bevor sie benachrichtigt wurden, wussten 371 von 461 (80.5 %) der Webseitenbetreibenden, dass sie Google Analytics auf ihrer Webseite verwenden. 272 von 462 (58.9 %) hatten von der IP-Anonymisierungsfunktion gehört, bevor sie benachrichtigt wurden. 58 von 458 (12.7 %) waren sich der fehlenden IP-Anonymisierung bewusst, bevor sie benachrichtigt wurden. Webseitenbetreibende, deren IP-Anonymisierung noch nicht behoben wurde, wurden gefragt, warum sie das Problem bisher nicht gelöst hatten ($N = 54$; Mehrfachnennungen möglich). 22 Webseitenbetreibende gaben an, dass das Problem unbekannt sei, 20 gaben an, dass sie nicht wüssten, wie das Problem zu lösen sei. Einige Webseitenbetreibende gaben an, das Problem habe keine Priorität (12 Antworten), sie fänden keine Zeit, sich mit dem Problem zu befassen (10 Antworten), oder die Benachrichtigung erscheine ihnen nicht vertrauenswürdig (6 Antworten).

Vertrauen in die Benachrichtigung

In der Umfrage stimmten 316 von 460 (68.7 %) Webseitenbetreibende (eher) der Aussage zu, dass die Meldung einen vertrauenswürdigen Eindruck machte. Die Benachrichtigung wurde von den Teilnehmenden aus der Versuchsgruppe ‚Absender: Forschungsgruppe Rechtswissenschaften' als am vertrauenswürdigsten und von denen aus der Gruppe ‚Absender: Privatperson' als am wenigsten vertrauenswürdig empfunden. Bei den beiden anderen Faktoren sind die Unterschiede weniger stark ausgeprägt. Mit zwei offenen Fragen wurden die Webseitenbetreibenden gefragt, welche Faktoren dazu geführt haben, der Benachrichtigung zu vertrauen bzw. zu misstrauen. Insgesamt beantworteten 377 Teilnehmende die Vertrauensfrage und 252 die Misstrauensfrage (Mehrfachnennungen möglich). Die

daraus resultierenden vertrauensbezogenen Faktoren lassen sich in formale, inhaltliche und überprüfbare Aspekte unterteilen.

Formale Vertrauensfaktoren

Unter den formalen Faktoren scheint der Absender der Benachrichtigung von besonderer Bedeutung zu sein, da dieser insgesamt 348-mal genannt wurde (Mehrfachnennungen möglich). Insbesondere der Bezug zur Universität, der von 174 von 377 (46.1 %) Teilnehmenden genannt wurde, scheint relevant zu sein. Die Möglichkeit, den Absender zu kontaktieren, ist ebenfalls bedeutsam und wurde von 44 von 377 (11.7 %) Teilnehmenden genannt. Ein weiterer formaler Aspekt ist der gute Sprachgebrauch, der von 63 von 377 (16.1 %) Teilnehmenden erwähnt wurde. Zum Beispiel wurde genannt, dass die Mitteilung „*gut formuliert*“ (P892) war und „*keine Rechtschreibfehler*“ (P1181) enthielt. Von den 259 Teilnehmenden, die einen Brief erhalten hatten, bewerteten 25 (9.6 %) die Tatsache, dass es sich um einen „*echten Brief*“ handelte, als vertrauensfördernd. Interessanterweise wurden sogar kleine Aspekte wie das Logo oder der Briefkopf (13.0 %; 49 von 377 Befragten) und die Unterschrift (3.1 %; 12 von 377 Befragten) von einigen als vertrauensfördernd angesehen, was zeigt, dass selbst scheinbar kleine Gestaltungsentscheidungen Auswirkungen auf die wahrgenommene Vertrauenswürdigkeit haben können.

Die gleichen Faktoren führten jedoch bei anderen Teilnehmenden zu Misstrauen: 41 von 252 (16.3 %) Teilnehmende nannten eine schlechte Formulierung und 46 (18.2 %) das Layout als Grund für das Misstrauen gegenüber der Benachrichtigung. 12 (4.8 %) Teilnehmende gaben an, dass der Erhalt eines Briefes das Vertrauen schwächt, wobei sich P1136 fragte: „*Wer macht sich die Mühe, meine Webseite zu untersuchen?*“

Inhaltsbezogene Vertrauensfaktoren

Neben den formalen Aspekten gab es auch verschiedene inhaltliche Aspekte, die das Vertrauen in die Benachrichtigung förderten. 94 von 377 (24.3 %) Teilnehmende gaben die sachliche Richtigkeit und die ausführliche Erläuterung als vertrauensfördernd an und 56 von 377 (14.8 %) Teilnehmenden erwähnten dasselbe bezüglich des Prüftools. Für mehrere Teilnehmende war die zugrundeliegende Motivation des Absenders relevant. 76 von 377 (20.2 %) Teilnehmenden hielten es für vertrauensfördernd, dass keine finanziellen Forderungen oder Gewinnabsichten des Absenders vorlagen und die Benachrichtigung keine Drohung enthielt. Im Gegensatz dazu gaben 38 von 252 (15.1 %) Teilnehmenden an, dass die Motivation des Absenders nicht klar war, und 64 (25.4 %) Teilnehmende empfanden die Benachrichtigung als Bedrohung, Spam oder Werbung.

Verifizierbarkeit erhöht das Vertrauen

Während 11 von 252 (4.4 %) Teilnehmenden angaben, dass sie Informationen von unbekannten Absendern generell nicht vertrauen, wurde in 119 von 377 (31.6 %) Antworten die Möglichkeit der Überprüfung als vertrauensfördernd eingestuft. Dazu gehört, dass der Absender überprüft werden kann, was einige taten, indem sie die angegebene Nummer anriefen, um sicherzugehen, dass der Brief von der angegebenen Person gesendet wurde. Für andere bedeutet dies, dass sie den Sachverhalt durch eigene Nachforschungen oder mithilfe von Expert:innen oder Bekannten verifizieren.

Problembehebung und Unterstützung

Mit den Benachrichtigungen sollten die Webseitenbetreibenden unterstützt werden. Deshalb wurde in der Umfrage auch gefragt, inwieweit die Erklärung in der Benachrichtigung und das Prüftool hilfreich waren und ob die Teilnehmenden zukünftig Benachrichtigungen erhalten möchten.

Problembehebung

339 von 437 (77.6 %) Teilnehmenden gaben an, dass sie das Problem der fehlenden IP-Anonymisierung anhand der Benachrichtigung nachvollziehen konnten. Viele Teilnehmende, die das Problem behoben hatten, gaben an, dass sie dies ohne Hilfe getan hatten (37.8 %), während 30.9 % berichteten, dass sie ihren externen Dienstleister gebeten hatten, das Problem zu lösen. 13.0 % leiteten das Problem an Kolleg:innen im Unternehmen weiter und 10.8 % lösten das Problem selbst, nachdem sie Hilfe erhalten hatten (andere: 7.5 %, $N = 362$).

Nützlichkeit des Prüftools

Das bereitgestellte Prüftool wurde von der Mehrheit der Teilnehmenden als (sehr) hilfreich bewertet (87.2 %; 266 von 305 Teilnehmenden). Dies steht im Einklang mit der Tatsache, dass das Instrument häufig als vertrauensbildender Faktor genannt wurde. Weitere 51 Teilnehmende gaben an, das Instrument nicht zu kennen, und 86 Teilnehmende gaben an, es nicht verwendet zu haben.

Zukünftige Benachrichtigungen

Die meisten Teilnehmenden (88.4 %) wünschten sich künftige Benachrichtigungen über Datenschutzprobleme auf ihrer Webseite ($N = 448$). Die Mehrheit (84.8 %) zog es vor, per E-Mail benachrichtigt zu werden. 28.2 % bevorzugten einen Brief, 3.7 % einen Blogbeitrag, 3.2 % einen Anruf (1.7 % bevorzugten etwas anderes, z. B. ein Serviceportal; $N = 401$; Mehrfachnennungen möglich). 30.5 % gaben an, dass sie bereit wären, für solche Benachrichtigungen zu bezahlen ($N = 383$).

3.3.8 Ergebnisse der Studie 1c – quantitative Analyse der Rückmeldungen

Die Ergebnisse der Umfrage erlauben bereits einen ersten Einblick, wie die Benachrichtigung von den teilnehmenden Webseitenbetreibenden wahrgenommen wurde, wie sie bei der Problemlösung vorgegangen sind und wie sie Unterstützungsangebote einschätzen. Im Rahmen des Feldexperiments erhielten die Studienorganisator:innen insgesamt 1043 Rückmeldungen (R) von Webseitenbetreibenden auf die Benachrichtigung. Um einen ersten Überblick zu bekommen, wurden die Rückmeldungen mittels einer quantitativen Analyse ausgewertet. Daraus entstanden vier Themen, die in Tabelle 1 aufzeigt und im Folgenden vorgestellt werden.

Tabelle 1. Überblick über die Ergebnisse der quantitativen Analyse.

Kategorie	Anzahl der Teilnehmenden, deren Rückmeldung der Kategorie zuzuordnen ist
Danksagung	260
Unterstützungsanfrage	204
Verifikation der Absender	32
Beschwerden	19

Verifikation der Absender

Insgesamt meldeten sich 32 Teilnehmende zurück, um die Echtheit der Nachricht zu überprüfen. Oft wählten sie eine andere Kontaktadresse, indem sie online nach dem Absender suchten und ihn über seine persönliche Adresse auf der Homepage der Universität kontaktierten oder Telefonnummern anriefen, die sie online oder im Brief gefunden hatten. Zwei Teilnehmende kontaktierten den Absender über Twitter. Der Ton der Nachrichten war oft freundlich und neugierig, manchmal aber auch feindselig, indem sie böse Absichten unterstellten oder sich darüber beschwerten, dass die Nachricht schwer zu verstehen sei. Die meisten konnten mit einer Covergeschichte beschwichtigt werden, ohne zu erwähnen, dass sie Teil einer Studie waren.

Unterstützungsanfragen

204 Empfänger (26.7 %) stellten Fragen zur Behebung der Fehlkonfiguration, baten um eine Überprüfung ihrer Lösungsversuche oder boten den Studienorganisator:innen Anmeldedaten für den Webserver an, damit diese das Problem für sie beheben können: „*wenn das für dich wichtig ist*“ (R347). Die Studienorganisator:innen gaben Anweisungen zur Behebung der Fehlkonfiguration, ergriffen aber keine Maßnahmen zur direkten Behebung des Problems.

Beschwerden

Beschwerden über die Benachrichtigung kamen von 19 Teilnehmenden. Während einige lediglich unzufrieden mit der unaufgeforderten Nachricht waren oder zum Ausdruck brachten, dass der Ton der Nachricht für sie stressig war, gingen andere weiter und drohten mit rechtlichen Schritten, versuchten, den Studienorganisator:innen die Zeit in Rechnung zu stellen, die sie für unsere Benachrichtigung aufgewendet hatten, oder wandten sich direkt an den Kanzler einer der beteiligten Universitäten, um sich zu beschweren.

Danksagung

Schließlich bedankten sich 260 Teilnehmende für die Benachrichtigung. Teilweise enthielten die Rückmeldungen auch Angebote für Zahlungen, Rabatte oder Geschenke. Einige Empfänger schickten unaufgefordert Pakete mit Geschenken, die von kostenlosen Zeitschriften und Tassen bis hin zu einer Spende an eine der beteiligten Universitäten reichten. Wann immer möglich, wurden die angebotenen Geschenke oder Zahlungen abgelehnt.

3.3.9 Ergebnisse der Studie 1c – qualitative Analyse der Rückmeldungen

Die thematische Analyse der Rückmeldungen der Webseitenbetreibenden auf die Benachrichtigungen aus dem Feldexperiment ergab vier Themen: die Umstände der Webseitenbetreibenden, die Gründe für die Fehlkonfiguration von Google Analytics, Lösungsansätze der Teilnehmenden bei der Behebung der Fehlkonfiguration und die Herausforderungen, auf die die Webseitenbetreibenden gestoßen sind. Einen Überblick über die Themen bietet Abbildung 5. Im Folgenden wird auch aus den Rückmeldungen der Webseitenbetreibenden zitiert, wobei die Nummerierung hier bis 1882 geht, da die fortlaufende Nummerierung aus dem Originaldatensatz übernommen wurde. Es wurde bewusst auf die Angabe exakter Zahlen verzichtet, um den Eindruck der Verallgemeinerbarkeit zu vermeiden. Es wurden nur die tatsächlich in den Rückmeldungen enthaltenen Informationen kodiert. Daher fehlen oft Hintergrundinformationen, z. B. in welchem Kontext eine Webseite erstellt wurde. Die Informationen aus den Rückmeldungen zeichnen wahrscheinlich ein verzerrtes Bild von den Lebensumständen der Webseitenbetreibenden, da davon auszugehen ist, dass sich z. B. vor allem Webseitenbetreibende mit geringeren technischen Kenntnissen an die Studienorganisator:innen gewandt haben, um Rat zu suchen. Folglich spiegeln die Daten wahrscheinlich nicht die allgemeine Population der Webseitenbetreibenden wider.

Wie sehen die Umstände der antwortenden Webseitenbetreibenden aus?
- Kontext der Webseitenbetreibenden
- Beteiligung der Webseitenbetreibenden an der Entwicklung und Wartung der Webseite
- Privatsphäremotivation der Webseitenbetreibenden

Warum haben Webseitenbetreibende die IP-Anonymisierung bisher nicht vorgenommen?
- Fehlerhafte technische Umsetzung
- Mangelndes Bewusstsein für Privatsphäre
- Unklare Zuständigkeit
- Vertrauen auf die Urteile anderer
- Bewusst unterlassene Wartung

Wie sind die Webseitenbetreibenden nach der Benachrichtigung mit der fehlenden IP-Anonymisierung umgegangen?
- Webseitenbetreibende implementieren die IP-Anonymisierung selbstständig
- Webseitenbetreibende implementieren die IP-Anonymisierung mit Unterstützung
- Webseitenbetreibende delegieren die IP-Anonymisierung
- Webseitenbetreibende implementieren die IP-Anonymisierung nicht

Welchen Hürden müssen Webseitenbetreibende bei der Implementierung der IP-Anonymisierung überwinden?
- Mangel an Ressourcen
- Mangel an technischem Wissen
- Probleme mit dem Code
- Abhängigkeiten und zähe Prozesse in Organisationen

Abbildung 5. Übersicht über die Themen, die das Ergebnis der thematischen Analyse sind.

Wie sehen die Umstände der antwortenden Webseitenbetreibenden aus?

Zunächst sollen die Umstände der im Datensatz enthaltenen Webseitenbetreibenden beleuchtet werden. Diese Informationen bilden die Grundlage, um zu verstehen, welche Hürden diese bei der Behebung von Privatsphärerisiken auf ihren Webseiten, speziell der fehlenden IP-Anonymisierung von Google Analytics, überwinden müssen und welche Ressourcen ihnen dafür zur Verfügung stehen.

Kontext der Webseitenbetreibenden

Die meisten Webseitenbetreibenden betreiben ihre Webseite im beruflichen Kontext, entweder als Angestellte in einem größeren Unternehmen oder als Selbstständige. Dennoch gab eine beträchtliche Anzahl an Teilnehmenden an, dass sie die Webseite in einem privaten Kontext betreiben. Zu den Gründen für eine Webseite im privaten Kontext gehören das Engagement in Vereinen (z. B. im Kultur- oder Sportbereich) und die Information der Öffentlichkeit über ein bestimmtes Anliegen (z. B. ein bestimmtes Tier). Private Webseitenbetreibende sind oft sehr motiviert, die Webseite einzurichten und zu pflegen, verfügen aber nicht unbedingt über die erforderlichen technischen Kenntnisse. Während Mitarbeitende in großen Unternehmen in der Regel auf die Unterstützung von Fachleuten wie Webentwicklern, Systemadministratoren und Anwälten zurückgreifen können, werden die Webseiten von Mitarbeitenden in kleineren Unternehmen oft von Dritten verwaltet, meist aus Mangel an Zeit und Wissen. Die bessere Unterstützung in größeren Unternehmen geht jedoch mit einem potenziellen Mangel an Flexibilität einher, da sich die Webseitenbetreibenden hier häufiger mit mehr Personen abstimmen müssen. Webseitenbetreibende, die eine Webseite im Rahmen einer selbständigen Tätigkeit betreiben, stoßen auf verschiedene Schwierigkeiten. Sie sind zwar darauf angewiesen, die Webseite zu betreiben, um ihre Dienstleistungen oder Produkte zu bewerben und zu verkaufen, verfügen aber nicht unbedingt über die notwendigen technischen Kenntnisse. Darüber hinaus müssen sie die Pflege der Webseite in ihr meist schon knappes Zeitbudget einpassen, wo diese manchmal hinter vermeintlich dringenderen Aufgaben zurücktritt.

Beteiligung der Webseitenbetreibenden an der Entwicklung und Wartung der Webseite

Obwohl sie die rechtliche Verantwortung für die Webseite tragen, gaben die meisten Teilnehmenden an, nicht aktiv an der Entwicklung und Wartung ihrer Webseite beteiligt zu sein. Während private Webseitenbetreibende ihre Webseite oft selbst entwickeln und pflegen, lagern die Teilnehmenden dies bei Webseiten, die sie im beruflichen Kontext besitzen, häufig aus: Im Falle von Angestellten hat die Organisation in der Regel eine externe Agentur mit dieser Aufgabe betraut. Selbstständige Webseitenbetreibende, die in der Regel über weniger finanzielle Mittel verfügen, nutzen zu diesem Zweck eher die kostenlosen Dienste von IT-versierten Personen aus ihrem privaten Umfeld, z. B. von ihren Enkelkindern. Die meisten Webseitenbetreibenden, die nicht an der Entwicklung und Wartung der Webseite beteiligt sind, sind sich jedoch weder möglicher Datenschutzprobleme bewusst noch fühlen sie sich für deren Lösung verantwortlich. Selbst bereitwillige Webseitenbetreibende scheitern oft daran, dass sie nicht wissen, wie sie Änderungen an der Webseite vornehmen können. In Fällen, in denen nur die Entwicklung der Webseite ausgelagert oder die Webseite von einem Vorgänger übernommen wurde, berichteten einige Teilnehmende, dass sie immer noch nicht in der Lage sind, angemessen auf Datenschutzprobleme zu reagieren, weil ihnen der Überblick über den Code der Webseite fehlt oder sie nicht einmal in der Lage sind, den Code zu lesen. Mehrere Teilnehmende gaben auch zu, dass sie Webseiten, die sie vor einiger Zeit entwickelt haben, nicht mehr pflegen.

Privatsphäremotivation der Webseitenbetreibenden

Die Bedeutung, die dem Schutz der Privatsphäre ihrer Nutzenden beigemessen wird, variiert zwischen den verschiedenen Webseitenbetreibenden. Viele Webseitenbetreibende antworteten, dass der Datenschutz für sie wichtig ist. Es ist nicht immer ersichtlich, ob es sich dabei um eine leere Floskel

handelt, bei der es in erster Linie um die Einhaltung von Vorschriften oder um den tatsächlichen Schutz der Privatsphäre der Nutzenden geht. Eine Minderheit gab zu, überhaupt kein Interesse am Schutz der Privatsphäre ihrer Nutzenden zu haben. Mehrere Webseitenbetreibende waren jedoch ausdrücklich daran interessiert, ihre Webseite so datenschutzfreundlich wie möglich zu gestalten. Die Webseitenbetreibenden der letztgenannten Gruppe unterstrichen ihre Absicht, indem sie berichteten, dass sie Google Analytics als Reaktion auf die Meldung sofort ersatzlos gelöscht oder durch eine datenschutzfreundlichere Alternative ersetzt haben. Diese Webseitenbetreibenden gaben in der Regel an, dass sie kein Interesse an den Daten der Nutzenden haben, z. B. weil sie eine nicht kommerzielle Webseite betreiben.

Warum haben Webseitenbetreibende die IP-Anonymisierung bisher nicht vorgenommen?
Als Nächstes werden die Gründe für die Entstehung von Datenschutzproblemen auf Webseiten aufgezeigt, da dies die Grundlage für die Entwicklung von Lösungen für diese Probleme bildet.

Fehlerhafte technische Umsetzung
Am häufigsten berichteten die Teilnehmenden, dass sie versucht haben, IP-Anonymisierung zu implementieren, aber an der technischen Umsetzung gescheitert sind. Einzelne manuelle Überprüfungen des Webseiten-Codes bestätigten, dass manchmal tatsächlich falscher Code importiert wurde, z. B. durch das Ignorieren der Groß- und Kleinschreibung. Dennoch bleibt unklar, inwieweit einige Teilnehmende technische Hürden als Entschuldigung für eine fehlende IP-Anonymisierung anführen. In einigen Fällen bestand das Hauptproblem darin, dass die IP-Anonymisierung nicht vollständig umgesetzt wurde, z. B. wenn eine Webseite von einer anderen Person oder einem Dienstleister entwickelt wurde und die Webseitenbetreibenden keinen Überblick über den Webseiten-Code hatten.

Mangelndes Bewusstsein für Privatsphäre
Nicht nur Webseitenbetreibende, die die Entwicklung oder Wartung ihrer Webseite an andere ausgelagert haben, waren sich manchmal nicht bewusst, dass ihre Webseite aufgrund der fehlenden IP-Anonymisierung von Google Analytics eine Verletzung der Privatsphäre darstellt.
Vor allem in Fällen, in denen die Entwicklung der Webseite von einem anderen Unternehmen übernommen wurde oder schon einige Zeit zurückliegt, waren sich die Webseitenbetreibenden nicht einmal bewusst, dass Google Analytics in ihre Webseite integriert wurde, und einige Webseitenbetreibende wussten nicht einmal, was Google Analytics ist. Einige Teilnehmende haben Google Analytics jedoch auch unwissentlich selbst in ihre Webseite integriert, indem sie eine Vorlage für die Entwicklung der Webseite verwendeten, die Google Analytics enthielt. Viele Teilnehmende wussten zwar, dass sie Google Analytics in ihre Webseite aufgenommen hatten, aber sie waren sich nicht bewusst, dass die Aktivierung der IP-Anonymisierung gesetzlich vorgeschrieben ist. Insbesondere Webseitenbetreibende, die die Webseite nebenbei betreiben und nicht sehr technisch versiert sind, berichteten, dass es für sie schwierig war, in Bezug auf die Webseite immer auf dem Laufenden zu sein. Andererseits waren einige Teilnehmende davon überzeugt, dass ihre Webseite rechtskonform sei, und gingen fälschlicherweise davon aus, dass sie bereits die IP-Anonymisierung vorgenommen hatten. Hier stellte sich meist heraus, dass die Umsetzung unvollständig oder fehlerhaft war.

Unklare Zuständigkeit

Einige Webseitenbetreibende wussten zwar, dass die Implementierung der IP-Anonymisierung für die Einhaltung der Rechtsvorschriften erforderlich ist, aber nicht, dass sie als Webseitenbetreibende rechtlich für deren Umsetzung verantwortlich sind. Selbst nach Erhalt der Benachrichtigung waren einige Teilnehmende davon überzeugt, dass sie nicht tätig werden müssen. So bestand beispielsweise Rückmeldung (R) R198 (Telefonanruf) darauf, dass Google die IP-Adressen von Webseite-Nutzenden innerhalb der EU automatisch anonymisieren würde. Andere verwiesen auf die de facto technischen Verantwortlichen, z. B. R77: „*Unser Vereinsmitglied, der die Web-Seite pflegt ist sich keiner Schuld bewusst.*“ Dies ist besonders in den Fällen problematisch, in denen die betreffende Person nicht mehr verfügbar ist, z. B. R833: „*leider ist mir mein webmaster abhanden gekommen.*“ Dennoch ist vor allem in größeren Organisationen oft unklar, wer für die technische Umsetzung der IP-Anonymisierung verantwortlich ist, z. B. R1368: „*Ich bin gerade dabei herauszufinden, wer dafür verantwortlich ist.*“ Einige Webseitenbetreibende sind nicht mehr zuständig, z. B. weil sie nicht mehr als Vorstandsmitglieder der Vereinigung aktiv sind, aber auf der Webseite noch als solche aufgeführt sind.

Vertrauen auf die Urteile anderer

Viele Webseitenbetreibende beauftragen andere mit der Entwicklung oder Wartung ihrer Webseite, z. B. Agenturen, oder verwenden Vorlagen für die Einrichtung ihrer Webseite. In vielen Fällen erwarten die Webseitenbetreibenden von den Dienstleistern, dass diese sich potenzieller Datenschutzprobleme bewusst sind, selbst wenn sie nicht mit der Pflege der Webseite, sondern nur mit deren Entwicklung beauftragt wurden. Wenn Vorlagen für die Erstellung der Webseite verwendet wurden, neigen viele Webseitenbetreibende zu der Annahme, dass sie auf der sicheren Seite sind, wenn sie einfach die Standardeinstellungen übernehmen. Vielen Webseitenbetreibenden scheint das Bewusstsein zu fehlen, dass sie als Eigentümer rechtlich für die regelmäßige Pflege der Webseite verantwortlich sind. Andere wiederum haben ihre Webseite explizit von einem Spezialisten (z. B. dem Datenschutzbeauftragten) auf die Einhaltung der DSGVO überprüfen lassen, ohne dass die fehlende IP-Anonymisierung bemerkt wurde. Es bleibt jedoch unklar, ob diese Überprüfung eine technische Prüfung des Webseiten-Codes durch eine technisch versierte Person umfasste oder ob z. B. nur die Datenschutzerklärung auf rechtliche Korrektheit geprüft wurde.

Bewusst unterlassene Wartung

Selbst Teilnehmende, die sich theoretisch darüber bewusst sind, dass sie für die Pflege der Webseite verantwortlich sind, begründeten das Fehlen der IP-Anonymisierung oft damit, dass die Webseite nicht aktuell sei, weil sie gerade überarbeitet werde, dass sie gerade an einer neuen Webseite arbeiteten und deshalb die alte nicht mehr warteten, oder dass die Wartung der Webseite schon vor langer Zeit aufgegeben worden sei und die Webseite nur noch als Artefakt im Internet stehe, z. B. R160: „[Die Webseite hat] *noch einen Stand von 2012.*“

Wie sind die Webseitenbetreibenden mit der fehlenden IP-Anonymisierung umgegangen?
Viele Webseitenbetreibenden berichteten, wie sie mit der fehlenden IP-Anonymisierung umgegangen sind. Folgende vier Ansätze wurden identifiziert:

Webseitenbetreibende implementieren die IP-Anonymisierung selbstständig
Die meisten Teilnehmenden berichteten, dass sie die IP-Anonymisierung nach Erhalt der Benachrichtigung selbst umsetzten. Diese Tatsache deutet darauf hin, dass die Benachrichtigung das Bewusstsein oder das Wissen geschaffen hat, das zuvor fehlte, um das Problem anzugehen. Dennoch kann es sein, dass insbesondere Teilnehmende, die die Webseite nicht im Rahmen ihrer Beschäftigung in einer größeren Organisation betreiben, auch aus Kostengründen (zwangsläufig) auf professionelle Unterstützung verzichten, z. B. R1123: „[...] *als relativ kleiner Verein* [...] [können wir uns] *die entsprechenden Fachleute für solche Themen gar nicht leisten* [...]." Dieses Ergebnis ist jedoch mit Vorsicht zu genießen, da nicht sichergestellt ist, dass die Teilnehmenden nicht Hilfe gesucht haben, ohne dies in ihren Rückmeldungen zu erwähnen.

Webseitenbetreibende implementieren die IP-Anonymisierung mit Unterstützung
Einige Teilnehmende gaben an, dass sie die fehlende IP-Anonymisierung selbst implementiert haben, dabei aber rechtliche oder technische Unterstützung in Anspruch genommen haben, z. B. um die richtige Stelle im Code zu finden oder um Fehler im Code zu identifizieren. Juristische Unterstützung wurde in der Regel angefordert, um zu prüfen, ob Maßnahmen erforderlich sind, z. B. R1562: „*Wir haben mit unserem Anwalt gesprochen und Sie haben Recht!*" Während die meisten Teilnehmenden die Studienorganisator:innen um technische oder rechtliche Unterstützung baten, gaben nur wenige Teilnehmende an, dass sie Google direkt um Unterstützung bei der Umsetzung der IP-Anonymisierung gebeten haben, z. B. R86: „*Ihr Schreiben habe ich zum Anlass genommen bei Google anzufragen, wie man seinen Analyticsaccount komplett schließen kann, da es dazu keine Informationen im Netz gibt*."

Webseitenbetreibende delegieren die IP-Anonymisierung
Viele Webseitenbetreibende gaben an, die Umsetzung der IP-Anonymisierung delegiert zu haben. Dieser Ansatz wurde beispielsweise gewählt, wenn die Webseitenbetreibenden sich nicht in der Lage oder verantwortlich fühlten, das Problem selbst zu lösen, z. B. weil sie die Webseite nicht selbst betreiben oder weil sie in einer größeren Organisation mit verteilten Zuständigkeiten arbeiten. Im beruflichen Kontext wurde oft ein interner oder externer IT-Experte oder der für die Entwicklung oder Wartung der Webseite zuständige Dienstleister mit der Umsetzung der IP-Anonymisierung beauftragt. Ebenso wird oft der Datenschutzbeauftragte hinzugezogen, manchmal wird sogar ein Rechtsanwalt mit der Umsetzung beauftragt. Teilnehmende, die die Webseite im privaten Kontext oder im Rahmen einer selbständigen Tätigkeit betreiben, gaben die Aufgabe jedoch oft an technisch versierte Personen aus ihrem privaten Umfeld weiter.

Webseitenbetreibende implementieren die IP-Anonymisierung nicht
Nur wenige Webseitenbetreibende gaben an, dass sie das Problem aufgrund von Zeitmangel oder unzureichenden Kenntnissen nicht lösen konnten, z. B. R1015: „*Es ist leider sehr kompliziert, das*

umzustellen und kostet mich Zeit&Geld, weswegen ich der Sache nicht weiter nach gegangen bin.“ Einige dieser Teilnehmenden wiesen aber auch direkt darauf hin, dass sie keine Notwendigkeit sehen, die fehlende IP-Anonymisierung umzusetzen. Wahrscheinlich gibt es noch mehr Webseitenbetreibende, die das Problem auf ihrer aktuellen Webseite nicht mehr lösen, weil sie, zum Beispiel planen, die Webseite neu zu erstellen.

Welche Hürden müssen Webseitenbetreibende bei der Implementierung der IP-Anonymisierung überwinden?

Nach Erhalt der Meldung standen die Webseitenbetreibenden, die versuchten, die IP-Anonymisierung zu implementieren, vor mehreren Hürden, die im Folgenden beschrieben werden.

Mangel an Ressourcen

Insbesondere private und selbständige Webseitenbetreibende haben oft nicht die finanziellen und zeitlichen Ressourcen, um sich um die technischen Aspekte ihrer Webseite zu kümmern. Zum einen muss die Pflege der Webseite im Tagesgeschäft oft hinter anderen Aufgaben zurückstehen, vor allem wenn private Probleme auftauchen, wie z. B. bei einer Webseitenbetreibenden, die berichtete, dass ihr Mann kürzlich verstorben sei. Zum anderen fehlt gerade diesen Webseitenbetreibenden das nötige Geld, um einen Spezialisten für die Webseitenwartung oder den Datenschutz zu beauftragen.

Mangel an technischem Wissen

Viele Teilnehmende berichteten, dass ihnen das technische Grundverständnis zur Umsetzung der IP-Anonymisierung fehle. Insgesamt bezeichneten sich viele Teilnehmende sogar als technisch unbegabt, z. B. R168: „*Ich bin 68J, Rentner und habe Wordpress über den Provider* […] *installiert. Ich verstehe das Javascript nicht und weiß nicht, wie ich das einbinden soll.*“ In diesem Zusammenhang beklagten einige Teilnehmende auch, dass es ohne technisches Fachwissen schwierig sei, über neue Datenschutzanforderungen auf dem Laufenden zu bleiben und diese umzusetzen, z. B. R267: „*Ich bin kein Profi in Webseiten und die laufenden Änderungen im Datenschutz kann man nur realisieren, wenn man sich täglich damit beschäftigt*.“

Probleme mit dem Code

Selbst Webseitenbetreibende, die im Prinzip das technische Verständnis für die Implementierung der IP-Anonymisierung haben, stießen bei der Arbeit mit dem Code oft auf Probleme. Einige Teilnehmende hatten z. B. Schwierigkeiten, die richtige Codestelle zu finden, während andere erfolglos versuchten, Google Analytics vollständig aus ihrem Code zu löschen. Andere berichteten, dass sie Fehlermeldungen erhalten, ohne den spezifischen Fehler identifizieren zu können, z. B. R71: „*Ich habe sofort versucht den Fehler zu beheben, leider konnte ich Ihn nicht finden.*“

Abhängigkeiten und zähe Prozesse in Organisationen

Mitarbeitende in größeren Organisationen haben oft sowohl zeitliche und finanzielle Ressourcen als auch Zugang zu internen oder externen Fachleuten, die sie bei der Implementierung der IP-Anonymisierung unterstützen können. Die Zugehörigkeit zu einer größeren Organisationsstruktur bringt

jedoch andere Herausforderungen mit sich, z. B. die Abhängigkeit von anderen Mitarbeitenden, die aufgrund von Urlaub oder Elternzeit nicht zur Verfügung stehen oder noch gar nicht gefunden wurden, wenn die Stelle, die für die Wartung der Webseite zuständig ist, gerade nicht besetzt ist. Komplexe Organisationsstrukturen, in denen jede Änderung von den Verantwortlichen auf verschiedenen Managementebenen genehmigt werden muss, können auch grundlegende Anpassungen wie den Verzicht auf Google Analytics oder die Implementierung der IP-Anonymisierung erheblich verzögern. Diesbezüglich berichtete z. B. R531: *„Ich habe bei Aufnahme meiner Tätigkeit und der damit verbundenen Bestandsaufnahme tatsächlich schon das Problem identifiziert und an meiner Geschäftsleitung weitergetragen. Die Angelegenheit wird seit letzter Woche auch intern diskutiert und es werden zurzeit nach Alternativen gesucht um eine angemessene Entscheidungsgrundlage für den Verantwortlichen ausgearbeitet.“*

3.3.10 Aus der thematischen Analyse abgeleitete Personas

Im vorherigen Unterkapitel wurden diverse Gründe für die Fehlkonfiguration von Google Analytics aufgezeigt sowie die Hürden benannt, die Webseitenbetreibende bei der Bewältigung dieser Herausforderung überwinden müssen. Die thematische Analyse hat gezeigt, dass Webseitenbetreibende Webseiten in verschiedenen Kontexten und unter verschiedenen Umständen betreiben, was zu spezifischen Hürden und Bedürfnissen führen kann. In diesem Unterkapitel wird erläutert, wie die vorherigen Erkenntnisse für drei Beispiel-Personas, die verschiedene Typen von Webseitenbetreibenden aus den Daten repräsentieren, konkret aussehen. In Abbildung 6 wird ein Überblick über die Personas gegeben. Personas, werden in dieser Arbeit als abstrakte Repräsentationen von Nutzenden (Guo et al., 2011; Pruitt & Grudin, 2003). Sie sind eine weit verbreitete Technik des Interaktionsdesigns, um die Entwicklung von Produkten zu unterstützen (Guo et al., 2011; Pruitt & Grudin, 2003). Die hier vorgestellten Personas wurden im Rahmen eines Workshops entwickelt. Die Personas wurden so ausgewählt, dass sie (1) die Mehrheit der Fälle in den Daten abdecken und (2) das breite Spektrum der Hintergründe von Webseitenbetreibenden und der damit verbundenen Herausforderungen widerspiegeln. Die Personas können helfen, die Herausforderungen der verschiedenen Webseitenbetreibenden zu verstehen. Darüber hinaus bieten sie eine Grundlage für die Entwicklung von Unterstützungsoptionen für Webseitenbetreibende, die ihre spezifischen Bedürfnisse berücksichtigen.

Abbildung 6. Beispiel-Personas, die verschiedene Webseitenbetreibende aus dem Datensatz repräsentieren. Die Abbildung orientiert sich an der Darstellung von Stöver et al. (2023).

Persona 1: Die unwissenden Privatpersonen

Persona 1, die unwissenden Privatpersonen, besitzen ihre Webseite entweder aus privatem Interesse, um z. B. über ein bestimmtes Anliegen zu informieren oder im Rahmen ihrer Tätigkeit in einem (kleineren) Verein. Sie sind technisch nicht versiert und stoßen bereits bei der Erstellung der Webseite, für die sie sich auf eine Vorlage oder auf die Unterstützung aus ihrem privaten Umfeld verlassen, an die Grenzen ihres technischen Verständnisses. Daher wissen sie in der Regel nicht einmal, dass sie Google Analytics auf ihrer Webseite verwenden. Da sie die von Google Analytics generierten Daten nicht benötigen und tendenziell großen Wert auf den Schutz der Privatsphäre ihrer Nutzenden legen, ärgern sie sich über die Erkenntnis, dass sie die IP-Adressen ihrer Nutzenden bisher (illegal) an Google weitergegeben haben und sehen dies als ein weiteres Beispiel dafür, dass sie sich gegen den übermächtigen Datensammler Google wehren müssen. Sie sind daher motiviert, das Problem der fehlenden IP-Anonymisierung sofort zu lösen, z. B. indem sie Google Analytics vollständig von ihrer Webseite entfernen. Obwohl sie in der Regel genügend freie Zeit haben, um sich mit der Lösung des Problems zu befassen, stoßen sie meist an die Grenzen ihres technischen Verständnisses. Sie fühlen sich schnell mit der Problemlösung überfordert, da ihnen ein grundlegendes Verständnis des Codes fehlt. Sie verfügen in der Regel nicht über die finanziellen Mittel, um professionelle Unterstützung in Anspruch zu nehmen; daher scheitern sie oft an der Umsetzung der IP-Anonymisierung. Während einige dazu übergehen, ihre Webseite abzuschalten, wenn sie ohnehin nicht mehr gepflegt wird, ignorieren andere das Problem aus Hilflosigkeit. Einige unwissende Privatpersonen wandten sich jedoch an die Studienorganisator:innen, um technische Unterstützung zu erhalten, da sie mit den in der Benachrichtigung enthaltenen Anweisungen überfordert waren. Mit Hilfe gelang es ihnen, die IP-Anonymisierung zu implementieren oder Google Analytics von ihrer Webseite zu entfernen.

Persona 2: Die vielbeschäftigten Selbstständigen

Persona 2, die vielbeschäftigten Selbstständigen, sind meist Selbstständige oder Personen, die ein kleines lokales Unternehmen besitzen. Sie haben ein begrenztes Interesse an Nutzendenmetriken und sind daher auf die Verwendung eines Tracking-Tools angewiesen. Dabei wissen sie oft nicht, dass sie als Webseitenbetreibende für die Umsetzung der IP-Anonymisierung verantwortlich sind und gehen davon aus, dass die Webdesign-Agentur, mit deren Hilfe sie die Webseite erstellt haben, oder sogar Google selbst bereits alle rechtlichen Anforderungen ordnungsgemäß umsetzt. Die Webseite ist für sie in der Regel nur Mittel zum Zweck und soll möglichst wenig ihrer ohnehin begrenzten Zeit in Anspruch nehmen, sodass sie sich über die Beschäftigung mit Datenschutzfragen ärgern. Da sie in der Regel nur über begrenzte finanzielle Mittel verfügen, sind sie bis zu einem gewissen Grad auf die Hilfe einer Agentur oder eines Anwalts angewiesen. Eine erste Hürde besteht jedoch darin, zu entscheiden, an wen sie sich wenden sollen, da die Beteiligten nicht im Informationsaustausch stehen und der Anwalt z. B. zwar Auskunft darüber geben kann, was datenschutzrechtlich erforderlich ist, aber nicht, wie dies technisch umgesetzt werden kann. Manche Persona 2 scheitern auch an der Umsetzung der IP-Anonymisierung von Google Analytics, weil sie nicht einmal über die Zugangsdaten zur Bearbeitung ihrer Webseite verfügen, da eine andere Person (die in manchen Fällen nicht mehr verfügbar ist) die Erstellung der Webseite für sie übernommen hat, ohne ihnen die Zugangsdaten nachträglich zur Verfügung zu stellen. Dementsprechend werden solche Webseiten oft gar nicht mehr gepflegt. Viele

Persona 2 beheben das Problem jedoch, indem sie (a) die IP-Anonymisierung implementieren, (b) Google Analytics gegen eine datenschutzfreundlichere Alternative wie Matomo[7] austauschen, (c) die Implementierung an eine Agentur oder eine technisch versierte Person aus ihrem privaten Umfeld delegieren oder (d) sich auf die im Rahmen der Benachrichtigung bereitgestellte Anleitung sowie das Tool zur Überprüfung der Implementierung verlassen.

Persona 3: Die informierten Multi-Stakeholder

Persona 3, die informierten Multi-Stakeholder, besitzen die Webseite aufgrund ihrer Tätigkeit in einem größeren Unternehmen. Google Analytics wird absichtlich auf der Webseite eingesetzt, um das Verhalten der Nutzenden zu verfolgen. Persona 3 ist sich größtenteils darüber bewusst, dass die DSGVO eine IP-Anonymisierung vorschreibt, weshalb die meisten Persona 3, im Gegensatz zu Persona 1 und 2, diese bereits bis zu einem gewissen Grad, aber oft nicht umfassend, umgesetzt haben. In dieser Hinsicht ist Persona 3 weniger am Schutz der Privatsphäre ihrer Nutzenden interessiert als an der Einhaltung der gesetzlichen Anforderungen, um Strafen zu vermeiden. Persona 3 verfügt über umfangreiche finanzielle und personelle Ressourcen, weshalb die Umsetzung der IP-Anonymisierung meist an interne oder externe Dienstleister delegiert wird. Eine Schwierigkeit bei der Umsetzung kann jedoch darin bestehen, dass den Beteiligten der Überblick über die meist komplexen Webseitenstrukturen fehlt. Darüber hinaus befindet sich die Organisation von Persona 3 meist in einem Zielkonflikt, da sie gerne umfangreiche Nutzerdaten sammeln möchte, weshalb sie z. B. Google Analytics nicht komplett löschen oder durch ein weniger sensibles Tracking-Tool ersetzen möchte. An der Entscheidung, wie das Problem zu lösen ist, sind daher in der Regel verschiedene Akteure im Unternehmen beteiligt, die zum Teil über sehr unterschiedliches technisches und rechtliches Hintergrundwissen verfügen, was die Kommunikation zusätzlich erschwert. Je nach Organisationsstruktur durchläuft die Entscheidung mehrere Managementebenen und Entscheidungsgremien, was den Prozess erheblich verlangsamt. Ein Teil der verschickten Benachrichtigungen enthielt eine Erklärung, dass IP-Adressen bei der Erhebung der Analysedaten pseudonymisiert oder anonymisiert werden müssen, um den Datenschutzgesetzen zu entsprechen. Diese Hinweise wurden von Persona 3 meist als besonders hilfreich empfunden, da sie diese Aussage als zusätzliches Argument in der internen Kommunikation anführen konnten. Obwohl Persona 3 bereits wusste, dass die IP-Anonymisierung gesetzlich vorgeschrieben war, verlieh die Benachrichtigung diesem Argument zusätzliches Gewicht. Daher haben die meisten Persona 3 die Implementierung der IP-Anonymisierung nach Erhalt der Benachrichtigung mithilfe interner Dienstleister (z. B. der IT-Abteilung) umgesetzt.

3.3.11 Diskussion

Im Rahmen eines Feldexperiments wurden Webseitenbetreibende über die fehlende IP-Anonymisierung von Google Analytics informiert, was ein Privatsphärerisiko darstellt. Um die Hintergründe besser zu verstehen, wurde eine Umfrage unter den betroffenen Webseitenbetreibenden durchgeführt und ihre Rückmeldungen auf die Benachrichtigungen wurden mithilfe einer thematischen Analyse qualitativ analysiert.

[7] Matomo ist eine Open Source Web-Analytic-Platform (*https://matomo.org/free-software/*, o. J.).

Da die qualitative Analyse der Rückmeldungen das Kernstück dieses Kapitels bildet, werden die Ergebnisse daraus als Ausgangslage für die Diskussion verwendet und um Erkenntnisse aus der Umfrage und dem Feldexperiment ergänzt. Die thematische Analyse der Antworten ergab vier Themen, nämlich die Umstände der Webseitenbetreibenden, die Gründe für das Fehlen der IP-Anonymisierung, die Lösungsansätze der Webseitenbetreibenden und die Hürden, denen die Webseitenbetreibenden begegnet sind. Diese Themen zeigen, dass Webseitenbetreibende einen hohen Bedarf an Unterstützung haben, um datenschutzrechtliche Anforderungen korrekt umzusetzen. Die Umstände und Bedürfnisse von Webseitenbetreibenden sind jedoch so unterschiedlich, dass eine wirklich effektive Unterstützung auch diese berücksichtigen muss. Die Themen und die daraus abgeleiteten Personas zeigen, dass die unterschiedlichen Bedürfnisse der verschiedenen Zielgruppen in erster Linie ein Problem darstellen. Gleichzeitig bieten sie verschiedene Ansatzpunkte, wie die Unterstützung gestaltet werden kann und wie Webseitenbetreibende angesprochen werden können, um die Einhaltungsquoten zu verbessern. In diesem Abschnitt werden die Ergebnisse unter Bezugnahme auf die bisherige Forschung zusammengefasst und es wird aufgezeigt, welche Voraussetzungen erfüllt sein müssen, damit Webseitenbetreibende Datenschutzprobleme erfolgreich lösen können. Außerdem werden Maßnahmen vorgestellt, die die Bedürfnisse verschiedener Webseitenbetreibender berücksichtigen.

Hintergründe der Webseitenbetreibenden

Um die Ursachen für die fehlende IP-Anonymisierung aus Sicht der Webseitenbetreibenden zu verstehen, kann es sinnvoll sein, zunächst die Umstände, unter denen die Webseiten betrieben werden, zu ergründen. Die thematische Analyse zeigt, dass Webseitenbetreibende aus unterschiedlichen Beweggründen und unter diversen Umständen Webseiten betreiben. Diese unterschiedlichen Umstände führen zu spezifischen Herausforderungen und Unterstützungsbedürfnissen für verschiedene Webseitenbetreibende. Um diese Vielfalt greifbar zu machen, wurden drei Beispiel-Personas vorgestellt, die die Mehrzahl der Fälle abdecken und die große Bandbreite der Lebensumstände der Webseitenbetreibenden in den Daten widerspiegeln: Persona 1, die unwissenden Privatpersonen, betreiben ihre Webseite aus privatem Interesse, oft mit hoher Motivation, die Privatsphäre der Endnutzenden zu schützen, aber mit wenig technischen Fähigkeiten, um entsprechende Maßnahmen zu implementieren. Persona 2, die vielbeschäftigten Selbstständigen, besitzen die Webseite oft, um ihr kleines Unternehmen online zu repräsentieren, haben wenig Zeit für die Webseite und haben oft ein begrenztes Interesse an den Daten der Nutzenden. Persona 3, die informierten Multi-Stakeholder, besitzen die Webseite als Teil ihrer Arbeit in einem größeren Unternehmen, in dem sie auf Nutzendendaten angewiesen sind, und müssen oft andere Interessengruppen in Entscheidungen über die Webseite einbeziehen.

Forschungsfrage 1: Ursachen für die fehlende IP-Anonymisierung

Mit Forschungsfrage 1 wurde nach den Ursachen aus Sicht der Webseitenbetreibenden für die fehlende IP-Anonymisierung von Google Analytics auf ihren Webseiten gefragt. Insgesamt deuten die Ergebnisse der thematischen Analyse darauf hin, dass eine häufige Ursache für die fehlende IP-Anonymisierung darin besteht, dass den Webseitenbetreibenden das Bewusstsein für Datenschutzangelegenheiten fehlt.

Dieses Ergebnis steht im Einklang mit verwandten Arbeiten, in denen gezeigt wurde, dass sich Entwickler:innen oft nicht über die Datenpraktiken der Drittanbieterdienste bewusst sind, die sie in ihre Produkte integrieren (Alomar & Egelman, 2022; Balebako et al., 2014; Hadar et al., 2018). Die Daten der vorliegenden Arbeit zeigen, dass das Problem für Webseitenbetreibende sogar noch tiefgreifender ist: Insbesondere Persona 1 und 2 sind sich teilweise nicht nur des Fehlens der IP-Anonymisierung nicht bewusst, sondern wissen manchmal nicht einmal, was Google Analytics ist oder dass sie Google Analytics auf ihrer Webseite implementiert haben. Häufig wird die IP-Anonymisierung auch falsch implementiert, was oft mit minimalen Änderungen am Code behoben werden kann. Dieser Befund bestärkt die oben geführte Diskussion, dass Webseitenbetreibende sich von anderen *Expert Users* unterscheiden, weil ihnen im Gegensatz zu diesen manchmal das technische Verständnis des Webseiten-Codes fehlt. Im Gegensatz zu anderen *Expert Users* sind viele Webseitenbetreibende (insbesondere Persona 1 und 2) weder an Nutzendendaten interessiert noch benötigen sie diese. Viele Webseitenbetreibenden verfolgen mit ihrer Webseite keine wirtschaftlichen Interessen, sondern nutzen sie für private Interessen oder zur Präsentation ihres Kleinunternehmens, im Gegensatz zu Entwicklern, die oft eine unmittelbare Monetarisierung ihrer Apps anstreben (Mhaidli et al., 2019).
Ein weiterer Grund für das Fehlen der IP-Anonymisierung ist, dass Webseiten nicht mehr aktiv gepflegt werden. Dieser Aspekt wurde in anderen Kontexten noch nicht erwähnt, könnte aber in Zukunft an Relevanz gewinnen, vor allem mit der stetig steigenden Anzahl von mobilen Apps.
Ähnlich wie in der Forschung zu Expertennutzenden wird auch in dieser Arbeit gezeigt, dass Privatsphärerisiken (wie die fehlende IP-Anonymisierung) auch dadurch zustande kommen, dass sich Webseitenbetreibende ihrer Verantwortung nicht bewusst sind oder diese bei Drittanbietern oder den Nutzenden sehen (Mhaidli et al., 2019; Nurgalieva et al., 2021; Tahaei, Li, et al., 2022). Ähnlich wie bei Entwickler:innen verlassen sich viele Webseitenbetreibende auf andere Stellen wie Webdesign-Agenturen oder Datenschutzbeauftragte, wenn es um Datenschutzfragen geht (Mhaidli et al., 2019).
Die Ergebnisse der Umfrage bestätigen diese Erkenntnisse. Darin gaben nur 12.7 % der Teilnehmenden an, dass sie sich der fehlenden IP-Anonymisierung vor der Benachrichtigung bewusst waren, wobei 19.5 % nicht einmal wussten, dass sie Google Analytics auf ihrer Webseite verwendeten.

Forschungsfrage 2: Vorgehen bei der Problembehebung und Hürden

Mit der Forschungsfrage 2 sollte herausgefunden werden, (a) wie Webseitenbetreibende bei der Behebung der fehlenden IP-Anonymisierung von Google Analytics auf ihrer Webseite vorgehen und (b) welche Herausforderungen sie dabei bewältigen müssen.
Die Ergebnisse der thematischen Analyse zeigen, dass einige Webseitenbetreibende die Datenschutzprobleme selbst lösten, während andere technische und rechtliche Unterstützung suchten. Diese Beobachtung deutet auf einen großen Bedarf an Unterstützung der Webseitenbetreibenden in Fragen des Datenschutzes hin. Diese Unterstützung sollte sich vor allem an die Personas 1 und 2 richten, die wenig Geld und Zeit für Datenschutzmaßnahmen haben. Bei der Konzeption von Unterstützungsmöglichkeiten sollten die unterschiedlichen Bedürfnisse von Webseitenbetreibenden berücksichtigt werden.
Eine große Herausforderung, insbesondere für Persona 1 und 2, ist der Mangel an Ressourcen, was sich mit den Ergebnissen von Balebako et al. (2014) deckt, die zeigen, dass das Vorhandensein von

Ressourcen einen großen Einfluss darauf hat, ob Maßnahmen zum Schutz der Privatsphäre umgesetzt werden, und dass es vor allem in kleinen Unternehmen an Ressourcen fehlt. Darüber hinaus haben Personas 1 und 2 mit einem allgemeinen Mangel an technischem Wissen zu kämpfen. Diese Situation ist ein wesentlicher Unterschied zwischen der hier vorgestellten Studie und der Studie von Utz et al. (2022), in der die meisten Befragten einen technischen Hintergrund hatten.
Die Ergebnisse der Umfrage zeigen, dass gut ein Drittel das Problem mithilfe der Anleitung aus der Benachrichtigung und des bereitgestellten Prüftools selbst lösen konnte. 11 % lösten das Problem mit der Hilfe anderer. Die übrigen Teilnehmenden leiteten das Problem an externe Dienstleister oder Kolleg:innen weiter.
Unabhängig von den spezifischen Hürden müssen einige Grundvoraussetzungen erfüllt sein, damit Webseitenbetreibende Privatsphärerisiken auf ihren Webseiten beheben können. Diese Voraussetzungen werden im folgenden Abschnitt vorgestellt.

Voraussetzungen für die Behebung von Privatsphärerisiken
Die Ergebnisse der thematischen Analyse zeigen, dass mindestens sechs Voraussetzungen erfüllt sein müssen, damit alle Webseitenbetreibenden die Privatsphärerisiken auf ihrer Webseite beheben, sprich die IP-Anonymisierung von Google Analytics umsetzen können. In Abbildung 7 wird ein Überblick gegeben.

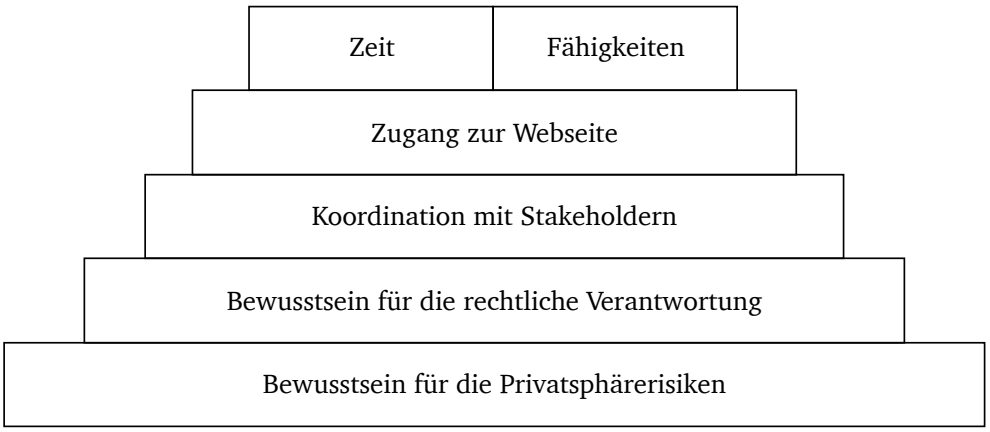


Abbildung 7. Voraussetzungen für die Behebung der fehlenden IP-Anonymisierung. Die Abbildung orientiert sich an der Darstellung von Stöver et al. (2023).

Bewusstsein für die Privatsphärerisiken
Erstens müssen sich Webseitenbetreibende darüber bewusst sein, dass ihre Webseite ein Privatsphärerisiko enthält. Daher müssen sie wissen, welche Dienste von Drittanbietern auf ihrer Webseite eingebunden sind, welche Daten sie sammeln und welche Privatsphärerisiken mit ihnen verbunden sind. Für den hier vorgestellten Anwendungsfall bedeutet dies, dass sich Webseitenbetreibende darüber bewusst sein müssen, dass Google Analytics auf ihrer Webseite integriert ist und dass eine IP-Anonymisierung notwendig ist.

Bewusstsein für die rechtliche Verantwortung

Webseitenbetreibende müssen sich darüber im Klaren sein, dass sie als Betreibende rechtlich für die Umsetzung von Datenschutzmaßnahmen auf ihren Webseiten verantwortlich sind – auch wenn sie nicht für die technische Umsetzung zuständig sind, weil z. B. ein IT-Mitarbeitender bzw. eine IT-Mitarbeitende oder eine Webdesign-Agentur damit betraut ist. Im untersuchten Beispiel fallen alle Webseiten unter die DSGVO, die Webseitenbetreibende zur Umsetzung von Datenschutzmaßnahmen verpflichtet.

Koordination mit Stakeholdern

In größeren Organisationen sind oft viele Interessengruppen direkt oder indirekt an Entscheidungen beteiligt, die die Webseite der Organisation betreffen. Dementsprechend müssen diese Gruppen zustimmen, dass es tatsächlich ein Privatsphärerisiko gibt, das gelöst werden muss. Auch wie das Problem gelöst werden soll, muss abgesprochen werden. Im vorliegenden Anwendungsfall ergibt sich die Notwendigkeit zum Handeln aus den Datenschutzgesetzen und wurde durch das Urteil des Landgerichts Dresden bestätigt. Dennoch müssen alle Beteiligten diese Rechtslage verstehen und dem Thema Priorität einräumen. Frühere Untersuchungen haben gezeigt, dass die allgemeine Datenschutzkultur in Unternehmen die Umsetzung von Datenschutzmaßnahmen beeinflusst.

Eine datenschutzfreundliche Kultur könnte auch dazu beitragen, das Thema bei den Entscheidungstragenden zu priorisieren. Ein Ansatz hierfür kann die Beschäftigung sogenannter Datenschutz-Champions sein –Menschen, denen die Förderung der Privatsphäre am Herzen liegt (Tahaei et al., 2021b).

Zugang zur Webseite

Um Änderungen am Code ihrer Webseite vornehmen zu können, benötigen die Webseitenbetreibenden Zugang zu diesem Code. Diese Voraussetzung wird zu einem Problem, wenn eine Webseite vor langer Zeit eingerichtet wurde und der Zugang verloren gegangen ist oder die Personen, die die Webseite gepflegt haben, nicht verfügbar sind (z. B. wenn der Webmaster im Urlaub ist). In dem vorliegenden Anwendungsfall haben einige Webseitenbetreibende festgestellt, dass sie auch die Zugangsdaten für ihr Google-Analytics-Konto benötigen, um die Privatsphärerisiken zu beheben.

Ein weiteres Problem tritt auf, wenn die IP-Anonymisierung nicht korrekt in den Dienst eines Drittanbieters implementiert wurde, den der Webseitenbetreibende auf seiner Webseite eingebunden hat (z. B. im Rahmen eines Kontaktformulars). In diesem Fall sind die Webseitenbetreibenden zwar rechtlich verantwortlich, können aber nicht tätig werden, da sie nicht über den erforderlichen Zugang zu den Systemen der Drittanbieter verfügen.

Zeit

Webseitenbetreibende brauchen Zeit, um sich mit dem Datenschutzproblem zu befassen, es zu lösen oder nach Alternativen zu suchen. Im vorliegenden Fall ist der Aufwand für die notwendigen Code-Änderungen meist gering und sollte wenig Zeit in Anspruch nehmen. Allerdings kann diese Anpassung für Webseitenbetreibende mit wenig technischem Wissen (Persona 1) oder für Personen, die mit verschiedenen Interessengruppen kommunizieren müssen (Persona 2), zeitaufwändig sein. Daher ist es essenziell, dass die Webseitenbetreibenden mit wenig Zeitaufwand entlastet werden. Im Sinne eines

Privacy-by-Design-Ansatzes könnten Agenturen oder Vorlagen-Anbieter z. B. datenschutzfreundliche Alternativen (z. B. Matomo) standardmäßig implementieren.

Technische Fähigkeiten
Webseitenbetreibende benötigen technische Fähigkeiten, um sich mit Datenschutzfragen zu befassen, oder sie müssen in der Lage sein, diese zu erwerben. Diese Voraussetzung ist ein bemerkenswerter Unterschied zu anderen Fachanwendern wie Entwickler:innen, die oft über das technische Know-how verfügen. Vielen Webseitenbetreibenden fehlt es jedoch an technischen Kenntnissen, insbesondere wenn die Webseite nur ein Mittel zum Zweck ist, z. B. um ein kleines Unternehmen im Internet zu repräsentieren. Für den vorliegenden Fall bedeutet dies, dass Webseitenbetreibende wissen müssen, an welcher Stelle im Code sie die IP-Anonymisierung implementieren müssen oder wie sie Google Analytics ganz von ihrer Webseite entfernen können. Insbesondere wenn die Unternehmen ihre Webseite nicht selbst erstellt haben, kann es schwierig sein, die richtigen Stellen im Code zu finden.

Forschungsfrage 3: Gestaltung von Benachrichtigungen
In Forschungsfrage 3 geht es darum, wie Benachrichtigungen gestaltet sein sollten, um die Webseitenbetreibenden effektiv dabei zu unterstützen, die fehlende IP-Anonymisierung von Google Analytics zu beheben. Auf Grundlage der Ergebnisse aus dem Feldexperiment, der Umfrage sowie der Analyse der Rückmeldungen lassen sich Implikationen für die Gestaltung von effektiven Benachrichtigungen ableiten, die im Folgenden diskutiert werden.
Die Ergebnisse des Feldexperiments zeigen, dass Benachrichtigungen eine effektive Maßnahme sein können, damit Webseitenbetreibende bestehende Fehlkonfigurationen beheben, die datenschutzrechtliche Konsequenzen für sie haben können. Die Ergebnisse zeigen weiterhin, dass das Problem der fehlenden IP-Anonymisierung besonders häufig gelöst wurde, wenn dieses in der Benachrichtigung als Rechtsverstoß formuliert wurde, und vor allem dann, wenn die Benachrichtigung in Form eines Schreibens einer juristischen Forschungsgruppe versandt wurde. Dabei wurde das Problem in 76.3 % der Fälle gelöst, während es nur in 33.9 % der Fälle gelöst wurde, wenn die Benachrichtigung per E-Mail von Informatikforschenden versandt wurde, die vor einem Datenschutzproblem warnten. Über alle Gruppen hinweg behoben 56.6 % der benachrichtigten Webseitenbetreibenden das Problem, verglichen mit 9.2 % in der Kontrollgruppe.
Die Ergebnisse der Umfrage zeigen, dass die informierten Webseitenbetreibenden einen Bedarf an Unterstützungsmaßnahmen haben. Die Mehrheit wünscht sich zukünftige Benachrichtigungen per E-Mail. Auch weitere Unterstützung in Form des Self-Check-Tools wurde von den meisten mindestens als hilfreich bewertet, wobei nur etwa ein Drittel der Webseitenbetreibenden bereit wäre, dafür zu zahlen. Die Umfrageergebnisse zeigen auch, wie essenziell vertrauensfördernde Maßnahmen sind, um Maßnahmen wie Benachrichtigungen effektiv zu machen. Dazu gehören neben der Möglichkeit, den Sender zu verifizieren, auch konkrete Unterstützungsangebote wie das Prüftool.
Zusammenfassend lässt sich sagen, dass Benachrichtigungen eine Möglichkeit sind, um Webseitenbetreibende zu unterstützen, die von diesen auch als hilfreich angesehen wird. Eine Benachrichtigung sollte nicht nur auf das Problem hinweisen, sondern auch konkret aufzeigen, wie dieses gelöst werden kann. Am besten geschieht dies durch ein konkretes Unterstützungsangebot wie

ein Prüftool oder durch individuelle Unterstützung. Als Medium der Benachrichtigung genügt eine E-Mail, die gegenüber dem Brief präferiert wird. Webseitenbetreibende bekommen in der Regel viele Nachrichten, deshalb ist es essenziell, dass sie der Benachrichtigung vertrauen können, um entsprechend zu handeln. Dafür ist auch der Absender einer solchen Benachrichtigung relevant. Es scheint hilfreich, wenn dieser den Webseitenbetreibenden bekannt ist, er eine glaubwürdige Intention hat und diese transparent und nachvollziehbar für die Webseitenbetreibenden darstellt. Eine Möglichkeit wäre, dass z. B. Berufsverbände solche Benachrichtigungen versenden.

Maßnahmen für verschiedene Webseitenbetreibende

Sowohl die Umfrage als auch die thematische Analyse haben gezeigt, dass einige Webseitenbetreibende Datenschutzprobleme selbst lösen, während andere technische und rechtliche Unterstützung suchen. Diese Beobachtung deutet auf einen großen Bedarf an Unterstützung der Webseitenbetreibenden in Datenschutzfragen hin.

Diese Unterstützung, die bereits in früheren Publikationen gefordert wurde, sollte sich vor allem an Personas 1 und 2 richten, die wenig Geld und Zeit für Datenschutzmaßnahmen haben. Bei der Konzeption von Unterstützungsmöglichkeiten sollten die unterschiedlichen Bedürfnisse von Webseitenbetreibenden berücksichtigt werden. Die thematische Analyse zeigt, dass Webseitenbetreibende unter verschiedenen Umständen agieren und vor unterschiedlichen Herausforderungen bei der Lösung von Datenschutzproblemen stehen. In dieser Arbeit werden diese Unterschiede in Form von drei Beispiel-Personas dargestellt. Die Voraussetzungen, um Datenschutzprobleme lösen zu können, sind nicht bei allen Webseitenbetreibenden gleich. Um Webseitenbetreibenden dabei zu helfen, die Anforderungen zu erfüllen, werden im Folgenden mehrere Maßnahmen vorgeschlagen (siehe Abbildung 8). Diese Maßnahmen bauen auf Vorschlägen auf, die in der Literatur bereits für *Expert Users* wie Entwickler:innen vorgeschlagen wurden. Maass et al. (2017) stellen beispielsweise ein automatisiertes Webseiten-Scanning-Portal vor, mit dem Sicherheits- und Datenschutzmerkmale von Webseiten bewertet werden können. Tahaei et al. (2022) schlagen die Erstellung von Multimedia-Materialien zum Datenschutz vor, die App-Entwickler:innen unterstützen. In einer Reihe von Studien wurde bereits untersucht, wie Entwickler:innen, Admins und Webseitenbetreibende über Datenschutz- und Sicherheitsprobleme informiert werden können (Canali et al., 2013; Çetin et al., 2017; Durumeric et al., 2014; Li, Durumeric, et al., 2016; Stock et al., 2016, 2018; Zeng, Li, & Stark, 2019). Mit Blick auf die Erkenntnisse dieser Arbeit ist es jedoch unerlässlich, diese Maßnahmen an die Gegebenheiten der verschiedenen Webseitenbetreibenden anzupassen.

Die Anpassung der Maßnahmen an die unterschiedlichen Umstände und Herausforderungen erhöht die Wahrscheinlichkeit, dass die Maßnahmen wirksam und nicht im schlimmsten Fall kontraproduktiv sind. Zum Beispiel können Meldungen, die Webseitenbetreibende über ein Datenschutzproblem auf ihrer Webseite informieren, einen unterschiedlichen Inhalt haben. Während die Erwähnung einer möglichen Strafe in einer Benachrichtigung in größeren Unternehmen ein gutes Argument für Maßnahmen sein kann, kann sie bei einer Privatperson möglichweise Angst als Reaktion auslösen. In Abbildung 8 werden verschiedene potenzielle Maßnahmen vorgestellt und es wird aufgezeigt, wie diese unter Berücksichtigung der Erkenntnisse aus dieser Arbeit für verschiedene Webseitenbetreibende angepasst werden können.

Adressierte Voraussetzung	Maßnahme	Beschreibung	Persona 1: Die unwissenden Privatpersonen	Persona 2: Die vielbeschäftigten Selbstständigen	Persona 3: Die informierten Multi-Stakeholder
Bewusstsein für Privatsphärerisiken	Informations-kampagnen	Webseitenbetreibende über bestehende Privatsphärerisiken informieren, die relevant für sie sind.	Sensibilisierung für mögliche Privatsphärerisiken; erinnern, dass Webseiten, die nicht mehr benötigt oder nicht gewartet werden, offline genommen werden sollten; geeignete Kanäle finden, z. B. Printmedien, NGOs, nationale Datenschutzbehörden.	Bewusstsein für Verantwortlichkeit schaffen, z. B. in Form von Newslettern, die Webseiten-betreibenden über ihre Handlungs-notwendigkeit informieren. Eine zentrale Anlaufstelle (z. B. Webseite) sollte alle nötigen Informationen zum Thema zusammenfassen.	Bewusstsein bei Entscheidungstragenden in Unternehmen schaffen, z. B. durch ausgewählte Wirtschaftsmedien.
Bewusstsein für rechtliche Verantwortung	Benach-richtigungen	Webseitenbetreibende über Privatsphärerisiken auf ihrer Webseite informieren.	Bewusstsein schaffen, dass ein Privatsphärerisiko auf der Webseite besteht. Auf die Nennung von Strafen verzichten, um Stress zu vermeiden.	Sollte Verantwortlichkeit der Webseitenbetreibenden verdeutlichen, jedoch auf Strafen verzichten, um Reaktanz zu vermeiden.	Kann auf rechtliche Konsequenzen Bezug nehmen inkl. Nennung von Strafen, um Priorisierung des Problems bei Entscheidungstragenden zu fördern.
Bewusstsein für Privatsphärerisiken	Prüftools	Webseitenbetreibenden die Möglichkeit geben selbst ihre Webseite auf spezifische Privatsphärerisiken zu überprüfen.	Konkret Privatsphärerisiko aufzeigen und Konsequenzen erklären.	Sollte speziell auf die, für Webseitenbetreibende relevanten, Aspekte fokussieren, z. B. Risiken fehlender Rechtskonformität.	Kann als zahlungspflichtiger Dienst angeboten werden, der Rechtskonformität der Webseite prüft.
Fähigkeit	Training	Technisches und rechtliches Wissen zu Privatsphäre vermitteln	Sollte kostengünstig sein, z. B. in Form von Videos oder Podcasts, die online zugänglich sind; einfach verständlich auch für technische Laien.	Sollte so wenig zusätzliche Arbeit wie möglich bereiten; könnte z. B. in bestehende Schulungen integriert.	Kann verschiedene Stakeholder adressieren, z. B. Ausbildung von Datenschutzbeauftragten zur Stärkung der Privatsphärekultur im Unternehmen.
Bewusstsein für Privatsphärerisiken, Fähigkeit, Zeit	Checklisten/ Richtlinien	Checklisten (was berücksichtigt werden sollte) und Richtlinien (wie dies umgesetzt werden kann) zur Verfügung stellen.	Sollte detailliert und gut für Personen mit geringem technischen Wissen verständlich sein.	Sollte kurz und einfach verständlich für Menschen mit wenig Zeit sein.	Kann technische Begriffe und Spezialfälle beinhalten, die relevant für komplexe Webseiten sind.

Abbildung 8. Maßnahmen für verschiedene Webseitenbetreibende. Die Abbildung orientiert sich an der Darstellung von Stöver et al. (2023).

3.3.12 Mögliche Auswirkungen der Datensatzwahl

Der Datensatz, der als Ausgangslage für die thematische Analyse diente, besteht aus realen Antworten von Webseitenbetreibenden zu einem bestimmten Problem (fehlende IP-Anonymisierung von Google Analytics). Die Wahl des Datensatzes ermöglicht völlig neue Einblicke, gleichzeitig könnte sie sich auf die in der thematischen Analyse aufgedeckten Themen ausgewirkt haben. Dieser mögliche Einfluss wird im Folgenden diskutiert.

Da der Datensatz sich auf einen bestimmten Anwendungsfall bezieht, haben vermutlich einige Themen, die aus der thematischen Analyse hervorgegangen sind, einen spezifischen Fokus. Aus diesem Grund sind die Themen möglicherweise nicht vollständig: Für andere Anwendungsfälle könnten sich zusätzliche Herausforderungen wie fehlende technische Lösungen ergeben. Zum Beispiel gibt es möglicherweise keine datenschutzfreundlichen Vorlagen für Cookie-Einwilligungserklärungen oder es entstehen zusätzliche Kosten für die Anonymisierung, z. B. wenn die von der datenschutzverletzenden Lösung erfassten Daten für die Webseitenbetreibenden wertvoller sind als in diesem Anwendungsfall.

Möglicherweise haben die Teilnehmenden nur deshalb geantwortet und sich erklärt, weil sie zunächst nicht wussten, was die eigentliche Intention der Benachrichtigungen war, nämlich die Datenerhebung für eine wissenschaftliche Studie, und möglicherweise hofften sie, durch eine Erklärung rechtliche Konsequenzen zu vermeiden oder die Verantwortung auf andere, z. B. einen externen Dienstleister, abzuwälzen. Aufgrund des rechtlichen oder offiziellen Rahmens der Benachrichtigung könnte es also sein, dass mehr Webseitenbetreibende die Implementierung der IP-Anonymisierung delegiert haben als in einem Umfeld, in dem informellere Meldungen verschickt worden wären. In diesem Fall hätten vielleicht mehr Webseitenbetreibende eine Antwort auf das Problem ignoriert oder verzögert.

Der Datensatz enthält etwas mehr Antworten von Webseitenbetreibenden, die per Brief benachrichtigt wurden, als von Teilnehmenden, die eine E-Mail erhalten haben. Die Anzahl der Antworten variiert auch zwischen den verschiedenen Argumenten. Webseitenbetreibende, die darüber informiert wurden, dass es sich bei dem Problem auf ihrer Webseite um einen Compliance-Verstoß handelt, der eine Strafgebühr nach sich ziehen kann, meldeten sich am häufigsten zurück. In dem Datensatz, der als Grundlage für die thematische Analyse diente, sind daher Antworten von Webseitenbetreibenden, die einen potenziell beängstigenden Hinweis mit besonderer Gewichtung (durch das Medium Brief) erhalten haben, überrepräsentiert. Aufgrund der rechtlichen Komponente haben sich die Webseitenbetreibenden möglicherweise häufiger an ihre Rechtsabteilung oder ihren Anwalt gewandt, während bei einem anderen, z. B. eher technischen Fokus vielleicht mehr Webseitenbetreibende ihre IT-Abteilung oder ihren Administrator um eine Lösung des Problems gebeten hätten. Die unterschiedlichen Benachrichtigungen können also tatsächlich unterschiedliche Reaktionen der Webseitenbetreibenden auslösen. Sie eröffneten außerdem einen größeren Möglichkeitsraum für Reaktionen als die Fokussierung auf eine einzige Art von Benachrichtigung, z. B. auf eine E-Mail ohne rechtliche Argumente. Der Datensatz bietet somit eine gute Grundlage für eine qualitative explorative Analyse, wie sie für diese Arbeit durchgeführt wurde. Es ist davon auszugehen, dass die verschiedenen Benachrichtigungen auch solche Webseitenbetreibenden erreichen könnten, die in früheren Studien nicht berücksichtigt wurden. So hätten sich z. B. die vielbeschäftigten Selbstständigen nicht die Zeit genommen, an einer Umfrage teilzunehmen oder auf eine eher nicht offiziell aussehende Meldung zu antworten.
Nicht zuletzt könnte es auch andere oder mehr Personas geben, die von der Autorin dieser Arbeit nicht aufgedeckt wurden, weil entsprechende Webseitenbetreibende sich nicht gemeldet haben, z. B. Fachleute, die das Problem nicht auf ihrer Webseite hatten oder es schnell selbst lösen konnten.

3.3.13 Limitationen

Die drei Studien weisen alle eine potenzielle Selbstselektion auf, die zur Verzerrung der Ergebnisse führen. Bei dem Feldexperiment ist die Gruppenzuordnung betroffen. Bei 87 der Webseitenbetreibenden war nur eine E-Mail-Adresse und bei 152 nur eine Postanschrift im Impressum angegeben, sodass diese der entsprechenden Gruppe zugeordnet werden mussten. Bei der Umfrage ist davon auszugehen, dass nur Webseitenbetreibende, die ein gewisses Maß an Vertrauen in die Benachrichtigung und die folgende Aufklärung hatten, daran teilgenommen haben. Auch ist davon auszugehen, dass die Umfrage besonders vielbeschäftige Webseitenbetreibende sowie Webseitenbetreibende, die keine Unternehmensinformationen weitergeben wollen oder dürfen, nicht erreicht hat. Auch bei den Rückmeldungen auf die Benachrichtigungen ist von einer Selbstselektion auszugehen. Möglicherweise haben die Teilnehmenden nur deshalb geantwortet und sich erklärt, weil sie zunächst nicht wussten, was die eigentliche Intention der Benachrichtigung war, nämlich die Datenerhebung für eine wissenschaftliche Studie, und möglicherweise hofften sie, durch eine Erklärung rechtliche Konsequenzen zu vermeiden oder die Verantwortung auf andere, z. B. einen externen Dienstleister, abzuwälzen. Aufgrund des rechtlichen oder offiziellen Rahmens der Meldungen könnte es also sein, dass mehr Webseitenbetreibende die Implementierung der IP-Anonymisierung delegiert haben als in einem Umfeld, in dem informellere Meldungen verschickt worden wären. In diesem Fall hätten vielleicht mehr Webseitenbetreibende eine Antwort auf das Problem ignoriert oder verzögert.

3.4 Zwischenfazit

Einem explorativen und qualitativen Ansatz folgend wurde die Perspektive von Webseitenbetreibenden auf ein bestehendes Privatsphärerisiko auf ihrer Webseite untersucht. Die Ergebnisse zeigen, dass zu den Ursachen mangelndes Bewusstsein und fehlerhafte Implementierungen zählen. Webseitenbetreibende müssen besondere Hürden bewältigen, wenn sie ein Datenschutzproblem angehen, z. B. mangelndes technisches Wissen oder zähe Organisationsstrukturen. Mit welchen Hürden die Webseitenbetreibenden konfrontiert sind und wie sie diese bewältigen, hängt jedoch stark von dem Kontext ab, in dem sie die Webseite betreiben. Bei der Entwicklung von Maßnahmen zur Unterstützung von Webseitenbetreibenden in Datenschutzfragen müssen deren unterschiedliche Kontexte und die daraus resultierenden Bedürfnisse berücksichtigt werden. Die Analysen zeigen, dass sich Webseitenbetreibende von anderen Personen, die Systeme betreiben und entwickeln, unterscheiden können. Daher ist zu schlussfolgern, dass in der S&P-Forschung speziell auf die Perspektive dieser noch nicht ausreichend erforschten Gruppe eingegangen werden sollte.

Die Ergebnisse der Untersuchungen liefern Erkenntnisse dazu, was die Ursachen für bestehende datenschutzrechtlich relevante Privatsphärerisiken auf Webseiten sind, wie Webseitenbetreibende beim Beheben vorgehen, welche Herausforderungen sie dabei überwinden müssen und wie sie effektiv unterstützt werden können. Hierbei lag der Fokus jedoch primär auf der Behebung von datenschutzrechtlich relevanten bestehenden Privatsphärerisiken auf bereits existierenden Webseiten. Täglich werden jedoch neue Webseiten online gestellt oder Webseitenbetreibende erweitern ihre bestehenden Webseiten mithilfe der Dienste von Drittanbietern (Utz et al., 2022). Wie bereits aufgeführt, greifen Personen, die Webseiten erstellen, bei der Auswahl von Drittanbieterdiensten häufig auf Standardlösungen zurück und berücksichtigen privatsphärerelavante Aspekte selten und primär, wenn es rechtliche Anforderungen gibt (Utz et al., 2022). Im Umkehrschluss kann diese Erkenntnis bedeuten, dass Webseitenbetreibende die Lösungen von Drittanbietern übernehmen, die möglicherweise ein primäres Interesse an Nutzendendaten haben und ihre Lösungen entsprechend wenig privatsphärefreundlich gestalten. Unklar ist jedoch, inwiefern die Gestaltung dieser Standardlösungen hinsichtlich Privatsphäreaspekten den Interessen und Vorstellungen der Webseitenbetreibenden entspricht. Während sich der erste Teil der Arbeit (Kapitel 3) auf ein bestehendes Privatsphärerisiko auf Webseiten fokussiert, liegt der Fokus im zweiten Teil der Arbeit (Kapitel 4) darauf, wie Privatsphärerisiken verhindert werden können. Dazu wird die Perspektive der Webseitenbetreibenden im Moment der Auswahl von Webseitenelementen beleuchtet, die potenziell Privatsphärerisiken für Nutzende beinhalten. Konkret geht es um die Auswahl von Cookie-Einwilligungserklärungen, die so gestaltet sind, dass sie ein Privatsphärerisiko für die Nutzenden darstellen.

4 Herausforderung 2: Entstehung von Privatsphärerisiken vermeiden – Untersucht am Beispiel der Vermeidung von Deceptive Designs bei der Erstellung von Cookie-Einwilligungserklärungen

Im vorherigen Kapitel ging es um die Herausforderung von Webseitenbetreibenden, bestehende Privatsphärerisiken wie die fehlende IP-Anonymisierung von Google Analytics zu beheben. Dieses Kapitel ist der Herausforderung von Webseitenbetreibenden gewidmet, die Entstehung von Privatsphärerisiken zu vermeiden. Diese Herausforderung wird am Beispiel der Erstellung von Cookie-Einwilligungserklärungen untersucht.

4.1 Motivation und Überblick

Webseitenbetreibende sind in der Regel dazu verpflichtet, die Einwilligung der Nutzenden einzuholen, wenn sie auf ihrer Webseite personenbezogene Daten erheben und/oder nicht zwingend notwendige Cookies setzen wollen. Um diese Einwilligung einzuholen, greifen Webseitenbetreibende auf sogenannte Cookie-Einwilligungserklärungen zurück. Je nach Gestaltungsform unterstützen diese die Nutzenden eher mehr oder eher weniger dabei, ihre Privatsphäre zu schützen. Enthalten diese Einwilligungserklärungen z. B. Gestaltungselemente, die Nutzende eher dazu bewegen, ihre Zustimmung zum Setzen von Cookies zu geben (z. B. durch die farbliche Hervorhebung von entsprechenden Buttons), kann das die Privatsphäre der Nutzenden einschränken. Diese Gestaltungselemente, die ein Privatsphärerisiko für die Nutzenden darstellen, werden auch *Deceptive Designs* genannt. Webseitenbetreibende haben es in der Hand, dieses Privatsphärerisiko durch die bewusste Gestaltung solcher Erklärungen zu vermeiden. Bisher ist jedoch ungeklärt, welche Aspekte Webseitenbetreibende bei der Gestaltung bzw. Erstellung von Cookie-Einwilligungserklärungen berücksichtigen und inwiefern es in ihrem Interesse ist, an dieser Stelle Privatsphärerisiken für Nutzende zu vermeiden. Dies soll mit dem folgenden Ziel adressiert werden:

Ziel 3: Entwicklung eines besseren Verständnisses für die Herausforderung für Webseitenbetreibende, die Entstehung von Privatsphärerisiken auf ihren Webseiten zu vermeiden. Untersucht am Beispiel der Gestaltung von Cookie-Einwilligungserklärungen.

Auch im Fall der Vermeidung von Privatsphärerisiken stellt sich die Frage, wie Webseitenbetreibende dabei unterstützt werden können. Deshalb lautet das nächste Ziel:

Ziel 4: Erarbeitung von Maßnahmen zur Unterstützung von Webseitenbetreibenden bei der Vermeidung von Privatsphärerisiken auf ihren Webseiten. Untersucht an den Beispielen (a) der Bereitstellung von Informationen bei der Auswahl von Einwilligungserklärungen sowie (b) der Gestaltungsmöglichkeiten von Einwilligungserklärungen mithilfe von CMP-Vorlagen.

Zur Bearbeitung der Ziele 3 und 4 werden in diesem Kapitel zwei Studien vorgestellt. In Studie 2a wird zunächst die Nutzendenperspektive auf verschiedene Gestaltungsoptionen von Cookie-Einwilligungserklärungen untersucht. Die Ergebnisse dienen als Grundlage für Studie 2b, in der die Perspektive der Webseitenbetreibenden, auch im Vergleich zur Nutzendenperspektive, auf die

verschiedenen Gestaltungsoptionen untersucht wird. In Studie 3 werden die Vorlagen für Cookie-Einwilligungserklärungen von CMPs im Hinblick darauf analysiert, inwiefern sie den Webseitenbetreibenden die Möglichkeit bieten, Cookie-Einwilligungserklärungen ohne *Deceptive Designs* zu entwickeln.

In Abbildung 9 wird ein Überblick über Kapitel 4 gegeben. Im Folgenden werden zunächst die theoretischen Grundlagen sowie die bisherige Forschung, die für dieses Kapitel relevant ist, vorgestellt. Dazu zählt eine Einführung in das Thema der *Deceptive Designs* sowie der *Deceptive Designs* in Cookie-Einwilligungserklärungen. In einem Exkurs wird die Rolle der CMPs erläutert und im Anschluss wird die bisherige Forschung zu *Deceptive Designs* in Cookie-Einwilligungserklärungen, die mit CMPs erstellt wurden, zusammengefasst. Abschließend wird das Nudging als mögliche Maßnahme zur Beeinflussung von privatsphärerelevanten Entscheidungen vorgestellt. In den weiteren Unterkapiteln werden die Studien 2a und 2b sowie Studie 3 beschrieben – jeweils bestehend aus Erläuterungen zur Methode, der Darstellung der Ergebnisse, einer Diskussion und dem Aufzeigen der Limitationen der Studien.

Kapitel 4: Untersuchung Herausforderung 2: Entstehung von Privatsphärerisiken vermeiden
– Untersucht am Beispiel der Erstellung von Cookie-Einwilligungserklärungen.
Forschungsziele 3 & 4

Studie 2a	Online Experiment + Umfrage ($N = 376$)
Studie 2b	Online Experiment + Umfrage ($N = 195$)
Studie 3	Analyse von Vorlagen ($N = 15$)

Abbildung 9. Überblick über Kapitel 4.

4.2 Theoretische Grundlagen und bisherige Forschung

In diesem Unterkapitel werden die theoretischen Grundlagen sowie die bisherige Forschung, die für die Studien in Kapitel 4 relevant ist, vorgestellt. Dazu wird zunächst beschrieben, was *Deceptive Designs* sind und welche Rolle sie in Cookie-Einwilligungserklärungen spielen. Des Weiteren wird die Rolle von CMPs vorgestellt und der aktuelle Forschungsstand zu *Deceptive Designs* in Einwilligungserklärungen von CMPs zusammengefasst. Abschließend wird das Nudging als eine mögliche Maßnahme, um das Entscheidungsverhalten von Webseitenbetreibenden bei der Auswahl von Cookie-Einwilligungserklärungen zu beeinflussen, vorgestellt.

4.2.1 Deceptive Designs

Deceptive Designs oder *Dark Patterns* sind laut Brignull (Brignull, o. J.) Tricks auf Webseiten oder in Apps, die die Nutzenden dazu verleiten, Dinge zu tun, die sie nicht beabsichtigen, z. B. etwas zu kaufen oder sich anzumelden. Mathur et al. (2019, S. 81) definieren *Deceptive Designs* als „*Designentscheidungen für Benutzeroberflächen, die einen Online-Dienst begünstigen, indem sie Nutzende zu unbeabsichtigten und potenziell schädlichen Entscheidungen zwingen, lenken oder täuschen*“. In der bisherigen Forschung wurden bereits zahlreiche *Deceptive-Design*-Strategien identifiziert (Mathur et al., 2021). Eine Taxonomie von verschiedenen Strategien, die bereits im Kontext von Cookie-Einwilligungserklärungen

untersucht wurden (Soe et al., 2020), stammt von Gray et al. (2018). Sie leiten insgesamt fünf *Deceptive-Design*-Strategien aus der Literatur ab, die in
Tabelle 2 aufgeführt sind. Ausgehend von diesen Strategien wurden für diese Arbeit Definitionen für den Kontext von Cookie-Einwilligungserklärungen abgeleitet, die die Grundlage für die Studien dieses Kapitels bilden.

Tabelle 2. Die Tabelle gibt einen Überblick über die fünf von Gray abgeleiteten Strategien für *Deceptive Designs* mit den entsprechenden Definitionen von Gray sowie den Definitionen, die für den Kontext der Cookie-Einwilligungserklärungen angepasst wurden.

Deceptive-Design-Strategien	Definition nach Gray	Definition angepasst für Cookie-Einwilligungserklärungen
Interface Interference (dt. Störung der Benutzeroberfläche)	Manipulation der Benutzeroberfläche, die bestimmte Aktionen gegenüber anderen bevorzugt (Gray, S. 5).	Die Gestaltung (Farbe, Schriftart, Größe) der Buttons für das Akzeptieren und Ablehnen von Cookies ist nicht gleichwertig.
Obstruction (dt. Hindernis)	Erschweren eines Prozesses über das notwendige Maß hinaus mit der Absicht, bestimmte Handlungen abzuschrecken.	Die Option, alle Cookies abzulehnen, ist auf der ersten Seite des Hinweises nicht verfügbar.
Forced Action (dt. erzwungene Handlung)	Die Nutzenden müssen eine bestimmte Aktion ausführen, um auf eine bestimmte Funktion zugreifen zu können (oder dies weiterhin zu können).	Die Nutzenden können die Webseite erst dann betreten, wenn sie auf den Hinweis reagiert haben.
Sneaking (dt. heimlich, schleichend)	Der Versuch, Informationen zu verbergen, zu verschleiern oder zu verzögern, die für die Nutzenden relevant sind.	Nutzende stimmen unwissentlich Cookies zu (z. B. weil die Einwilligungserklärung ein Opt-out vorsieht).
Nagging (dt. nörgelnd)	Umleitung der erwarteten Funktionalität, die über eine oder mehrere Interaktionen hinaus bestehen bleibt.	Nach ihrer Entscheidung werden die Nutzenden erneut durch einen Hinweis gefragt, ob sie bei ihrer Entscheidung bleiben wollen.

4.2.2 Deceptive Designs in Cookie-Einwilligungserklärungen

Deceptive Designs in Cookie-Einwilligungserklärungen bedeuten, dass z. B. Buttons, die Struktur und Beschriftungen absichtlich so gestaltet sind, dass sie Nutzende eher zur Zustimmung verleiten und diese damit potenziell gegen ihre eigenen Interessen handeln (Süddeutsche Zeitung, o. J.). Dazu gehört, dass die Ablehnung der Cookie-Nutzung schwieriger ist als die Akzeptanz (*Obstruction*), z. B. durch das Verstecken des Ablehnen-Buttons auf einer tieferen Ebene (Mager & Kranz, 2021; Nouwens et al., 2020) oder dadurch, dass der Akzeptieren-Button prominenter angezeigt wird als der Ablehnen-Button (*Interface Interference*), z. B. durch farbliche Hervorhebung (Machuletz & Böhme, 2020; Utz et al., 2019). Ein Beispiel für eine Cookie-Einwilligungserklärung mit mehreren *Deceptive Designs*, das aus der Praxis stammt, findet sich in Abbildung 10.

In mehreren Studien wurde die Prävalenz von *Deceptive Designs* in Cookie-Einwilligungserklärungen auf EU-Webseiten untersucht und es wurde gezeigt, dass *Obstruction* und *Interface Interference* die häufigsten *Deceptive Designs* darstellen (Kampanos & Shahandashti, 2021; Krisam et al., 2021; Soe et al., 2020). Soe et al. (2020) analysierten die Cookie-Einwilligungserklärungen von 300 skandinavischen und englischen Nachrichten-Webseiten in den Jahren 2019 und 2020 im Hinblick auf die von Gray et al. (2018) vorgeschlagenen *Deceptive Designs*. Ihre Analyse zeigt, dass die meisten Webseiten mindestens ein *Deceptive Design* in ihren Cookie-Einwilligungserklärungen verwenden, wobei *Obstruction* und *Interface Interference* die häufigsten sind. Diese sind auf fast der Hälfte der untersuchten Webseiten zu finden. Kampanos und Shahandashti (2021) analysierten mehr als 700 Cookie-Einwilligungserklärungen

von Webseiten in Griechenland und dem Vereinigten Königreich und fanden ebenfalls *Obstruction* und *Interface Interference* in den meisten Einwilligungserklärungen. Krisam et al. (2021) analysierten die Cookie-Einwilligungserklärungen der 500 beliebtesten deutschen Webseiten und fanden bei 85 % der untersuchten Webseiten *Interface Interference* und bei 78.5 % *Obstruction* in den Einwilligungserklärungen.

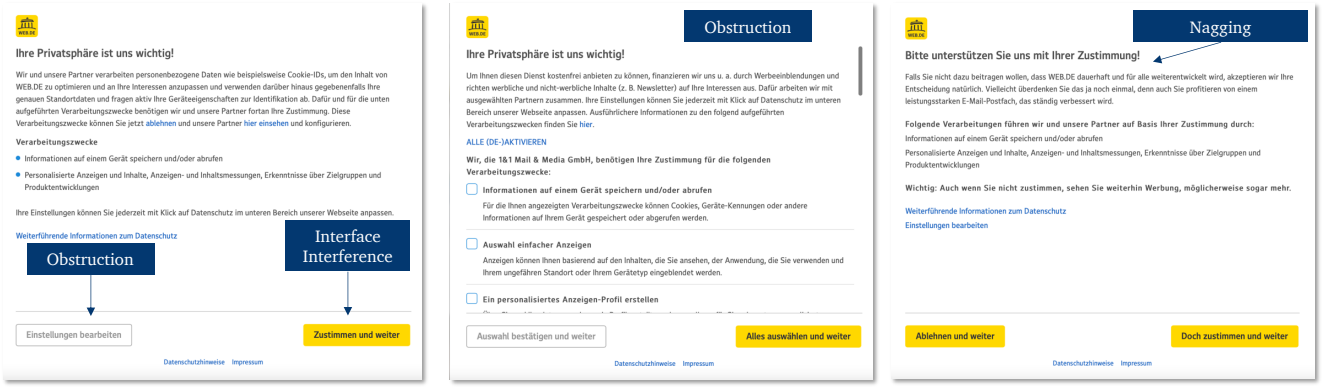


Abbildung 10. Beispiel für eine Cookie-Einwilligungserklärung aus der Praxis, die verschiedene *Deceptive Designs* enthält (*Web.de*, o. J.).

Frühere Untersuchungen deuten darauf hin, dass die Gestaltung von Cookie-Einwilligungserklärungen einen Einfluss auf das Ausmaß hat, in dem Nutzende der Verwendung von Cookies zustimmen (Bermejo Fernandez et al., 2021; Machuletz & Böhme, 2020; Mager & Kranz, 2021; Nouwens et al., 2020; Utz et al., 2019). Es hat sich wiederholt gezeigt, dass *Deceptive Designs* die Akzeptanz von Cookies erhöhen. Dennoch gibt es gemischte Ergebnisse hinsichtlich des Ausmaßes, in dem bestimmte *Deceptive Designs* die Reaktion der Nutzenden auf die Cookie-Zustimmung beeinflussen. Graßl et al. (2021), die ebenfalls die Wirkung von *Deceptive Designs* untersuchten, fanden beispielsweise keinen signifikanten Einfluss von *Obstruction* (in diesem Fall das Verstecken des Ablehnen-Buttons auf einer zweiten Ebene) und *Interface Interference* (in diesem Fall die farbliche Hervorhebung des Akzeptieren-Buttons) auf die Zustimmungsraten. Dies könnte darauf zurückzuführen sein, dass die meisten Teilnehmenden selbst in der Ausgangsbedingung der Verwendung von Cookies zustimmten. Graßl et al. (2021) kehrten in einer Untersuchung die *Deceptive Designs* um, um die Nutzenden dazu zu bewegen, die Verwendung von Cookies abzulehnen (sogenannte *Bright Patterns*). Dabei fanden sie signifikante Auswirkungen für *Obstruction*. In der vorliegenden Studie liegt der Fokus daher auf den *Deceptive Designs*, die am weitesten verbreitet und am leichtesten zu erkennen sind: *Obstruction* und *Interface Interference*.

4.2.3 Exkurs: Consent Management Platform

Für die Erstellung von Cookie-Einwilligungserklärungen für ihre Webseiten greifen Webseitenbetreibende zunehmend auf die Vorlagen von CMPs zurück. CMP „*bezeichnet das Unternehmen oder die Organisation, die die Transparenz für den Endnutzenden sowie dessen Zustimmung und Einwände zentralisiert und verwaltet*“ (IAB, o. J., S. 6). Für Webseitenbetreibende kann es vorteilhaft sein, auf die Vorlagen von CMPs zurückzugreifen, weil diese eine einfache Möglichkeit bieten, Einwilligungsklärungen zu erstellen, von denen Webseitenbetreibende sich erhoffen, rechtssicher zu sein. Auf der Grundlage von 161 Mio. Browser-Crawls schätzen Hils et al. (2020), dass sich der Einsatz

von CMPs zwischen Juni 2018 und Juni 2019 verdoppelt und bis Juni 2020 nochmals verdoppelt hat, wobei CMPs hauptsächlich auf mittelgroßen populären Webseiten verwendet wurden. Andere Studien konzentrierten sich darauf, inwiefern Cookie-Einwilligungserklärungen, die durch die Verwendung beliebter CMPs implementiert wurden, mit rechtlichen Anforderungen übereinstimmen und welche *Deceptive Designs* sie im Falle der Nichteinhaltung enthalten (Nouwens et al., 2020; Utz et al., 2019).

4.2.4 Deceptive Designs in Einwilligungserklärungen von Content Management Platforms

Nouwens et al. (2020) bewerteten die Gestaltung der am häufigsten verwendeten CMPs (Cookiebot, Crownpeak(Crownpeak Technology, Inc, o. J.), OneTrust, QuantCast, TrustArc) im Vereinigten Königreich im Hinblick auf die Anforderungen der DSGVO und die Datenschutzrichtlinien für elektronische Kommunikation (ePrivacy-Richtlinien), indem sie die Implementierungen der mit diesen CMPs erstellten Cookie-Einwilligungserklärungen auf den 10 000 meistbesuchten Webseiten im Vereinigten Königreich auswerteten. Sie fanden heraus, dass weniger als 12 % der untersuchten Cookie-Einwilligungserklärungen die von Nouwens et al. (2020) definierten Mindestanforderungen erfüllten, um den europäischen rechtlichen Anforderungen zu entsprechen: (1) Die Zustimmung muss explizit erteilt werden (z. B. durch Klicken auf einen Button, anstatt weiter auf der Webseite zu surfen), (2) das Akzeptieren aller Cookies muss genauso einfach sein wie das Ablehnen aller Cookies (z. B. muss sich der Alle-Ablehnen-Button auf derselben Ebene befinden wie der Alle-Akzeptieren-Button – ist das nicht erfüllt, stellt dies *Obstruction* nach Gray et al. (2018) dar) und (3) die Einwilligungserklärung darf keine bereits angekreuzten Kästchen enthalten (d. h. Opt-in statt Opt-out). Ihre Ergebnisse deuten darauf hin, dass Cookie-Einwilligungserklärungen die letzten beiden Anforderungen häufig nicht erfüllen, da der Alle-Ablehnen-Button häufig schwerer zugänglich ist als der Alle-Akzeptieren-Button und detaillierte Cookie-Einstellungen häufig auf einem Opt-out-Verfahren beruhen.

Degeling et al. (2019) analysierten 6579 der beliebtesten Webseiten in verschiedenen EU-Ländern in den Jahren 2017 und 2018 nach Inkrafttreten der DSGVO. Sie fanden heraus, dass die meisten der häufig verwendeten CMPs, wie ihre crawlingbasierte Analyse von EU-Webseiten zeigte, nicht die technischen Eigenschaften unterstützen, die erforderlich sind, um die DSGVO-Anforderungen für Cookie-Einwilligungserklärungen zu erfüllen. In dieser Studie wurde jedoch nicht die Prävalenz von *Deceptive Designs* bewertet, sondern der Schwerpunkt lag auf technischen Aspekten wie der Frage, ob Bibliotheken für die Cookie-Einwilligung (einschließlich CMPs) es ermöglichen, die Verwendung von Cookies abzulehnen oder die Einwilligung für verschiedene Cookie-Kategorien einzuholen (d. h. für Cookies, die für verschiedene Zwecke verwendet werden und die häufig mit der Erhebung unterschiedlicher Arten von Daten verbunden sind).

Bei einer genaueren Betrachtung einer zufällig ausgewählten Stichprobe von 1000 Webseiten aus ihrem ursprünglichen Satz in einer nachfolgenden Studie stellten Utz et al. (2019) fest, dass mehr als 57 % der Webseiten versuchten, die Nutzenden mithilfe von *Interface Interference* zur Cookie-Akzeptanz zu bewegen. Ihre Ergebnisse deuten ferner darauf hin, dass mehr als 95 % der Webseiten es nicht zulassen, die Cookie-Nutzung auf der ersten Ebene zu verweigern, was der *Obstruction*-Strategie nach der von Gray et al. (2018) vorgeschlagenen Definition des *Deceptive Designs* entspricht.

Matte et al. (2020) untersuchten 1426 Webseiten mit Cookie-Einwilligungserklärungen, die von CMPs implementiert wurden. Sie fanden zwar auf mehr als der Hälfte der Webseiten mindestens einen

Rechtsverstoß, sie analysierten die Cookie-Einwilligungserklärungen jedoch nicht im Hinblick auf die in der Studie betrachteten *Deceptive Designs*. In einer neueren Studie erweiterten Bollinger et al. (2022) diese Analyse, indem sie 30 000 Webseiten durchforsteten. Sie fanden in mehr als 90 % der analysierten Cookie-Einwilligungserklärungen datenschutzrechtliche Verstöße.
Nach Abschluss der CMP-Analysen im Rahmen der vorliegenden Arbeit wurde eine ähnliche und damit relevante Arbeit von Toth et al. (2022) veröffentlicht. In ihrer Arbeit untersuchten die Autor:innen die Konfigurationsprozesse von Cookie-Einwilligungserklärungen mithilfe von fünf bekannten CMP-Anbietern. Ihre Ergebnisse deuten darauf hin, dass die Standardvorlagen für Cookie-Einwilligungserklärungen oft nicht rechtskonform sind. Im Diskussionsteil dieses Kapitels werden die Parallelen zwischen Toth et al. (2022) und dieser Arbeit aufzeigt und die Ergebnisse verglichen.

4.2.5 Nudging als Maßnahme

Es stellt sich die Frage, ob und wie Webseitenbetreibende dazu bewegt werden können, Privatsphärerisiken bei der Erstellung von Cookie-Einwilligungserklärungen zu vermeiden.
Ein möglicher Ansatz könnte hier das sogenannte Nudging (dt. Stupsen) darstellen. Durch umfangreiche Forschung konnte bereits belegt werden, dass Menschen z. B. durch Formulierungen, Framing oder Farben in Richtung bestimmter, z. B. privatsphäreförderlicher Handlungen gestupst werden können (Acquisti et al., 2018). Tahaei et al. (2021a) nutzten Nudging, um Entwickler:innen dazu zu bewegen, privatsphärefreundlichere Entscheidungen zu treffen. Dazu führten sie ein Online-Experiment mit 400 Teilnehmenden durch, die Erfahrung in der Entwicklung mobiler Apps hatten. In einem hypothetischen Szenario wurden die Teilnehmenden gebeten, eine Reihe von Entscheidungen bezüglich der Integration von Werbung in eine fiktive App zu integrieren. Die wichtigste Entscheidung betraf die Wahl zwischen personalisierter und nicht personalisierter Werbung. Hier konnten die Autor:innen zeigen, dass Teilnehmende in der Bedingung, in der die Folgen der Anzeigenpersonalisierung für die Privatsphäre der Nutzenden hervorgehoben wurden, im Vergleich zur Kontrollgruppe signifikant häufiger (11.06-mal) nicht personalisierte Anzeigen wählten. Die Autor:innen kommen zu dem Schluss, dass Entwickler:innen in ihrer Arbeit von Benutzeroberflächen beeinflusst werden und transparente Entscheidungsoptionen benötigen.

4.3 Studie 2 – Untersuchung der Perspektive von Nutzenden und Webseitenbetreibenden auf verschiedene Cookie-Einwilligungserklärungen

Ziel der Studie 2 ist zum einen die Entwicklung eines besseren Verständnisses für die Herausforderung von Webseitenbetreibenden, die Entstehung von Privatsphärerisiken auf ihren Webseiten zu vermeiden (Ziel 3) und zum anderen, aufzuzeigen, wie Webseitenbetreibende dabei unterstützt werden können, die Entstehung von Privatsphärerisiken auf ihren Webseiten zu vermeiden (Ziel 4). Im folgenden Unterkapitel werden die Forschungsfragen, die sich aus diesen Zielen ergeben, hergeleitet und beschrieben.

4.3.1 Forschungsfragen

Im vorherigen Unterkapitel wurde aufzeigt, dass Webseitenbetreibende häufig Cookie-Einwilligungserklärungen mit *Deceptive Designs* verwenden. Die Ergebnisse aus Kapitel 3 deuten darauf hin, dass Webseitenbetreibende sich nicht immer den Privatsphärerisiken auf ihren Webseiten bewusst

sind und diese nicht zwangsläufig in ihrem Interesse sind, vor allem dann nicht, wenn diese einen datenschutzrechtlichen Verstoß darstellen. Auf den ersten Blick könnte es für Webseitenbetreibende vorteilhaft sein, die Nutzenden durch die Verwendung eines *Deceptive Designs* in Cookie-Einwilligungserklärungen dazu zu bewegen, alle Cookies zu akzeptieren, da die Sammlung von Statistiken und Werbedaten Teil ihres Geschäftsmodells sein könnte. Es könnte jedoch auch von Interesse sein, Vertrauen aufzubauen und positives Nutzendenfeedback auf der Webseite zu erhalten, indem die Verwendung von Cookies transparent dargestellt und eine informierte Entscheidung ermöglicht wird. Was Webseitenbetreibende über verschiedene Gestaltungsvarianten von Einwilligungserklärungen denken, ist noch ungeklärt. Deshalb widmet sich die nächste Forschungsfrage diesem Thema:

Forschungsfrage 4: Inwiefern spiegeln verschiedene Gestaltungen von Cookie-Einwilligungserklärungen die Interessen von Webseitenbetreibenden wider?

Weiterhin ist noch ungeklärt, inwiefern sich die Webseitenbetreibenden über die Präferenzen der Nutzenden bewusst sind und diese in ihren Entscheidungen bei der Auswahl von Cookie-Einwilligungserklärungen einbeziehen. Das soll mit der nächsten Forschungsfrage adressiert werden:

Forschungsfrage 5: Inwiefern sind sich Webseitenbetreibende über die Präferenzen der Nutzenden hinsichtlich der Gestaltung von Cookie-Einwilligungserklärungen bewusst und berücksichtigen diese?

Die bisherige Forschung, inklusive der Untersuchung aus Kapitel 3, deutet daraufhin, dass das Bewusstsein für Privatsphärerisiken unter Webseitenbetreibenden gering sein könnte (Utz et al., 2022). Deshalb liegt die Vermutung nahe, dass sich Webseitenbetreibende auch bei der Auswahl von Cookie-Einwilligungserklärungen nicht oder eingeschränkt darüber bewusst sind, dass diese potenziell so gestaltet sind, dass sie ein Privatsphärerisiko für Nutzende darstellen. In Kapitel 3 konnte bereits gezeigt werden, dass Benachrichtigungen eine effektive Maßnahme darstellen, um das Bewusstsein von Webseitenbetreibenden über bereits bestehende Privatsphärerisiken auf ihren Webseiten zu erhöhen.
Henning et al. (2022) wiesen Webseitenbetreibende ebenfalls mit Benachrichtigungen darauf hin, dass die auf ihrer Webseite eingesetzten Einwilligungserklärungen *Deceptive Designs* enthalten. Jedoch konnten sie nicht feststellen, dass die Webseitenbetreibenden die Einwilligungsklärungen nach der Benachrichtigung anpassten. In dem Fall waren Benachrichtigungen also keine effektive Maßnahme. Eine Erklärung sehen Henning et al. (2022) in den Ergebnissen der Umfrage, die sie im Anschluss durchführten. Einige Webseitenbetreibende beschrieben, dass sie keinen Einfluss auf die Gestaltung der bereits implementierten Einwilligungserklärungen haben. Auch stellen *Deceptive Designs* in Einwilligungsklärungen unter der aktuellen Rechtsprechung nur teilweise einen Rechtsverstoß dar. Das könnte ebenfalls die Motivation der Webseitenbetreibenden einschränken, Änderungen vorzunehmen, da anders als bei der in Kapitel 3 behandelten Fehlkonfiguration nicht zwangsläufig hohe Strafen zu befürchten sind.

Es stellt sich also die Frage, welche Möglichkeiten es gibt, um zu verhindern, dass Privatsphärerisiken überhaupt entstehen. Eine Möglichkeit besteht darin, beim Entscheidungsprozess der Webseitenbetreibenden für Webseitenelemente – in dem Fall bei der Erstellung der Cookie-Einwilligungserklärungen – anzusetzen. Wie bereits in Unterkapitel 4.2.5 erwähnt, konnten Tahaei et al. (2021a) in einem Online-Experiment mit App-Entwickler:innen zeigen, dass Teilnehmende durch die Bereitstellung von entsprechenden Informationen zur Auswahl privatsphärefreundlicherer Alternativen bewegt werden können. Dieser Ansatz könnte auch interessant sein, um eine bewusstere Entscheidung von Webseitenbetreibenden zu fördern. Damit beschäftigt sich die folgende Forschungsfrage:

Forschungsfrage 6: Inwiefern können Webseitenbetreibende durch Informationsbereitstellung dazu motiviert werden, Cookie-Einwilligungserklärungen ohne *Deceptive Designs* auszuwählen?

Im Folgenden wird die Methode der Studie vorgestellt, die zur Beantwortung der Forschungsfragen 4–6 dient. Die Studie besteht aus zwei Teilen (Studie 2a und 2b).

4.3.2 Methode der Studie 2a – Perspektive der Nutzenden

Studie 2a hatte zum Ziel, zunächst die Perspektive von Nutzenden auf verschiedene Gestaltungsvarianten von Cookie-Einwilligungserklärungen zu untersuchen. Die Erkenntnisse aus der Studie dienten als Grundlage für die Studie 2b, in der Webseitenbetreibenden diese Informationen zur Verfügung gestellt wurden. Außerdem konnte so abgeglichen werden, inwiefern die Webseitenbetreibenden die Präferenzen von Nutzenden kennen. Studie 2a wurde in Form eines Online-Experiments sowie einer Online-Umfrage durchgeführt.

Ablauf

Zu Beginn erhielten alle Teilnehmenden einen *Aufklärungsbogen* sowie eine Erklärung zum Datenschutz. Im weiteren Verlauf wurden die Teilnehmenden um *Demographischen Daten*, wie das Geschlecht, das Alter, den höchsten Bildungsabschluss, die aktuelle berufliche Tätigkeit sowie das Land, in dem sie aktuell wohnen, gebeten. Es folgte der *Fragebogen zur interaktionsbezogenen Technikaffinität (ATI)* mit insgesamt neun Items (Franke et al., 2019). Daraufhin wurden die Teilnehmenden in die *Coverstory* für das nun folgende Experiment eingeführt. Dazu erhielten sie die Information, dass sie einen Onlineshop für hochwertige Outdoor-Bekleidung besuchen und im Anschluss ihre Meinung dazu teilen sollten. Die Teilnehmenden sollten sich zudem die im Onlineshop angebotenen Produkte anschauen und sich das Produkt merken bzw. notieren, das sie am ehesten kaufen würden. Per Link wurden die Teilnehmenden auf den fiktiven Onlineshop weitergeleitet, wobei sie nichtwissend zufällig einer von vier Gruppen zugeteilt wurden (siehe Tabelle 3).

Tabelle 3. Zuteilung der Gruppen.

Versuchsgruppe	**Versuchsgruppe 1**	**Versuchsgruppe 2**	**Versuchsgruppe 3**	**Versuchsgruppe 4**
Angezeigte Einwilligungserklärung	Gestaltungsvariante 1 *– Deceptive Design* 1	Gestaltungsvariante 2 *– Deceptive Design* 2	Gestaltungsvariante 3 *– Balanced Design*	Gestaltungsvariante 4 *– Bright Design*

Entsprechend ihrer Gruppeneinteilung wurde den Teilnehmenden eine von vier Gestaltungsvarianten (siehe Abbildung 11 bis Abbildung 14) einer Cookie-Einwilligungserklärung beim Betreten des Onlineshops angezeigt.

Abbildung 11. Gestaltungsvariante 1 – *Deceptive Design* 1: In Gestaltungsvariante 1 war der Alles-Akzeptieren-Button farblich hervorgehoben (*Interface Interference*). Außerdem konnten Einstellungen erst auf der zweiten Seite vorgenommen werden (*Obstruction*). Wollten die Teilnehmenden nicht allen Cookies zustimmen, wurde ihnen eine dritte Seite anzeigt, auf der sie gebeten wurden, ihre Entscheidung zu überdenken (*Nagging*).

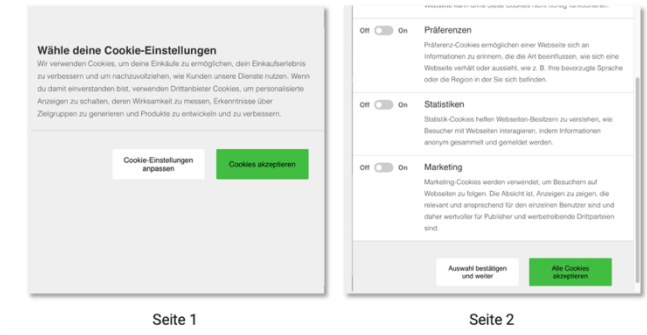


Abbildung 12. Gestaltungsvariante 2 – *Deceptive Design* 2: Gestaltungsvariante 2 enthielt analog zu Gestaltungsvariante 1 die *Deceptive Designs Interface Interference* sowie *Obstruction*, jedoch keine dritte Seite mit *Nagging*.

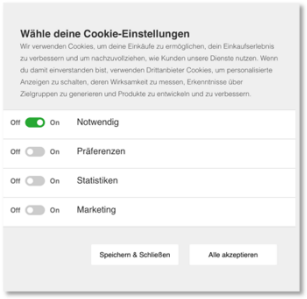


Abbildung 13. Gestaltungsvariante 3 – *Balanced Design*: Gestaltungsvariante 3 sollte keine *Deceptive Designs* enthalten und fungierte somit als ein *Balanced Design*.

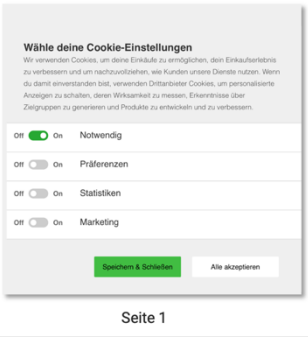


Abbildung 14. Gestaltungsvariante 4 – *Bright Design*: Angelehnt an Graßl et al. (2021) war in Gestaltungsvariante 4 der Alles-Ablehnen-Button farblich hervorgehoben.

Nach der Interaktion mit dem Onlineshop konnten die Teilnehmenden selbstständig zur Befragung zurückkehren bzw. wurden nach spätestens fünf Minuten automatisch dorthin zurückgeleitet. Im Rahmen weiterer Fragebogenfragen wurden die Teilnehmenden gebeten, anzugeben, welche(s) der Produkte aus dem Onlineshop sie am ehesten kaufen würden. Weiterhin wurden sie mithilfe des Standardized User Experience Percentile Rank Questionnaire (SUPR-Q) von Sauro et al. (2015) auf einer fünfstufigen Likert-Skala (1 – *stimme überhaupt nicht zu* bis 5 – *stimme voll und ganz zu*) zu ihrer Wahrnehmung des Onlineshops befragt. Der Fragebogen wurde ins Deutsche übersetzt und auf den Kontext der Studie angepasst. Mithilfe der Trust-Scale von Gulati et al. (2019) wurden die Teilnehmenden auf einer fünfstufigen Likert-Skala (1 – *stimme überhaupt nicht zu* bis 5 – *stimme voll und ganz zu*) zur Vertrauenswürdigkeit der Webseite bzw. den dahinterstehenden Webseitenbetreibenden befragt. Des Weiteren wurden die Teilnehmenden zu ihren Privatsphärebedenken bezüglich des Onlineshops mithilfe der siebenstufigen Likert-Skala (1 – *stimme überhaupt nicht zu* bis 7 – *stimme voll und ganz zu*) von Xu et al. (2011) befragt. Es folgte ein weiterer Fragenblock zur Wahrnehmung und Bewertung den im Onlineshop verwendeten Cookie-Einwilligungserklärungen. Darin wurden die Teilnehmenden zunächst gefragt, ob sie sich an eine Einwilligungserklärung erinnern konnten. Den Teilnehmenden, die sich erinnern konnten, wurden alle vier Gestaltungsvarianten der Einwilligungserklärung angezeigt und sie wurden gebeten, anzugeben, welche Variante ihnen im Onlineshop angezeigt wurde. Daraufhin wurden alle Teilnehmenden gebeten, die vier Gestaltungsvarianten auf einer siebenstufigen Likert-Skala (1 – *gefällt mir gar nicht* bis 7 – *gefällt mir sehr gut*) zu beurteilen. Der gesamte Fragebogen findet sich in Anhang B.

Experimentelles Design

Studie 2a inkludierte ein Online-Experiment mit einem Ein-Faktor-zwischen-Probanden-Design. Es gab eine unabhängige Variable mit vier Stufen. Die unabhängige Variable stellte die Cookie-Einwilligungserklärung dar, die den Teilnehmenden beim Betreten des Onlineshops angezeigt wurde. Diese konnte eine von vier Gestaltungsvarianten annehmen. Als abhängige Variablen wurden die Interaktion der Nutzenden (Zeit, Anzahl der Klicks) sowie ihre Bewertung des Onlineshops (UX, Vertrauen, Privatsphärebedenken bezüglich der Webseite) erfasst.

Datenerfassung

Der Fragebogen wurde auf der Onlineplattform Soscisurvey.de (Leiner, 2014) gehostet. Der fiktive Onlineshop wurde mithilfe einer lizenzfreien Vorlage aufgesetzt und auf OneDrive gehostet (Microsoft, 2007). Die Interaktionsdaten der Teilnehmenden mit der Cookie-Einwilligungserklärung sowie dem Onlineshop wurden erfasst und als JSON-String in Soscisurvey.de gespeichert.

Bereinigung und Auswertung der Daten

Die im JSON-Format gespeicherten Interaktionsdaten der Teilnehmenden wurden mithilfe eines Python-Skripts in CSV-Format konvertiert. Die Datenauswertung erfolgte mit SPSS (IBM, 2020). Insgesamt nahmen 518 Personen an der Studie teil. Im Zuge der Datenbereinigung wurden insgesamt 145 Personen ausgeschlossen, weil sie nicht die technischen Anforderungen erfüllten ($n = 6$), die Aufmerksamkeitsfragen nicht korrekt beantworteten ($n = 7$), keine sinnvollen Antworten im offenen Antwortfeld abgaben ($n = 3$), eine besonders kurze Bearbeitungszeit ($n = 6$) aufwiesen (M-(1.75*SD)), keine Interaktionsdaten mit dem Onlineshop gespeichert wurden ($n = 25$) bzw. die Interaktion mit dem Onlineshop bei 0 Millisekunden lag ($n = 19$) oder sie nicht mit dem Onlineshop interagierten ($n = 76$). Die finale Stichprobe bestand daher aus 376 Teilnehmenden. Für die Auswertung wurden sowohl deskriptivstatistische als auch inferenzstatistische Verfahren gerechnet. Die offenen Antworten wurden in Microsoft Excel ausgewertet (Microsoft, 2018).

Rekrutierung und Stichprobe

Die erforderliche Stichprobengröße wurde a priori mit G*Power berechnet (Buchner et al., 2014). Die optimale Stichprobengröße liegt bei 276 für die Berechnung einer ANOVA mit vier Gruppen mit Cohen's f = 0.25, Typ-I-Fehlerwahrscheinlichkeit $\alpha = .05$, Power 1-$\beta = .95$ (Walther, 2021).

Die Teilnehmenden wurden über die Plattform Clickworker mit einer in Deutschland lebenden Zufallsstichprobe rekrutiert (Clickworker GmbH, 2022). Im Durchschnitt brauchten die Teilnehmenden zwölf Minuten für die Studienteilnahme. Dafür erhielten sie 2.38 €, was einem Stundensatz von 11.90 € entspricht und damit über dem Mindestlohn von 9.82 € in Deutschland zum Zeitpunkt der Durchführung der Studie liegt.

Von der endgültigen Stichprobe ($N = 376$) identifizierten sich 155 Personen als Frauen, 217 als Männer, eine Person als andere und drei machten keine Angaben zu ihrem Geschlecht. Alle Teilnehmenden waren mindestens 18 Jahre alt, das Durchschnittsalter lag bei $M = 40.91$ ($SD = 13.00$). Was die Bildung betrifft, so hatten 200 Teilnehmende einen Schulabschluss und 160 einen Hochschulabschluss, eine Person einen anderen Abschluss, vier einen Meister und elf eine Promotion. Die Technikaffinität (ATI) der Stichprobe betrug $M = 3.90$ ($SD = 0.49$) von 6 Punkten. Die Datenschutzbedenken (IUIPC 8) der Stichprobe lagen bei $M = 5.64$ ($SD = 1.09$) für die Subskala Control, $M = 6.19$ ($SD = 0.99$) für die Subskala Awareness und $M = 5.21$ ($SD = 1.36$) für die Subskala Collection aus jeweils 7 Punkten.

4.3.3 Methode der Studie 2b – Perspektive der Webseitenbetreibenden

Nachdem in Studie 2a die Nutzendenperspektive auf verschiedene Gestaltungsvarianten von Cookie-Einwilligungserklärungen untersucht wurde, wurden die Ergebnisse als Grundlage für Studie 2b genutzt, in der die Perspektive der Webseitenbetreibenden untersucht wurde.

Ablauf

Zu Beginn erhielten alle Teilnehmenden einen *Aufklärungsbogen* sowie eine Erklärung zum Datenschutz. Es folgte ein Block mit Fragen zur Bewertung von verschiedenen Cookie-Einwilligungserklärungen. Dabei wurden alle Teilnehmenden gebeten, die vier Gestaltungsvarianten (siehe Abbildung 11 bis Abbildung 14) der Cookie-Einwilligungserklärungen auf einer siebenstufigen Likert-Skala (1 – *gefällt mir gar nicht* bis 7 – *gefällt mir sehr gut*) zu beurteilen. Daraufhin wurden die Teilnehmenden gebeten, die Gestaltungsoption auszuwählen, von der sie annehmen, dass sie Nutzenden von Webseiten am besten gefällt. Im weiteren Verlauf wurden die Teilnehmenden zufällig und nichtwissend einer von zwei Gruppen (Experimental- vs. Kontrollgruppe) zugeordnet. Entsprechend ihrer Gruppeneinteilung wurden ihnen nun erneut die vier Gestaltungsvarianten für Einwilligungserklärungen angezeigt. Die Experimentalgruppe enthielt zusätzlich zu den Gestaltungsvarianten Informationen über die Nutzendeninteraktion und -präferenz bezüglich der verschiedenen Varianten (siehe Abbildung 15). Die Teilnehmenden beider Gruppen wurden gebeten, auszuwählen, welche Gestaltungsvariante ihnen als Webseitenbetreibende am besten gefällt. Abschließend erhielten alle Teilnehmenden Fragen zu ihrer Demographie (Alter, Geschlecht) und zu ihrer Webseite. Dazu zählten Fragen nach der Art und dem Zweck der Webseite (offene Antworten), nach dem rechtlichen Rahmen, den monatlichen Seitenzugriffen, dem Einsatz von Cookies, den Einnahmen über Daten, die durch Cookies gesammelt werden, und die Frage, wer die aktuelle Einwilligungserklärung auf der Webseite gestaltet hat. Alle Teilnehmenden wurde nach Beendigung der Studie über deren Zweck aufgeklärt und erhielten, um der Kontrollgruppe keine Informationen vorzuenthalten, die Hintergrundinformationen zu den verschiedenen Gestaltungsvarianten. Der gesamte Fragebogen kann in Anhang C eingesehen werden.

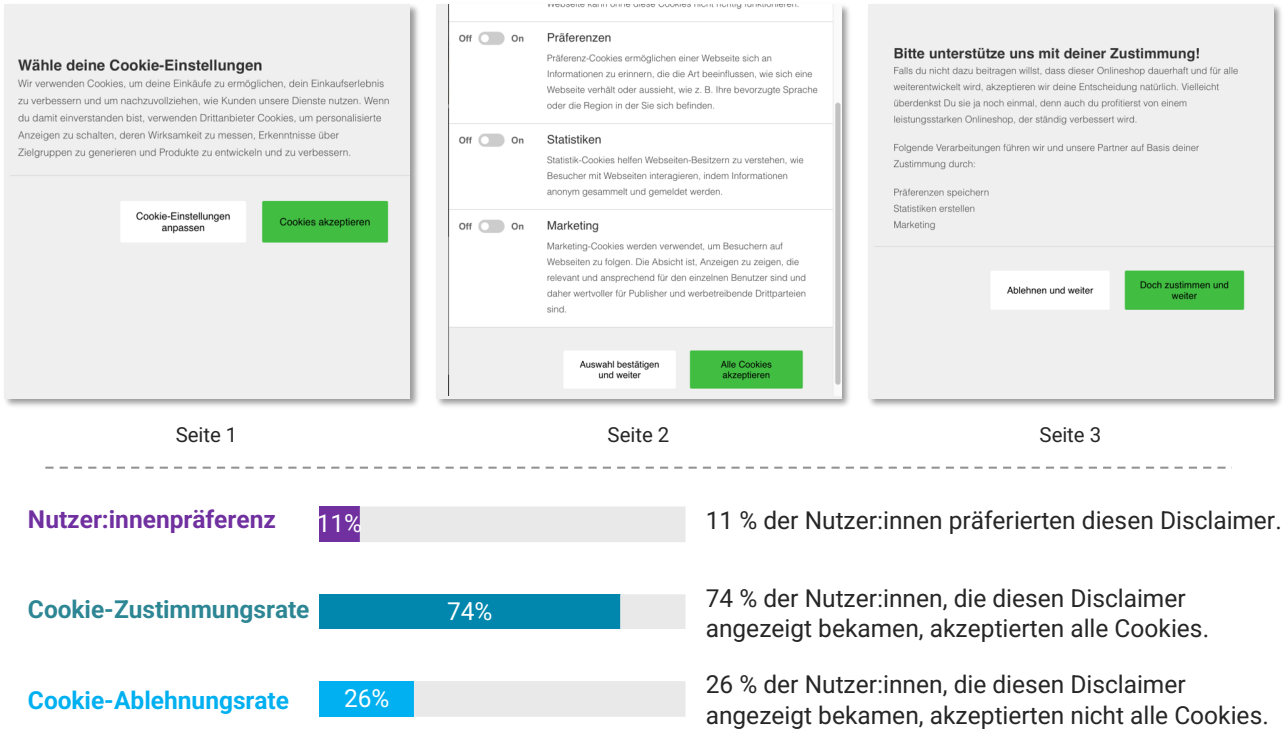


Abbildung 15. Beispiel für die Informationsbereitstellung.

Experimentelles Design

Im Rahmen von Studie 2b wurde ein Online-Experiment mit einem Zwei-Gruppen-Plan (Experimental- vs. Kontrollgruppe) durchgeführt. Die unabhängige Variable stellte die Informationsbereitstellung bei der Auswahl der Gestaltungsvarianten dar, wobei der Experimentalgruppe Informationen angezeigt wurde, während die Kontrollgruppe diese nicht sah. Als abhängige Variable wurde gemessen, welche der vier Gestaltungsvarianten die Teilnehmenden auswählten.

Erfassung, Bereinigung und Auswertung der Daten

Der Fragebogen wurde auf der Onlineplattform Soscisurvey.de gehostet (Leiner, 2014). Insgesamt nahmen 220 Personen an der Studie teil. Davon wurden 21 ausgeschlossen, deren Datensätze keine Antworten enthielten. Datensätze von vier weiteren Personen wurden ausgeschlossen, weil sie keine sinnvollen Antworten enthielten. Der finale Datensatz, der die Grundlage für die Auswertung bildete, bestand aus 195 Einträgen. Deskriptivstatistische und inferenzstatistische Verfahren wurden mit SPSS (IBM, 2020) berechnet, die offenen Antworten wurden mit Excel ausgewertet (Microsoft, 2018).

Rekrutierung und Stichprobe

Die Teilnehmenden wurden sowohl per E-Mail-Listen als auch über die Rekrutierungsplattform Clickworker rekrutiert, wobei die finale Stichprobe zu 51.3 % aus selbst rekrutierten und zu 48.7 % aus durch Clickworker rekrutierten Teilnehmenden bestand (Clickworker GmbH, 2022).

Insgesamt nahmen 220 Personen an der Studie teil. Im Zuge der Datenbereinigung wurden 21 leere Datensätze entfernt und 4 weitere Personen, die keine sinnvollen offenen Antworten gaben, ausgeschlossen. Die finale Stichprobe bestand aus 195 Teilnehmenden. Davon gehörten 87 Teilnehmende der Versuchsgruppe 1, 99 der Versuchsgruppe 2, 97 der Versuchsgruppe 3 und 93 der Versuchsgruppe 4 an.

Von der endgültigen Stichprobe ($N = 195$) identifizierten sich 57 Personen als Frauen, 120 als Männer, eine Person als andere und 17 machten keine Angaben zu ihrem Geschlecht. Alle Teilnehmenden waren mindestens 18 Jahre alt. Insgesamt 19 Personen waren zwischen 18 und 24 Jahren alt, 53 zwischen 25 und 34, 63 zwischen 35 und 49, 36 zwischen 50 und 64 und 7 Personen waren älter als 64. 17 Personen machten keine Angaben zum Alter.

4.3.4 Ethische Überlegungen

Die Studie folgt den Richtlinien der Ethikkommission der TU Darmstadt sowie der Universität Glasgow. Da die Studie im Rahmen einer Kooperation mit Forschenden der Universität Glasgow durchgeführt wurde, wurde bei der dortigen Ethikkommission ein Ethikantrag eingereicht. Dieser erhielt ein positives Votum. Um die Privatsphäre der Teilnehmenden zu schützen, wurde die Erhebung personenbezogener Daten auf ein Mindestmaß beschränkt. Vor Beginn der Studie erhielten alle Teilnehmenden eine Einverständniserklärung (mit Datenschutzbestimmungen), der sie zustimmen mussten. Alle Teilnehmenden wurden darüber informiert, dass sie jederzeit ohne negative Folgen aus der Studie aussteigen können und in diesem Fall alle ihre Daten gelöscht werden würden. Des Weiteren wurde sichergestellt, dass die Daten der Studienteilnehmenden nur von Mitgliedern der beteiligten

Forschungsgruppen eingesehen und bearbeitet werden können, worüber die Teilnehmenden informiert wurden. Außerdem wurden allen Teilnehmenden die Kontaktdaten der Forschenden sowie der Datenschutzbeauftragten der beteiligten Institutionen zur Verfügung gestellt, sodass sie sich auch nach Abschluss der Studie an diese wenden konnten. Die Umfragedaten wurden nur auf deutschen Servern gespeichert, die DSGVO-konform sind. Um Priming-Effekte zu vermeiden, erhielten Teilnehmende der Studie 2a eine Coverstory. Bei der Entscheidung für die Coverstory wurde der erwartete Nutzen sorgfältig gegenüber potenziellen Nachteilen für die Studienteilnehmenden abgewogen. Nach Beendigung der Studie oder bei Abbruch wurden alle Teilnehmenden über die Coverstory bzw. den tatsächlichen Zweck der Studie aufgeklärt. Als Teil des Experiments in Studie 2b erhielt nur die Versuchsgruppe zusätzliches Informationsmaterial zu den Cookie-Einwilligungserklärungen. Um einen möglichen Nachteil der Kontrollgruppe auszugleichen, erhielt auch die Kontrollgruppe nach Beendigung des Experiments die entsprechenden Informationen.

4.3.5 Ergebnisse der Studie 2a – Perspektive der Nutzenden

Ziel der Studie 2a war es, die Perspektive von Nutzenden auf verschiedene Gestaltungsvarianten von Cookie-Einwilligungserklärungen zu untersuchen. Dazu interagierten Teilnehmende im Rahmen eins Online-Experiments mit einer von vier Gestaltungsvarianten, die in einem fiktiven Onlineshop implementiert war. Im Anschluss wurden die Teilnehmenden zur Wahrnehmung des Onlineshops sowie der verwendeten Einwilligungserklärung befragt und gebeten, verschiedene Gestaltungsoptionen von Cookie-Einwilligungserklärungen zu bewerten. Im Folgenden werden die Ergebnisse vorgestellt.

Interaktion mit der Cookie-Einwilligungserklärung

Interaktionsdauer mit der Cookie-Einwilligungserklärung. Im Durchschnitt interagierten die Teilnehmenden $M = 7783.78$ ($SD = 12\,281.94$) Millisekunden (ms) mit der Einwilligungserklärung. Teilnehmende der Versuchsgruppe 1 ($M = 9359.10$; $SD = 10\,334.96$) interagierten am längsten mit der Einwilligungserklärung, gefolgt von Versuchsgruppe 3 ($M = 8442.87$; $SD = 16\,999.17$) und Versuchsgruppe 2 ($M = 7652.12$ $SD = 13\,587.23$). Teilnehmende der Versuchsgruppe 4 reagierten mit $M = 5762.87$ ($SD = 3142.55$) am kürzesten mit der Einwilligungserklärung. Um zu prüfen, ob sich die Interaktionsdauer zwischen den Teilnehmenden der verschiedenen Versuchsgruppen unterschied, wurde eine Welch-ANOVA durchgeführt.[8] Diese zeigt einen signifikanten Unterschied zwischen den Gruppen, $F(3,\ 170.80) = 4.22$, $p = .007$. Der Dunnett-T3-Post-Hoc-Test ergab, dass es lediglich zwischen Versuchsgruppe 1 (*Deceptive Design* 1) und Versuchsgruppe 4 (*Bright Design*) mit einer mittleren Differenz von 3596.23 ms einen Unterschied mit einer Signifikanz von $p = 0.14$ und Cohens $d = 0.471$ gibt.

Cookie-Zustimmungsrate. Bei der Interaktion mit der Einwilligungserklärung akzeptierten 48.9 % der Teilnehmenden alle Cookies. Wie in Abbildung 16 dargestellt, war die höchste Zustimmungsrate in Versuchsgruppe 1 (*Deceptive Design* 1) mit 77.0 % der Teilnehmenden, die alle Cookies akzeptierten, zu

[8] Es konnte keine ANOVA berechnet werden, da die Voraussetzungen für die Berechnung in den Daten nicht erfüllt waren. Es lag keine Normalverteilung der Daten vor. Außerdem enthielten die Daten viele Ausreißer.

verzeichnen. In Versuchsgruppe 2 (*Deceptive Design* 2) lag die Zustimmungsrate bei 71.7 %, in Versuchsgruppe 3 bei 30.9 % und in Versuchsgruppe 4 bei 17.2 %. Ein Chi-Quadrat-Test wurde zwischen der Versuchsgruppenzugehörigkeit und der Frage, ob alle Cookies akzeptiert wurden, durchgeführt. Keine erwarteten Zellhäufigkeiten waren kleiner als 5. Es gab einen statistisch signifikanten Zusammenhang zwischen der Zugehörigkeit der Versuchsgruppe und der Frage, ob alle Cookies akzeptiert wurden, $\chi^2(3) = 98.07$, $p < .001$, Cramer $V = .511$.

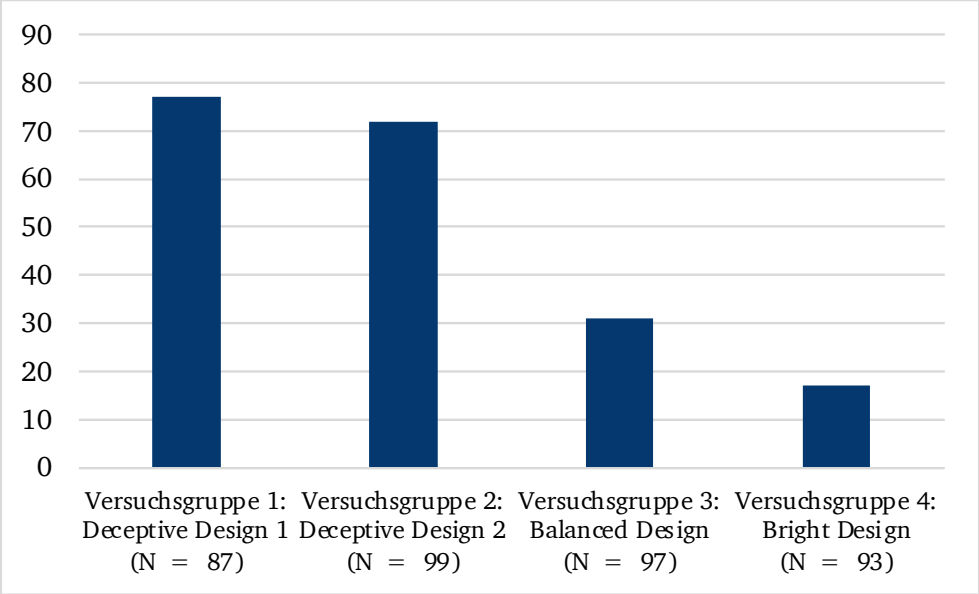


Abbildung 16. Anteil der Teilnehmenden in %, die alle Cookies akzeptiert haben, aufgeteilt nach Versuchsgruppen.

Bewertung der verschiedenen Gestaltungsvarianten

Die Mehrheit (57.7 %) der Teilnehmenden wählte als präferierte Cookie-Einwilligungserklärung die Gestaltungsvariante 4 (*Bright Design*) aus (siehe Abbildung 18). Diese wurde auf einer siebenstufigen Likert-Skala (1 – *gefällt mir gar nicht* bis 7 – *gefällt mir sehr gut*) mit $M = 5.35$ ($SD = 1.55$) am besten bewertet. Am seltensten (11.2 %) wurde die Gestaltungsvariante 1 (*Deceptive Design* 1) präferiert, die den Teilnehmenden mit $M = 3.57$ ($SD = 1.77$) im Durchschnitt am wenigsten gefiel.

Einfluss der Gestaltung der Cookie-Einwilligungserklärung auf die Nutzendeninteraktion mit dem Onlineshop

Im Folgenden wird die Interaktion der Teilnehmenden mit dem Onlineshop anhand der Variablen Zeit auf der Webseite, Anzahl der Klicks auf der Webseite sowie Anzahl der ausgewählten Produkte dargestellt. Um die Unterschiede zwischen den Versuchsgruppen bezüglich der Interaktion mit dem Onlineshop zu untersuchen, wurde für jede Variable eine Welch-ANOVA[9] durchgeführt und anschließend eine Bonferroni-Korrektur vorgenommen (Hemmerich, 2023).

[9] Es konnte keine ANOVA berechnet werden, da die Voraussetzungen für die Berechnung in den Daten nicht erfüllt waren. Es lag keine Normalverteilung der Daten vor. Außerdem enthielten die Daten viele Ausreißer.

Verweildauer auf dem Onlineshop. Die durchschnittliche Verweildauer der Teilnehmenden (in Millisekunden) auf dem Onlineshop lag bei $M = 123\,637.74$ ($SD = 73\,965.87$), wobei diese Zeitangabe nicht die Interaktion mit der Cookie-Einwilligungserklärung beinhaltet. Dabei verbrachten Teilnehmende der Versuchsgruppe 1 die längste Zeit auf dem Onlineshop ($M = 136\,532.92$; $SD = 76\,412.06$), gefolgt von Versuchsgruppe 4 ($M = 126\,300.29$; $SD = 74\,647.81$) und Versuchsgruppe 2 ($M = 117\,982.38$; $SD = 701\,114.29$). Die kürzeste Zeit verbrachten Teilnehmende der Versuchsgruppe 3 auf dem Onlineshop ($M = 115\,291.18$; $SD = 74\,302.23$). Die Welch-ANOVA ergab, dass die Unterschiede bezüglich der Verweildauer auf dem Onlineshop zwischen den Versuchsgruppen nicht signifikant sind $F(3, 205.18) = 1.48$, $p = .66$.

Anzahl der Klicks auf dem Onlineshop. Im Durschnitt machten die Teilnehmenden $M = 7.06$ ($SD = 5.23$) Klicks auf dem Onlineshop, wobei die Versuchsgruppe 1 mit $M = 7.75$ ($SD = 6.12$) am meisten Klicks tätigte, gefolgt von Gruppe 4 ($M = 7.43$; $SD = 4.91$) und Gruppe 3 ($M = 6.68$; $SD = 4.89$). Durchschnittlich am wenigsten Klicks tätigte Gruppe 2 ($M = 6.49$; $SD = 5.05$). Auch hier ergab die Welch-ANOVA keine signifikanten Unterschiede zwischen den Versuchsgruppen, $F(3, 203.90) = 1.15$, $p = .99$.

Anzahl der ausgewählten Produkte. Im Durschnitt wählten die Teilnehmenden $M = 1.07$ ($SD = 0.27$) Produkte im Onlineshop aus. Teilnehmende der Versuchsgruppe 4 wählten im Durschnitt am meisten Produkte aus ($M = 1.10$; $SD = 0.30$), gefolgt von Gruppe 3 ($M = 1.07$; $SD = 0.30$) und Gruppe 2 ($M = 1.06$; $SD = 0.28$). Am wenigsten Produkte wählte Gruppe 1 aus ($M = 1.05$; $SD = 0.21$). Auch hier ergab die Welch-ANOVA keine signifikanten Unterschiede zwischen den Versuchsgruppen $F(3, 205.87) = 0.61$, $p > .999$.

Einfluss der Gestaltung der Cookie-Einwilligungserklärungen auf die Nutzendenwahrnehmung des Onlineshops

Wie die Teilnehmenden den Onlineshop wahrnahmen, wurde anhand der Variablen wahrgenommene Vertrauenswürdigkeit des Onlineshops, User Experience des Onlineshops sowie Privatsphärebedenken bezüglich des Onlineshops erfasst. Die Vertrauenswürdigkeit wurde mithilfe der Trust-Scale von Gulati et al. (2019) auf einer fünfstufigen Likert-Skala (1 – *stimme überhaupt nicht zu* bis 5 – *stimme voll und ganz zu*) erfasst. Die *User Experience* wurde mithilfe des SUPR-Q von Sauro et al. (2015) auf einer fünfstufigen Likert-Skala (1 – *stimme überhaupt nicht zu* bis 5 – *stimme voll und ganz zu*) erfasst. Die Privatsphärebedenken wurden mithilfe der siebenstufigen Likert-Skala (1 – *stimme überhaupt nicht zu* bis 7 – *stimme voll und ganz zu*) von Xu et al. (2011) erfasst. Tabelle 4 umfasst die Mittelwerte (Standardabweichungen) der Subskalen für die verschiedenen Versuchsgruppen sowie die Ergebnisse der Welch-ANOVA,[10] die durchgeführt wurde, um die Unterschiede zwischen den Versuchsgruppen zu untersuchen. Für die p-Werte wurde eine Korrektur nach Bonferroni durchgeführt (Hemmerich, 2023). Es konnten keine signifikanten Unterschiede gezeigt werden.

[10] Es konnte weder eine MANOVA noch eine ANOVA berechnet werden, da die Voraussetzungen für die Berechnungen in den Daten nicht erfüllt waren. Es lag keine Normalverteilung der Daten vor. Außerdem enthielten die Daten viele Ausreißer.

Tabelle 4. Ergebnisse der Bewertung des Onlineshops.

	Gruppe 1 *M* (*SD*)	Gruppe 2 *M* (*SD*)	Gruppe 3 *M*(*SD*)	Gruppe 4 *M*(*SD*)	Ergebnisse Welch-ANOVA
Vertrauenswürdigkeit des Onlineshops					
Wahrgenommenes Risiko	3.90 (0.79)	3.85 (0.80)	4.07 (0.75)	3.82 (0.92)	$F(3, 205.00) = 1.97, p > .999$
Wohlwollen	3.36 (0.73)	3.58 (0.66)	3.58 (0.73)	3.57 (0.70)	$F(3, 205.13) = 1.995, p > .999$
Kompetenz	3.22 (0.82)	3.48 (0.81)	3.54 (0.82)	3.39 (0.93)	$F(3, 205.31) = 2.58, p = .605$
Vertrauen	3.32 (0.77)	3.46 (0.68)	3.46 (0.75)	3.39 (0.87)	$F(3, 204.34) = .676, p > .999$
User Experience des Onlineshops					
Benutzbarkeit	4.17 (0.73)	4.21 (0.65)	4.37 (0.61)	4.29 (0.64)	$F(3, 204.58) = 1.79, p > .999$
Vertrauen	3.58 (0.69)	3.57 (0.81)	3.49 (0.71)	3.59 (0.95)	$F(3, 205.17) = .58, p > .999$
Loyalität	4.37 (1.70)	4.61 (1.74)	4.45 (1.83)	4.55 (1.94)	$F(3, 205.74) = .34, p > .999$
Erscheinungsbild	3.92 (0.73)	3.91 (7.21)	4.06 (0.67)	4.02 (0.65)	$F(3, 205.34) = 1.09, p > .999$
Privatsphärebedenken bezüglich des Onlineshops					
Privatsphärebedenken	3.24 (1.23)	3.37 (1.28)	3.08 (1.37)	3.34 (1.44)	$F(3, 205.82) = .89, p > .999$
Privatsphärerisiken	3.24 (1.23)	3.50 (1.22)	3.17 (1.26)	3.41 (1.33)	$F(3, 205.61) = 1.43, p > .999$
Privatsphärekontrolle	4.32 (1.24)	4.19 (1.26)	4.23 (1.32)	4.17 (1.31)	$F(3, 205.90) = .25, p > .999$

4.3.6 Ergebnisse der Studie 2b – Perspektive der Webseitenbetreibenden

Im Rahmen von Studie 2b wurde die Perspektive der Webseitenbetreibenden auf verschiedene Gestaltungsvarianten von Cookie-Einwilligungserklärungen mithilfe einer Online-Umfrage untersucht. Darüber hinaus wurde mithilfe eines in die Umfrage integrierten Online-Experiments untersucht, ob durch die Bereitstellung von Informationen die Entscheidung der Webseitenbetreibenden für eine Gestaltungsvariante beeinflusst werden kann. Als bereitgestellte Informationen dienten die in Studie 2a erhobenen Daten. Im Folgenden werden die Ergebnisse der Studie 2b dargestellt.

Hintergründe zu den Webseiten

In der Umfrage wurden die Teilnehmenden nach verschiedenen Hintergrundinformationen zu ihren Webseiten befragt, die im Folgenden vorgestellt werden.

Monatliche Seitenzugriffe. Die meisten Teilnehmenden betreiben Webseiten mit verhältnismäßig wenigen Seitenzugriffen. Ihre Webseiten verzeichnen entweder 100–999 (26.7 % der Teilnehmenden) oder 1000–9999 (22.6 % der Teilnehmenden) monatliche Seitenzugriffe. Eine Übersicht der Verteilung der Seitenzugriffe unter den Teilnehmenden findet sich in Tabelle 5.

Tabelle 5. Monatliche Seitenzugriffe der Teilnehmenden als Anteil der Teilnehmenden (*N* = 176) in % dargestellt.

Monatliche Seitenzugriffe	0–99	100–999	1.000–9.999	10.000–99.999	100.000–999.999	1.000.000+	weiß nicht	keine Antwort
Anteil der Teilnehmenden in %	16.9	26.7	22.6	9.7	4.1	8.7	8.7	9.7

Rechtlicher Rahmen der Webseiten. Die Mehrheit (78.5 %) der Teilnehmenden gab an, dass ihre Webseite unter die DSGVO falle. Ein kleiner Teil der Teilnehmenden (11.3 %) gab an, den rechtlichen Rahmen ihrer Webseite nicht zu kennen.

Eingesetzte Cookies auf den Webseiten. Die meisten Teilnehmenden (74.9 %) gaben an, auf ihrer Webseite Cookies einzusetzen. Nur ein Teil (35.9 %) gab an, Präferenz-Cookies zu setzen. Rund ein Drittel (33.8

%) gab an, Marketing-Cookies zu setzen. Einige Teilnehmende gaben an, nicht zu wissen, ob Marketing-Cookies (8.2 %) bzw. Präferenz-Cookies (9.2 %) auf ihrer Webseite gesetzt wurden.

Einnahmen durch Cookies. Nur ein Teil der Teilnehmenden (16.9 %) gab an, Einnahmen durch Cookies zu generieren. Die Mehrheit der Teilnehmenden (68.2 %) gab an, keine Einnahmen zu generieren. Die übrigen Teilnehmenden machten keine Angaben oder wussten nicht, ob sie Einnahmen mit durch Cookies gespeicherten Daten generieren.

Gestaltung der Cookie-Einwilligungserklärungen. Die meisten Teilnehmenden (35.4 %) gaben an, ihre Cookie-Einwilligungserklärung selbst erstellt zu haben. Insgesamt 21.5 % hatten die Vorlage des Webseitenanbieters (meist WordPress) verwendet. 12.3 % der Teilnehmenden gaben an, keine Cookie-Einwilligungserklärung auf ihrer Webseite zu verwenden. Insgesamt 7.7 % hatten die Einwilligungserklärung mit einer CMP erstellt (z. B. mit Cookiebot). 9.2 % wussten nicht, woher die Einwilligungserklärung stammte. Weitere 5.1 % gaben sonstige Quellen für ihre Einwilligungserklärungen an. Darunter wurden u. a. Werbeagenturen, früherer Betreibende der Webseite sowie CMPs genannt. Die restlichen Teilnehmenden machten keine Angaben.

Einschätzung der Nutzendenpräferenz

Die teilnehmenden Webseitenbetreibenden wurden gefragt, welche der vier Gestaltungsvarianten für Cookie-Einwilligungserklärungen (siehe Abbildung 11 bis Abbildung 14) ihrer Meinung nach die Präferenz von Nutzenden darstellt. Die Mehrheit der Teilnehmenden (53.2 % von $N = 126$, die dazu eine Angabe gemacht hatten) gab an, dass die Gestaltungsvariante 4 (*Bright Design*) die präferierte Variante der Nutzenden sei. Nur 5.6 (von $N = 126$) schätzten die Gestaltungsvariante 1 (*Deceptive Design* 1) als die von den Nutzenden präferierte Variante ein. Ein Überblick über die Angaben zur Einschätzung der Nutzendenpräferenz findet sich in Abbildung 18.

Bewertung und Auswahl der Cookie-Einwilligungserklärung

Im weiteren Verlauf wurden die teilnehmenden Webseitenbetreibenden gebeten, eine der vier Gestaltungsvarianten (siehe Abbildung 11 bis Abbildung 14) für eine Cookie-Einwilligungserklärung auszuwählen, die ihnen als Webseitenbetreibende am ehesten zusagt. Die Mehrheit (42.1 %) der Teilnehmenden wählte als präferierte Variante die Gestaltungsvariante 4 (*Bright Design*) . Diese wurde auf einer siebenstufigen Likert-Skala (1 – *gefällt mir gar nicht* bis 7 – *gefällt mir sehr gut*) mit $M = 5.22$ ($SD = 1.66$) am besten bewertet. Die am seltensten präferierten Varianten stellten Gestaltungsvariante 1 (*Deceptive Design* 1) und Gestaltungsvariante 2 (*Deceptive Design* 2) dar (beide 14.9 %), wobei die Gestaltungsvariante 1 $M = 2.90$ ($SD = 2.02$) den Teilnehmenden im Durchschnitt am wenigsten gefiel. Ein Chi-Quadrat-Test wurde zwischen der Versuchsgruppe und der Auswahl der Gestaltungsvariante durchgeführt. Keine erwarteten Zellhäufigkeiten waren kleiner als 5. Es gab keinen statistisch signifikanten Zusammenhang zwischen der Versuchsgruppe und der Tatsache, welche Gestaltungsoption ausgewählt wurde, $\chi^2(3) = 4.378$, $p = .223$.

Um herauszufinden, ob bzw. welche Prädiktoren vorhersagen, ob die Teilnehmenden eine Gestaltungsvariante mit oder ohne *Deceptive Designs* auswählen, wurde ein binomiales logistisches

Regressionsmodell berechnet. Darin eingeschlossen wurden die Variablen, ob die Teilnehmenden Einnahmen mit den Daten aus den Cookies ihrer Webseiten generierten (ja/nein) und ob sie notwendige (ja/nein), Marketing- (ja/nein) oder Präferenz-Cookies (ja/nein) auf ihrer Webseite einsetzten. Dieses Modell war statistisch nicht signifikant, χ^2 (4) = 5.63, p = .229.

Ein Chi-Quadrat-Test wurde zwischen der monatlichen Anzahl der Seitenzugriffe (in Kategorien, wie oben in den Hintergründen zu den Webseiten beschrieben) und der präferierten Gestaltungsvariante durchgeführt. Keine erwarteten Zellhäufigkeiten waren kleiner als 5. Es gab keinen statistisch signifikanten Zusammenhang zwischen der monatlichen Anzahl der Seitenzugriffe und der Tatsache, welche Gestaltungsoption ausgewählt wurde, $\chi^2(5) = 3.914$, p = .562.

Ein weiterer Chi-Quadrat-Test wurde zwischen der Einnahmengenerierung durch Cookie-Daten und der präferierten Gestaltungsvariante durchgeführt (siehe Abbildung 17). Keine erwarteten Zellhäufigkeiten waren kleiner als 5. Es konnte ein statistisch signifikanter Zusammenhang zwischen der Gruppe der Teilnehmenden, die Einnahmen mit den Cookie-Daten generieren, und denen, die keine Einnahmen generieren, und der gewählten Gestaltungsoption gezeigt werden, $\chi^2(1) = 6.764$, p = .009. φ = 0.202.

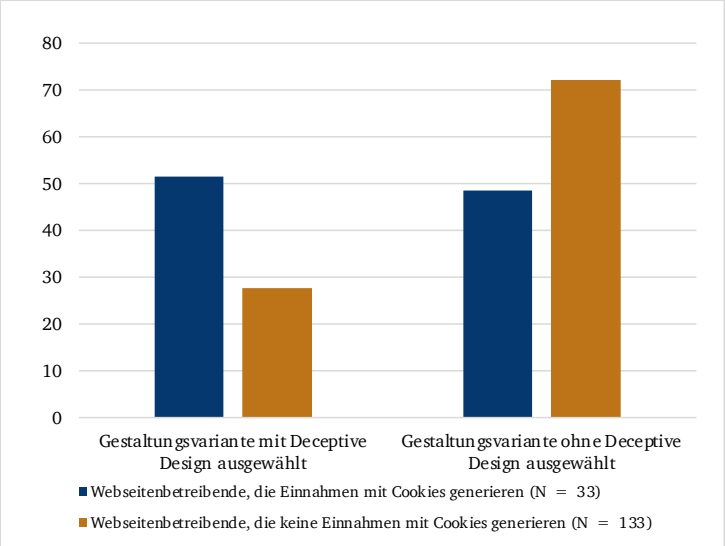


Abbildung 17. Anteil der Webseitenbetreibenden (in %), die eine Gestaltungsvariante für eine Cookie-Einwilligungserklärung mit und ohne Deceptive Design ausgewählt hat.

Begründung der Auswahl der Cookie-Einwilligungserklärung. Die Auswertung der offenen Antworten ergab, dass ein Grund der Teilnehmenden für die Auswahl von Gestaltungsvarianten mit *Deceptive Designs* die Hoffnung ist, dass Nutzende eher Cookies zustimmen. Person P75 erklärte seine Wahl so: „*Da es für den Besucher am aufwendigsten ist die Cookies abzulehnen und somit die Chance größer ist, dass die Cookies akzeptiert werden.*“ Eine weitere Begründung der Auswahl ist, dass diese Gestaltungsvarianten optisch ansprechend und informativ sind. Teilnehmende, die eine Gestaltungsvariante ohne *Deceptive Designs* auswählten, begründeten dies ebenfalls mit der ansprechenden Gestaltung, z. B. schrieb P20: „*Am übersichtlichsten.*“ Weitere Begründungen umfassen auch die explizite Erwähnung des Wunsches, ein positives Nutzungserlebnis auf der Webseite zu schaffen und „*seriös*“ (P36) zu wirken. P38 beschrieb dies so: „*Das ist bei den gezeigten Optionen die minimalst invasive Form um meine Besuchenden zu nerven. Als Websitebetreiber bin ich daran interessiert, meinen*

Besuchenden ein positive User Experience zu ermöglichen, ihnen auf Augenhöhe zu begegnen und sie nicht mit Tricks etwas auswählen zu lassen was sie eigentlich nicht möchten oder wo sie unnötig drüber nachdenken müssen was sie wählen.“ Das positive Erleben auf der Webseite scheint gerade dann zentral, wenn die Webseite eher Mittel zum Zweck ist, wie P96 erläuterte: *„Da unsere Seite nur zur Information vor einem physischen Besuch dient, ist die Akzeptanz und das gute Gefühl der Besucher wichtiger als die Marketingfunktionen.*“

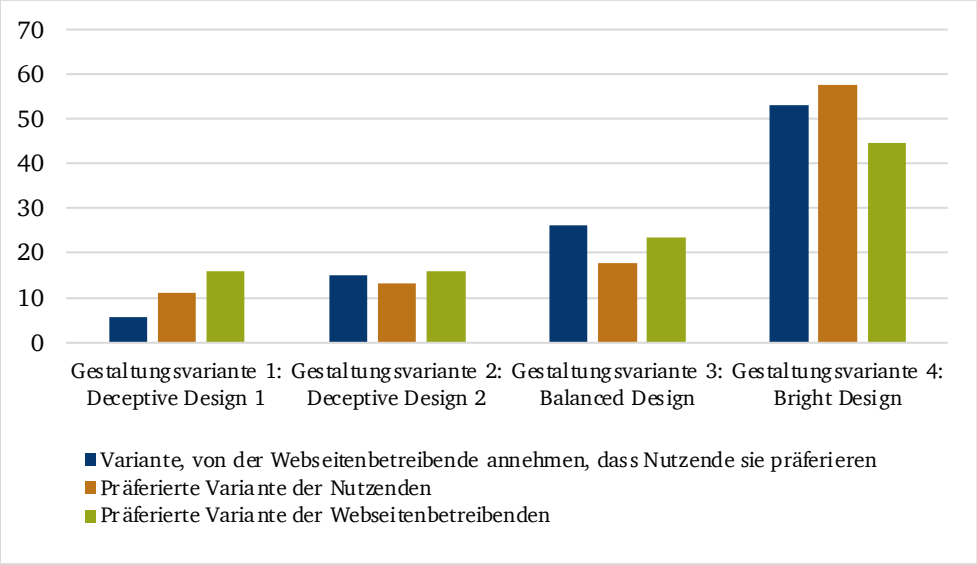


Abbildung 18. Präferierte Gestaltungsvarianten für Einwilligungserklärungen von Nutzenden und Webseitenbetreibenden sowie die Einschätzung der Webseitenbetreibenden über die präferierten Varianten der Nutzenden.

4.3.7 Diskussion

Ziel der Studie war es, sowohl die Perspektive der Nutzenden als auch der Webseitenbetreibenden auf verschiedene Gestaltungsvarianten von Cookie-Einwilligungserklärungen zu untersuchen und dabei Gemeinsamkeiten und potenzielle Diskrepanzen aufzudecken. Auch wenn der Fokus dieser Arbeit auf den Webseitenbetreibenden liegt, wurde in Studie 2a zunächst die Nutzendenperspektive beleuchtet, weil diese als Ausgangslage für Studie 2b diente.

Um zu untersuchen, ob die Gestaltung von Cookie-Einwilligungserklärungen einen Einfluss auf die Interaktion mit der Einwilligungserklärung sowie auf die Wahrnehmung und die Interkation mit der Webseite hat, wurden die Teilnehmenden im Rahmen eines Online-Experiments gebeten, mit einem fiktiven Onlineshop zu interagieren. Beim Betreten des Onlineshops wurde den Teilnehmenden eine von vier Gestaltungsvarianten einer Cookie-Einwilligungserklärung anzeigt.

Die Ergebnisse zeigen, dass die Gestaltung der Einwilligungserklärung einen signifikanten Einfluss auf das Ausmaß der Zustimmung der Teilnehmenden zu Cookies hat. Die Versuchsgruppen, denen eine Einwilligungserklärung mit einem *Deceptive Design* angezeigt wurde, stimmten häufiger allen Cookies zu als Teilnehmende, denen eine Gestaltungsvariante mit einem *Balanced* oder einem *Bright Design* angezeigt wurde. Diese Ergebnisse replizieren, was Utz et al. (2019) bereits zeigen konnten. Entgegen der vorherigen Vermutung konnte kein Einfluss der Gestaltung der Einwilligungserklärung auf die Wahrnehmung sowie die Interaktion der Nutzenden mit dem Onlineshop gezeigt werden. Dafür gibt es mindestens zwei mögliche Erklärungen. Zum einen könnte es sein, dass die Teilnehmenden in ihrem

Alltag bereits so an die Interaktion mit Einwilligungserklärungen beim Besuch von Webseiten gewöhnt sind, dass die Interaktion im vorliegenden Online-Experiment keine bewusste Interaktion darstellte. Gestützt wird diese Erklärung dadurch, dass die Interaktionszeit der Nutzenden mit den Einwilligungserklärungen sehr kurz war und nur ein Teil der Teilnehmenden sich in der späteren Befragung genau erinnern konnte, ob und welche Gestaltungsvariante ihnen zuvor angezeigt worden war. Eine weitere Erklärung dafür, warum die Gestaltungsvarianten keinen Einfluss auf die Wahrnehmung bzw. die Interaktion mit der Webseite hatten, könnte darin liegen, dass die Teilnehmenden *Deceptive Designs* in Einwilligungserklärungen aufgrund ihrer weiten Verbreitung bereits so gewöhnt sind, dass sie diese entweder routiniert umgehen oder bereits resigniert haben und allen Cookies zustimmen. Eine Beobachtung, die dafürsprechen würde, ist die Tatsache, dass die Nutzenden überwiegend eine Einwilligungserklärung mit einem *Deceptive Design* wählten, als sie gefragt wurden, was sie denken, welche Gestaltungsvariante Webseitenbetreibende bevorzugen. Es kann also sein, dass Teilnehmende bereits erwarten, dass sie beim Besuch einer Webseite eine Einwilligungserklärung mit einem *Deceptive Design* vorfinden. Das ist insofern beunruhigend, weil die Befragung zeigt, dass nur wenige Teilnehmende Einwilligungserklärungen mit einem *Deceptive Design* bevorzugen. Die meisten Teilnehmenden präferieren eine Einwilligungserklärung mit einem *Balanced* oder einem *Bright Design*. Wie die offenen Antworten zeigen, werden diese Varianten bevorzugt, weil Nutzende damit den Schutz ihrer Privatsphäre priorisieren.

In Studie 2b wurde die Perspektive der Webseitenbetreibenden mithilfe einer Online-Umfrage untersucht, in die ein Experiment integriert war. Als die teilnehmenden Webseitenbetreibenden gefragt wurden, was sie vermuten, welche Gestaltungsvarianten für Einwilligungserklärungen von Nutzenden präferiert werden, zeigte sich, dass die Webseitenbetreibenden dies gut einschätzen konnten. Als die Webseitenbetreibenden gebeten wurden, eine Gestaltungsvariante auszuwählen, wählte ein großer Teil der Teilnehmenden eine Variante, die auch der Nutzendenpräferenz entspricht. Einwilligungserklärungen mit *Deceptive Designs* wurden primär von Webseitenbetreibenden gewählt, die Einnahmen mit den durch Cookies gespeicherten Daten generieren. Interessanterweise wählten jedoch Webseitenbetreibende, die Webseiten mit vielen monatlichen Seitenzugriffen haben, nicht häufiger eine Einwilligungserklärung mit einem *Deceptive Design* als solche mit wenigen monatlichen Seitenzugriffen. Die offenen Antworten weisen darauf hin, dass vielmehr die Ziele, die mit der Webseite verfolgt werden, eine Rolle spielen. So beschrieben Teilnehmende z. B., dass sie bewusst keine *Deceptive Designs* einsetzen möchten, weil sie einen seriösen Eindruck machen und den Nutzenden ein positives Erleben auf der Webseite bereiten möchten. Andere, die *Deceptive Designs* auswählten, beschrieben, dass ihr Geschäftsmodell auf den Daten der Nutzenden basiert.

Hierbei zeigt sich, dass ein Teil der Webseitenbetreibenden sich von anderen *Expert Users* unterscheidet. In der Forschung wurde gezeigt, dass z. B. App-Entwickler:innen sich bewusst gegen privatsphärefreundliche Varianten entscheiden, um ihre App mit den Nutzendendaten zu monetarisieren (Mhaidli et al., 2019). Die mithilfe des Experiments untersuchte Bereitstellung von Informationen konnte die Entscheidung der Webseitenbetreibenden bezüglich der Gestaltung der Einwilligungserklärung nicht beeinflussen. Eine mögliche Erklärung dafür ist, dass den Webseitenbetreibenden in der Experimentalgruppe zu viele Informationen bereitgestellt wurden, die nicht (vollständig) gelesen oder erfasst wurden. Diese Erklärung wäre jedoch zugleich ein Indikator

dafür, dass eine ähnliche Maßnahme in der Praxis keinen Effekt zeigen würde, da Webseitenbetreibende im Alltag vermutlich noch weniger Zeit aufwenden würden. Eine weitere mögliche Erklärung dafür, warum die Bereitstellung von Informationen keinen Effekt zeigte, könnte darin liegen, dass den Webseitenbetreibenden die bereitgestellten Informationen möglichweise bereits bekannt waren. Diese Erklärung wird durch Aussagen der Webseitenbetreibenden in den offenen Antworten gestützt.

Es stellt sich jedoch die Frage, ob Webseitenbetreibende ihre Vorstellungen von Cookie-Einwilligungserklärungen (und deren Grad an Privatsphärefreundlichkeit) in der Praxis auch umsetzen können. Eine funktionierende Cookie-Einwilligungserklärung zu erstellen, mit der Webseitenbetreibende auf der rechtlich sicheren Seite sind, ist nicht immer einfach (Hils et al., 2020). Deshalb greifen Webseitenbetreibende zunehmend auf die Dienste von CMPs zurück, um Cookie-Einwilligungserklärungen zu erstellen. CMPs enthalten in der Regel bestimmte Gestaltungsvorlagen für die Erstellung von Cookie-Einwilligungserklärungen. Inwiefern diese Vorlagen die Erstellung von privatsphärefreundlichen Cookie-Einwilligungserklärungen begünstigen oder hindern, ist jedoch unklar und soll in Studie 3 untersucht werden.

4.3.8 Limitationen

Die Studie hat einige Limitationen, die sich auf das Versuchsdesign, die Rekrutierung der Teilnehmenden sowie die Stichprobenzusammensetzung beziehen. Diese werden im Folgenden beschrieben.

Versuchsdesign: Die Gestaltungsvarianten 1 und 2 der Cookie-Einwilligungserklärungen waren so gewählt, dass sie im Vergleich zu den Gestaltungsvarianten 3 und 4 mehrere *Deceptive Designs* enthielten. Zur Umsetzung des *Deceptive Designs Obstruction* wurde bei den Gestaltungsvarianten 1 und 2 eine zweite Seite eingeführt. Diese wiederum enthielt Informationen zur Beschreibung der verschiedenen Cookie-Zwecke, die in den Gestaltungsvarianten 3 und 4 nicht enthalten waren. Idealerweise hätten diese Informationen dort auf der ersten Seiten gestanden. Dieser Fehler in der Gestaltung führte dazu, dass sowohl einige Nutzende als auch Webseitenbetreibende die Gestaltungsvarianten 1 und 2 präferierten und dies damit begründeten, eine besser informierte Entscheidungen treffen zu können. Daher wurden möglicherweise Einwilligungserklärungen mit *Deceptive Designs* etwas häufiger ausgewählt oder positiv bewertet, als es unter anderen Umständen der Fall gewesen wäre. Eine weitere Limitation betrifft das Experiment der Studie 2a. Hier wurde als Beispielwebseite ein Onlineshop gewählt. Es ist jedoch nicht klar, inwiefern die Ergebnisse auf andere Webseiten übertragen werden können. Es könnte z. B. sein, dass Nutzende bei Onlineshops eher allen Cookies zustimmen als bei anderen Webseiten, weil sie sich davon einen direkten Vorteil in Form einer personalisierten Shoppingerfahrung erhoffen. Eine weitere Limitation, die das Experiment aus Studie 2b betrifft, besteht darin, dass nicht geprüft wurde, ob die Teilnehmenden der Experimentalgruppe die bereitgestellten Informationen tatsächlich gelesen und verstanden haben. So kann nicht ausgeschlossen werden, dass mit dem Experiment kein Effekt gezeigt werden konnte, weil die Teilnehmenden die entsprechenden Informationen nicht gelesen haben.

Rekrutierung der Teilnehmenden: Ungefähr die Hälfte der Studienteilnehmenden aus Studie 2b wurde mithilfe einer E-Mail-Liste rekrutiert. Diese hatte ihren Ursprung in der Umfrage der Studie 1, bei der die Teilnehmenden freiwillig ihre E-Mail-Adresse für weitere Studienaufrufe mit den Studienorganisator:innen teilen konnten. Es ist davon auszugehen, dass dieser Teil der Stichprobe ein

besonderes Interesse an Privatsphärethemen hat. Allerdings zeigt ein deskriptiver Vergleich der Antworten der Studienteilnehmenden, die über die E-Mail-Liste rekrutiert wurden, mit denen der Studienteilnehmenden, die über die Rekrutierungsplattform rekrutiert wurden, keine auffälligen Unterschiede. Es ist trotzdem nicht auszuschließen, dass die Form der Rekrutierung bestimmte Webseitenbetreibende angesprochen hat, was zu einer Verzerrung der Ergebnisse geführt haben kann.
Stichprobenzusammensetzung: Ein Großteil der teilnehmenden Webseitenbetreibenden in Studie 2b betreibt eine Webseite mit eher wenigen monatlichen Seitenzugriffen und nur ein kleiner Teil der Befragten generiert Einnahmen mit den durch Cookies gespeicherten Daten. Inwiefern die Ergebnisse dieser Studie repräsentativ für die Gesamtheit der Webseitenbetreibenden ist, bleibt fraglich. Dennoch liefern die Ergebnisse spannende Erkenntnisse über eine Teilgruppe der Webseitenbetreibenden.

4.4 Studie 3 – Untersuchung von Vorlagen für Cookie-Einwilligungserklärungen

In diesem Unterkapitel wird die Studie 3 dieser Arbeit vorgestellt. Dazu werden zunächst die Forschungsfragen hergeleitet, bevor die Methode erläutert wird sowie die Ergebnisse vorgestellt und diskutiert werden.

4.4.1 Forschungsfragen

Die Ergebnisse aus der vorangegangenen Studie deuten darauf hin, dass *Deceptive Designs* in Einwilligungserklärungen nur im Interesse von einem Teil der Webseitenbetreibenden ist. Dies sind nicht zwangsläufig die Betreibenden von Webseiten mit vielen Seitenzugriffen, sondern primär diejenigen, die Einnahmen mit Cookie-Daten generieren. Die anderen Webseitenbetreibenden äußern, dass sie die Privatsphäre der Nutzenden schützen wollen oder ihnen das positive Nutzungserlebnis auf ihrer Webseite wichtig ist. Sie präferieren daher Gestaltungsvarianten für Einwilligungserklärungen, die keine *Deceptive Designs* enthalten. Es stellt sich jedoch die Frage, ob diese Webseitenbetreibenden ihre Präferenzen bei der Erstellung von Cookie-Einwilligungserklärungen in der Praxis auch tatsächlich umsetzen können. Für Webseitenbetreibende kann es schwierig sein eine funktionierende Cookie-Einwilligungserklärung zu erstellen, mit sie auf der rechtlich sicheren Seite sind (Hils et al., 2020). Zunehmenden greifen sie deshalb auf die Dienste von CMPs zurück, um Cookie-Einwilligungserklärungen zu erstellen. CMPs bieten in der Regel bestimmte Gestaltungsvorlagen für die Erstellung von Cookie-Einwilligungserklärungen. Inwiefern diese Vorlagen die Erstellung von Cookie-Einwilligungserklärungen, die *Deceptive Designs* enthalten, begünstigen oder hindern, ist jedoch unklar. Deshalb lautet die letzte Forschungsfrage dieser Arbeit wie folgt:

Forschungsfrage 7: Inwiefern können Webseitenbetreibende durch entsprechende Vorlagen darin unterstützt werden, *Deceptive Designs* in Cookie-Einwilligungserklärungen zu vermeiden?

In der folgenden Untersuchung werden die Vorlagen der CMPs für Cookie-Einwilligungserklärungen analysiert, um folgende Unterfragen zu adressieren:

- **Forschungsfrage 7a:** Enthalten die Standardvorlagen für Cookie-Einwilligungserklärungen der CMPs bereits *Deceptive Designs* und wenn ja, welche?

- **Forschungsfrage 7b:** Erlauben es die Vorlagen für Cookie-Einwilligungserklärungen der CMPs, Erklärungen mit einem *Balanced Design* und/oder einem *Bright Design* zu erstellen?

Um diese Fragen zu beantworten, wurden die Angebote von freiverfügbaren CMPs analysiert. Das methodische Vorgehen wird im nächsten Unterkapitel beschrieben.

4.4.2 Methode

Um die oben beschriebenen Forschungsfragen zu adressieren, wurde in drei Schritten vorgegangen: (1) Identifizierung relevanter CMPs, (2) Erstellung von Cookie-Einwilligungserklärungen mithilfe der Vorlagen der identifizierten CMPs und (3) Analyse der erstellten Cookie-Einwilligungserklärungen.

Schritt 1: Identifizierung relevanter CMPs

Die Auswahl der relevantesten CMPs ist eine anspruchsvolle Aufgabe, da verschiedene Toplisten existieren (G2, o. J.; Gradow & Greiner, 2021; Kevel, o. J.). Die Analysen von Hils et al. (2020) zeigen, dass der Marktanteil verschiedener CMPs sehr dynamisch ist und je nach den analysierten Webseiten variiert. Für die vorliegende Studie wurde beschlossen, Quellen (Top-Listen, verwandte Arbeiten sowie eine eigene Google-Suche) von CMPs zusammenzuführen, um eine umfassende Liste von CMPs zu erstellen (siehe Anhang D). Zu diesem Zweck wurde zunächst die Perspektive von Webseitenbetreibenden eingenommen, die auf der Suche nach einer geeigneten Cookie-Einwilligungserklärung für ihre Webseite sind. Ausgangspunkt für die Zusammenstellung der relevanten CMPs waren daher CMPs, die auf den ersten vier Seiten der Google-Suche im Inkognito-Modus für die Begriffe ‚Cookie-Einwilligungserklärung' und ‚Consent Management Platform' zu finden waren. Diese Liste wurde durch die CMPs ergänzt, die in verwandten Arbeiten (Gradow & Greiner, 2021; Nouwens et al., 2020) und Top-Listen (G2, o. J.; Kevel, o. J.) aufgeführt sind. Insgesamt wurden 49 CMPs identifiziert (siehe Anhang D), die als Grundlage für Schritt 2 dienten.

Schritt 2: Erstellung von Cookie-Einwilligungserklärungen

Das Ziel von Schritt 2 war es, verschiedene Cookie-Einwilligungserklärungen unter Verwendung der in Schritt 1 identifizierten CMPs zu erstellen. Zu diesem Zweck wurden zwei unabhängige Forschende angewiesen, sich in die Perspektive der Webseitenbetreibenden zu versetzen und drei Cookie-Einwilligungserklärungen unter Verwendung der Vorlagen der CMPs zu erstellen. Die Erstellung der Einwilligungserklärungen wurde von zwei unabhängigen Forschenden vorgenommen, um die Qualität der Daten zu erhöhen. Die auf diese Weise erstellten Cookie-Einwilligungserklärungen wurden von einer dritten Person verglichen. Da das vorgegebene Verfahren nur bis zu einem gewissen Grad standardisiert war und die Webseiten der CMPs oft unübersichtlich waren, waren nicht alle Ergebnisse identisch (z. B. gab es Unterschiede in der Hintergrundfarbe). Die Unterschiede wurden in der Forschungsgruppe diskutiert und bei marginalen Unterschieden (z. B. bei unterschiedlichen Schriftarten) wurde eine Designvariante als Basis für die Analyse gewählt. In einem Fall (CCM (CCM19, o. J.)) waren die Ergebnisse jedoch so unterschiedlich, dass alle Varianten in den weiteren Analyseprozess einbezogen wurden. Zur besseren Übersicht wurde jedoch nur die Variante mit den meisten *Deceptive Designs* in die Endauswertung einbezogen. Die Erstellung der Cookie-Einwilligungserklärungen erfolgte in der Zeit

vom 10. bis zum 11. März 2022. Zum Zwecke der Vergleichbarkeit wurden aus der resultierenden Liste alle CMPs ausgewählt, die kostenlos waren und keinen persönlichen Kontakt mit einem Vertriebsmitarbeitenden erforderten. Insgesamt erfüllten 15 der 49 CMPs diese Anforderungen (siehe Anhang D). Wenn möglich, wurden die folgenden drei Arten von Cookie-Einwilligungserklärungen mit den Vorlagen der CMPs erstellt:

- *Einwilligungserklärung mit Standardeinstellungen:* Für die Erstellung dieser Einwilligungserklärungen wurden die voreingestellten Standardeinstellungen der CMPs genutzt und es wurde lediglich darauf geachtet, dass die Einwilligungserklärungen in englischer Sprache verfasst wurden und falls es die Option ‚DSGVO-konform' gab, wurde diese ausgewählt.
- *Einwilligungserklärung mit Balanced Design:* Hier war das Ziel, eine Cookie-Einwilligungserklärung zu generieren, bei der die Buttons zum Akzeptieren und Ablehnen von Cookies bezüglich der Größe, der Farbe und der Position gleich und auf der ersten Seite der Einwilligungserklärung platziert sind.
- *Einwilligungserklärung mit Bright Design:* Angelehnt an den Vorschlag von Graßl et al. (2021) sollte diese Cookie-Einwilligungserklärung die Nutzenden dazu verleiten, alle Cookies abzulehnen. Zu diesem Zweck sollte der Alle-Ablehnen-Button visuell hervorgehoben sein.

Schritt 3: Analyse von Cookie-Einwilligungserklärungen

In Schritt 3 wurden die in Schritt 2 erstellten Cookie-Einwilligungserklärungen von zwei unabhängigen Forschenden analysiert, die nicht an der Erstellung der Einwilligungserklärungen beteiligt waren. Zu diesem Zweck erhielten sie Screenshots der Einwilligungserklärungen mit *Balanced Design* und der Standard-Cookie-Einwilligungserklärungen, ohne die Information, welche Erklärung sich auf welchen Fall bezog. Den Forschenden wurden die *Deceptive-Design*-Strategien nach Gray et al. (2018) sowie die auf diesen Kontext angepassten Definitionen zur Verfügung gestellt (siehe Tabelle 2). Bei der Analyse lag der Schwerpunkt auf den *Deceptive Designs Obstruction* und *Interface Interference*, die Soe et al. (2020) als die häufigsten *Deceptive Designs* in Cookie-Einwilligungserklärungen identifiziert haben. Die Forschenden wurden gebeten, die Einwilligungserklärungen im Hinblick auf die folgenden Aspekte zu bewerten:

- *Obstruction*: Enthält die Einwilligungserklärung *Obstruktion*? [ja/nein/unklar]
- *Interface Interference*: Enthält die Einwilligungserklärung *Interface Interference*? [ja/nein/unklar]
- Andere *Deceptive Designs*: Enthält die Einwilligungserklärung andere *Deceptive Designs*? [ja/nein/unklar] + Beschreibung der anderen *Deceptive Designs*
- Gesamtbewertung: Gibt es in der Einwilligungserklärung *Deceptive Designs*? [ja/nein/unklar]
- Anzahl *Deceptive Designs*: Wie viele *Deceptive Designs* enthält die Einwilligungserklärung?

Außerdem konnten die Forschenden die Cookie-Einverständniserklärungen kommentieren. Nachdem sie ihre Bewertungen abgegeben hatten, wurden sie von einer dritten Forscherin verglichen. Unstimmigkeiten in den Bewertungen wurden durch eine Diskussion mit den Forschenden gelöst.

4.4.3 Ergebnisse

Ausgangspunkt dieser Studie waren die Fragen, ob und welche *Deceptive Designs* bereits in den Standard-Einwilligungserklärungen von CMPs enthalten sind und ob die Erstellung von Erklärungen mit *Balanced* und *Bright Designs* überhaupt möglich ist. Insgesamt wurden die Vorlagen von 15 CMPs untersucht. Von jedem dieser CMPs wurden, sofern möglich, eine Standard- (insgesamt 15), eine *Balanced-Design*- (insgesamt 12) sowie eine *Bright-Design*-Cookie-Einwilligungserklärung (insgesamt 10) in die Ergebnisse einbezogen. Im Folgenden werden die Ergebnisse der Analysen sowie weitere Beobachtungen vorgestellt, die bei der Erstellung der Einwilligungserklärungen von den Forschenden gemacht wurden.

Deceptive Designs in Standardvorlagen für Einwilligungserklärungen

Deceptive Designs: Obstruction und Interface Interference. Zunächst wurden die Standardvorlagen für Cookie-Einwilligungserklärungen im Hinblick auf die beiden *Deceptive Designs*, die laut Soe et al. (2020) am häufigsten in Cookie-Einwilligungserklärungen vorkommen, untersucht: *Interface Interference* und *Obstruction*. Einen Überblick über die Ergebnisse befinden sich in Abbildung 19. Die Analyse zeigt, dass 9 von 15 Vorlagen mindestens eines dieser beiden *Deceptive Designs* enthalten. *Interface Interference* tritt am häufigsten auf (8 von 15). Abbildung 20 zeigt ein Beispiel für einen Hinweis mit *Interface Interference*. *Obstruction* wurde nur in einer der Vorlagen eindeutig identifiziert (siehe Abbildung 21), was einen möglichen Verstoß gegen die DSGVO darstellt (Nouwens et al., 2020).

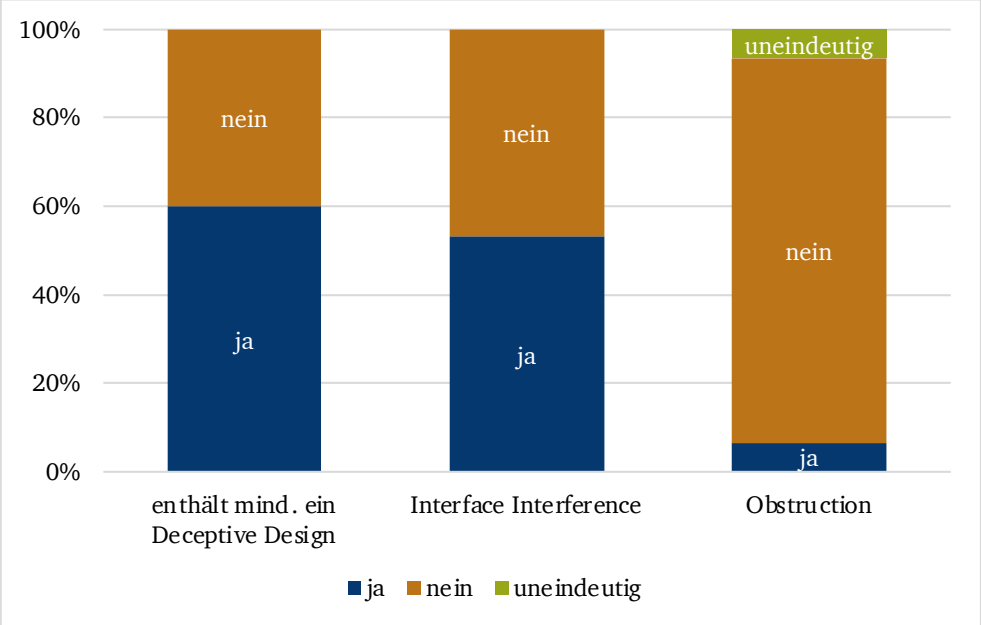


Abbildung 19. Ergebnisse der Analysen der Standardvorlagen für Cookie-Einwilligungserklärungen von 15 populären CMPs. Die Abbildung orientiert sich an der Darstellung von Stöver et al. (2022).

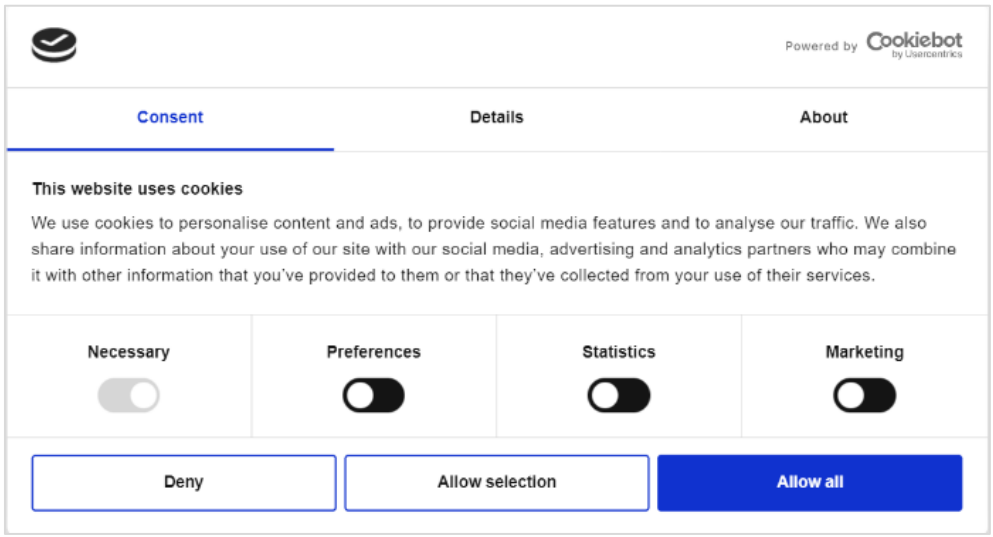


Abbildung 20. Cookie-Einwilligungserklärung, die mit der Standardvorlage von Cookiebot generiert wurde und *Interface Interence* enthält (Cookiebot, o. J.).

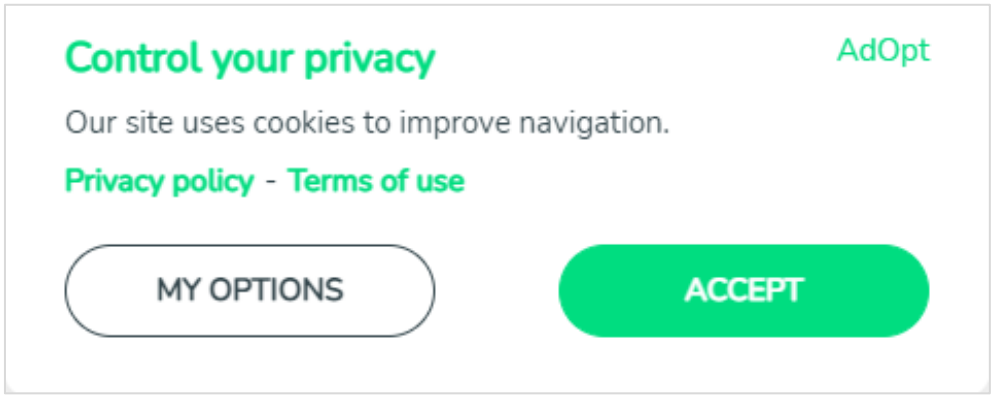


Abbildung 21. Cookie-Einwilligungserklärung, die mit der Standardvorlage von AdOpt generiert wurde und *Obstruction* enthält (AdOpt, o. J.).

Andere Deceptive Designs: Die Standardvorlagen für Cookie-Einwilligungserklärungen wurden auch dahingehenden untersucht, ob sie andere *Deceptive Designs* als *Obstruction* und *Interface Interference* enthielten. In 12 der 15 analysierten Einwilligungserklärungen sahen die Forschenden die Möglichkeit für *Sneaking* oder *Forced Action*. Zum Beispiel könnte der Akzeptieren-Button in Abbildung 21 eine *Forced Action* enthalten, je nachdem, was sich hinter dem Button ‚My Options' verbirgt. Einige Einwilligungserklärungen können *Sneaking* sein, wenn die Nutzenden sich der Folgen ihrer Wahl ‚Accept All' nicht bewusst sind (z. B. in Abbildung 23). Darüber hinaus stellten die Forschenden fest, dass nur 2 der 15 Einwilligungserklärungen auf der ersten Ebene personalisierte Einstellungen zuließen.

Balanced und Bright Designs in Vorlagen für Cookie-Einwilligungserklärungen

In diesem Abschnitt werden die Analysen in Zusammenhang mit der Forschungsfrage 7b vorgestellt: Erlauben es die Standardvorlagen für Cookie-Einwilligungserklärungen der CMPs, Erklärungen mit einem *Balanced Design* und/oder einem *Bright Design* zu erstellen? Einen Überblick über die Ergebnisse finden sich in Abbildung 22. Bei einer Einwilligungserklärung mit *Balanced Design* sollten die Buttons für die Zustimmung und für die Ablehnung von Cookies das gleiche Design haben. Die Erstellung dieses Designs war bei 10 von 15 der CMPs möglich. Ein Beispiel für eine Einwilligungserklärung mit *Balanced*

Design findet sich in Abbildung 23. Eine Einwilligungserklärung mit *Bright Design* hingegen sollte einen visuell hervorgehobenen Alle-Ablehnen-Button aufweisen. Eine solche Einwilligungserklärung konnte bei 10 von 15 der CMPs erstellt werden. Ein Beispiel für eine Einwilligungserklärung mit *Bright Design* findet sich in Abbildung 24.

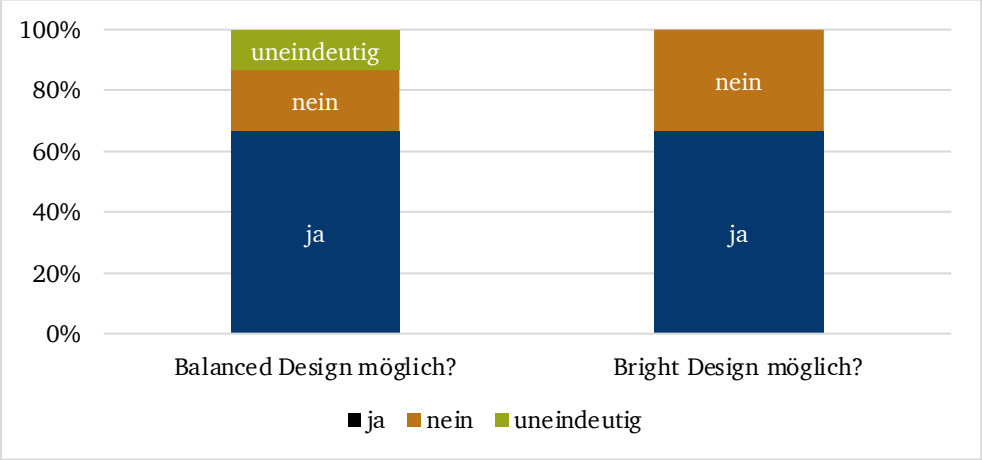


Abbildung 22. Ergebnisse der Analyse der Angebote der CMPs (*N* = 15). Die Abbildung orientiert sich an der Darstellung von Stöver et al. (2022).

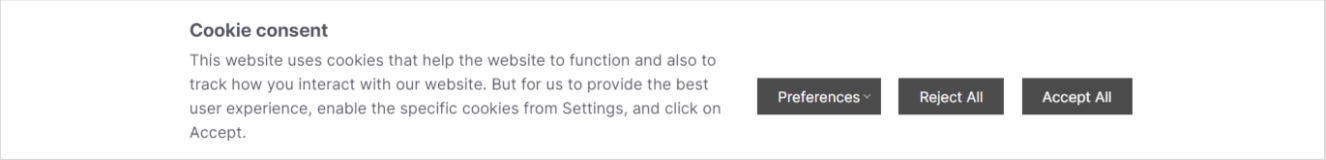


Abbildung 23. Einwilligungserklärung mit *Balanced Design*, die mit der Vorlage der CMP Cookie Yes erstellt wurde (CookieYes, o. J.).

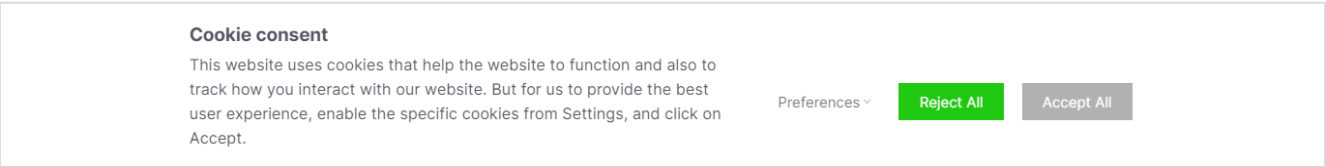


Abbildung 24. Einwilligungserklärung mit *Bright Design*, die mit der Vorlage der CMP Cookie Yes erstellt wurde (CookieYes, o. J.).

Beobachtungen bei der Erstellung von Cookie-Einwilligungserklärungen

Bei der Erstellung der Einwilligungserklärungen sind den Forschenden Dinge aufgefallen, die hier berichtet werden sollen: (1) Herausforderungen bei der Erstellung von *Balanced* und *Bright Designs*: Die Erstellung von *Balanced* und/oder *Bright Designs* war teilweise nur mit einem Premium-Account möglich (z. B. bei der CMP Cookie Hub (CookieHub ehf, o. J.)). In einem anderen Fall war die Erstellung zwar möglich, aber sehr umständlich. Zum Beispiel war in der Vorlage der CMP SmartLife (SmartLife - Online UG, o. J.) die Möglichkeit, die Farbe der Buttons anzupassen, hinter einer Ebene versteckt. (2) *Deceptive Designs* auf CMP-Webseiten: Auffällig war auch, dass einige der Webseiten der CMPs (z. B. SmartLife (SmartLife - Online UG, o. J.)) so gestaltet waren, dass Webseitenbetreibende nachdrücklich zum Kauf von Produkten aufgefordert wurden. Darüber hinaus waren sich die Forschenden oft nicht über die

tatsächlichen Folgen der verschiedenen Einstellungen bewusst, die sie bei der Erstellung der Einwilligungserklärungen vornahmen. Bei der Erstellung eines Hinweises mit der CMP CCM19 (CCM19, o. J.) war z. B. nicht klar, für welchen Button genau die Farbe angepasst wurde.

4.4.4 Diskussion

Das Ziel der Studie war es, Antworten auf die folgenden zwei Forschungsfragen zu finden: (1) Enthalten die Standardvorlagen für Cookie-Einwilligungserklärungen der CMPs bereits *Deceptive Designs* und wenn ja, welche? (2) Erlauben die Vorlagen der CMPs die Erstellung von Einwilligungserklärungen mit einem *Balanced Design* und/oder einem *Bright Design*? Um dies zu untersuchen, wurden die Vorlagen von 15 CMPs analysiert. In früheren Studien wurde untersucht, wie Cookie-Einwilligungserklärungen auf Webseiten, die CMP-Vorlagen verwenden, tatsächlich implementiert wurden (Kampanos & Shahandashti, 2021; Nouwens et al., 2020; Soe et al., 2020). Im Folgenden werden diese Ergebnisse zu den Ergebnissen der hier vorgestellten Studien in Beziehung gesetzt. Die folgenden drei Erkenntnisse lassen sich aus der vorliegenden Studie ableiten, wobei sich die Erkenntnisse 1 und 2 auf die Forschungsfragen beziehen:

Erkenntnis 1

Die Standardvorlagen für Einwilligungserklärungen von CMPs enthalten oft *Deceptive Designs*. Die Analyse der Einwilligungserklärungen hinsichtlich der *Deceptive Designs*, die in der Taxonomie von Gray et al. (2018) aufgeführt sind, zeigt, dass das *Interface Interference* mit 53.33 % in den CMP-Vorlagen am häufigsten vorkommt. Dies stimmt mit den Ergebnissen der Analyse von Cookie-Einwilligungserklärungen in der Praxis überein (Soe et al., 2020). Dies könnte ein Indikator dafür sein, dass viele Webseitenbetreibende die Vorlagen mit Standardeinstellungen verwenden, die *Deceptive Designs* enthalten. Insgesamt konnte mit dieser Studie gezeigt werden, dass 60 % der Standardvorlagen für Cookie-Einwilligungserklärungen definitiv ein *Deceptive Design* enthalten. Das ist weniger als bei anderen Analysen in diesem Bereich (Kampanos & Shahandashti, 2021; Nouwens et al., 2020; Soe et al., 2020). Hierfür gibt es drei mögliche Erklärungen. (1) In dieser Studie wurden nur Einwilligungserklärungen von kostenlosen CMPs analysiert. Daher werden nicht alle CMPs abgedeckt, die in verwandten Arbeiten analysiert wurden. (2) Hils et al. (2020) konnten in ihrer Studie zeigen, dass die CMP-Branche sehr dynamisch ist. Dies könnte der Grund dafür sein, dass alte Versionen der Einwilligungserklärungen noch auf Webseiten verfügbar sind oder dass die Analysen verwandter Arbeiten bereits veraltet sind. (3) Eine weitere Erklärung dafür, warum in dieser Studie weniger *Deceptive Designs* als in anderen Studien gefunden wurden, könnte darin liegen, dass nicht alle Webseitenbetreibende die Standard-Cookie-Einwilligungserklärungen der CMPs verwenden, sondern möglicherweise selbst *Deceptive Designs* integrieren.

Erkenntnis 2

Die Erstellung von datenschutzfreundlichen Einwilligungserklärungen ist oft unmöglich oder sehr umständlich. Die Analysen dieser Studie zeigen, dass Einwilligungserklärungen mit *Balanced* und *Bright Design* nur mit 62.5 % der CMPs erstellt werden können. Bei den CMPs, bei denen dies möglich war, war es teilweise sehr umständlich. Dies ist problematisch, da frühere Untersuchungen, z. B. die in Kapitel

3 berichteten Studien, gezeigt haben, dass Webseitenbetreibende oft viele verschiedene Aufgaben zu bewältigen haben, wobei insbesondere bei kleineren oder mittelgroßen Webseiten der Betrieb der Webseite nicht die Hauptaufgabe der Webseitenbetreibenden ist. Darüber hinaus fehlt diesen oft ein Bewusstsein für Privatsphärethemen und es fehlt an Wissen, wie diese umgesetzt werden können. Daher verlassen sie sich auf transparente Arbeitsmethoden von Drittanbietern wie CMPs. Es ist jedoch nicht immer klar, welche Interessen diese verfolgen.

Erkenntnis 3

CMPs können einen großen Einfluss darauf haben, welche *Deceptive Designs* in Cookie-Einwilligungserklärungen auf Webseiten verbreitet sind. Hils et al. (2020) zeigten, dass Einwilligungserklärungen von CMPs immer häufiger verwendet werden, sodass ihr Einfluss stetig zunimmt. Insbesondere wenn dominante CMPs *Deceptive Designs* fördern, kann dies für die Privatsphäre der Nutzenden kritisch sein. Der deutsche Marktführer ‚Cookiebot by Usercentrics' (Cookiebot, o. J.) erlaubt es beispielsweise nicht, die *Interface Interference* in der kostenlosen Version abzuschalten. Dies bedeutet, dass die Erstellung privatsphärefreundlicher Einwilligungserklärungen mit einer CMP oft unmöglich oder schwierig ist, selbst wenn Webseitenbetreibende dies wollen. Dies könnte eine mögliche Erklärung dafür sein, warum *Deceptive Designs* in Cookie-Einwilligungserklärungen immer noch so weitverbreitet sind.

Zusammenfassend lässt sich sagen, dass *Deceptive Designs* in den Standardvorlagen von CMPs üblich sind. Selbst wenn Webseitenbetreibende motiviert sind, Einwilligungserklärungen ohne *Deceptive Designs* zu erstellen, ist dies teilweise nicht möglich und CMPs verleiten Webseitenbetreibende eher dazu, weniger privatsphärefreundliche Cookie-Einwilligungserklärungen zu erstellen. Diese Erkenntnisse decken sich mit den Ergebnissen aus der Analyse von Toth et al. (2022), in der u. a. ebenfalls gezeigt wurde, dass die Standardvorlagen der CMPs häufig rechtswidrig sind und dass Webseitenbetreibende beim Erstellen von Einwilligungserklärungen auf der Webseite der CMPs einer Reihe an *Deceptive Designs* begegnen. Daher ist es essenziell, dass Webseitenbetreibende in die Lage versetzt werden, CMPs zu wählen, deren Vorlagen keine *Deceptive Designs* enthalten. Daraus lässt sich schließen, dass ein dringender Schritt zum Schutz der Privatsphäre der Nutzenden darin besteht, die CMPs zur Rechenschaft zu ziehen, da auch die Webseitenbetreibenden auf sie angewiesen sind.

4.4.5 Limitationen

Diese Studie hat einen explorativen Charakter, was einige Einschränkungen mit sich bringt, die im Folgenden beschrieben werden.

(1) Auswahl der untersuchten CMPs: Der Marktanteil von CMPs ist sehr dynamisch und hängt auch von der Größe der Webseiten ab (Hils et al., 2020). In dieser Studie wurde die Relevanz der untersuchten CMPs auf der Grundlage der bestehenden Literatur abgeleitet, die möglicherweise nicht den aktuellen Stand widerspiegelt. Daher sollten in Zukunft die relevanten CMPs erneut mithilfe eines Webcrawlers identifiziert werden.

(2) Eingeschränkte Analysen der Angebote der CMPs: In dieser Studie wurden nur Angebote von CMPs untersucht, die kostenlos waren und die keinen persönlichen Kontakt zu einem Vertriebsmitarbeitenden erforderten. Daher sind die Ergebnisse nicht für alle CMPs repräsentativ. Um eine bessere

Verallgemeinerbarkeit zu erreichen, sollten nach Möglichkeit alle relevanten CMPs analysiert werden. Es kann notwendig sein, zu diesem Zweck eine Coverstory zu verwenden, um das Verhalten der CMPs bei der Kontaktaufnahme nicht zu verzerren.

(3) Analysen der implementierten Cookie-Einwilligungserklärungen: In dieser Studie wurden nur Screenshots der Vorlagen für Cookie-Einwilligungserklärungen analysiert und nicht die tatsächlich auf einer Webseite implementierten Einwilligungserklärungen. Daher konnten die Forschenden nicht mit den Cookie- Einwilligungserklärungen interagieren und es war manchmal schwierig, zu beurteilen, inwieweit *Deceptive Designs* wie *Sneaking* oder *Forced Action* in den Einwilligungserklärungen enthalten waren. In der zukünftigen Forschung sollten die Einwilligungserklärungen tatsächlich in Webseiten implementiert werden, um weitere Analysen durchführen zu können.

(4) Momentaufnahme der Standard-Cookie-Einwilligungserklärungen: Es sollte auch beachtet werden, dass die Vorlagen, die in dieser Studie analysiert wurden, nur eine Momentaufnahme vom März 2022 darstellen. Hils et al. (Hils et al., 2020) haben bereits gezeigt, dass die CMP-Branche sehr dynamisch ist und sich die Relevanz einzelner CMPs und die Gestaltung der Einwilligungserklärungen in Zukunft ändern können. Es wäre interessant, zu analysieren, ob und wie die CMPs ihre Vorlagen anpassen (z. B. beeinflusst durch externe Ereignisse wie Gesetzesänderungen oder Gerichtsurteile).

(5) Einbindung von Webseitenbetreibenden: In dieser Studie wurde versucht, die Perspektive der Webseitenbetreibenden einzunehmen. In der zukünftigen Forschung sollten deren Perspektive sowie deren Interessen und Bedürfnisse jedoch detaillierter untersucht werden. Dies könnte durch eine direkte Befragung von Personen, die Webseiten betreiben, oder durch deren Beteiligung an der Erstellung von Einwilligungserklärungen mithilfe von CMPs geschehen.

5 Zusammenfassung, Beitrag der Arbeit und Ausblick

Privatsphärerisiken auf Webseiten stellen ein weitverbreitetes Phänomen dar, was darauf hindeutet, dass es auch für die Webseitenbetreibenden herausfordernd sein kann, diese zu beheben bzw. zu vermeiden. In dieser Arbeit wurden zwei konkrete Herausforderungen, denen Webseitenbetreibende gegenüberstehen, aus deren Perspektive untersucht. Damit sollte das übergeordnete Ziel der Arbeit adressiert werden, die Perspektive der bisher wenig berücksichtigten Gruppe der Webseitenbetreibenden zu untersuchen und aufzuzeigen, inwiefern diese zum Entstehen und Bestehen von Privatsphärerisiken auf Webseiten beitragen. Im Folgenden werden die Forschungsziele, das methodische Vorgehen und die Ergebnisse zusammengefasst sowie der Beitrag dieser Arbeit aufzeigt.

5.1 Zusammenfassung und Beitrag von Kapitel 3 (Ziel 1 & 2)

In Kapitel 3 wurde die Herausforderung für Webseitenbetreibende untersucht, bestehende Privatsphärerisiken auf ihren Webseiten zu beheben. Als Untersuchungsbeispiel für ein Privatsphärerisiko diente die fehlende IP-Anonymisierung von Google Analytics. Ziel war es zum einen, ein besseres Verständnis für die Herausforderung aus Sicht der Webseitenbetreibenden zu entwickeln (Ziel 1), und zum anderen, aufzuzeigen, wie Maßnahmen aussehen können, die Webseitenbetreibenden dabei zu unterstützen, bestehende Privatsphärerisiken auf ihren Webseiten zu beheben (Ziel 2). Um die Ziele zu adressieren, wurden drei Untersuchungen durchgeführt: Zunächst wurden 4594 Webseitenbetreibende durch E-Mails und Briefe über das bestehende Privatsphärerisiko (fehlende IP-Anonymisierung von Google Analytics) auf ihrer Webseite benachrichtigt und im Nachgang mithilfe einer Umfrage ($N = 477$) u. a. zum Problembewusstsein und zum Vorgehen bei der Behebung befragt. Die Rückmeldungen ($N = 1043$) der Webseitenbetreibenden wurden quantitativ und qualitativ analysiert, um mehr über die Hintergründe zu erfahren.

Sowohl die Umfrage als auch die Auswertung der Rückmeldungen zeigen, dass bestehende Privatsphärerisiken auf Webseiten, im untersuchten Fall die fehlende IP-Anonymisierung von Google Analytics, aus Sicht der Webseitenbetreibenden vielfältige Ursachen haben können. Eine zentrale Ursache ist das fehlende Bewusstsein der Webseitenbetreibenden für das bestehende Privatsphärerisiko. Darüber hinaus zählen auch unklare Zuständigkeiten, eine fehlerhafte technische Umsetzung und eine mangelnde Wartung der Webseite zu den Ursachen. Ist ihnen das Privatsphärerisiko erst einmal bewusst, müssen Webseitenbetreibende beim Beheben eine Reihe von Hürden überwinden. Diese sind abhängig von den Rahmenbedingungen bzw. dem Kontext der Webseitenbetreibenden. Zum Beispiel stellt der Mangel an Ressourcen – fehlende Zeit, um das Problem zu beheben, oder fehlendes Geld, um Externe damit zu beauftragen – für Privatpersonen oder Selbstständige eine Hürde dar. Webseitenbetreibende, die in größeren Unternehmen tätig sind, berichteten eher von der Hürde zäher Prozesse im Unternehmen oder von einem unübersichtlichen Webseiten-Code. Es wurde gezeigt, dass Webseitenbetreibende einen großen Unterstützungsbedarf bei der Behebung bestehender Privatsphärerisiken auf ihren Webseiten haben. In Kapitel 3 konnte gezeigt werden, dass die Benachrichtigung der Webseitenbetreibenden über ein bestehendes Privatsphärerisiko auf ihrer Webseite eine effektive Unterstützungsmaßnahme darstellt. Bei der Gestaltung der Benachrichtigungen sollten jedoch einige Faktoren, z. B. die Möglichkeit der Verifikation des Absenders, berücksichtigt werden, damit diese als vertrauenswürdig wahrgenommen werden. Die Ergebnisse dieses Kapitels veranschaulichen auch, dass es essenziell ist, bei der Entwicklung

von Maßnahmen die vielfältigen Hintergründe und Bedürfnisse der Webseitenbetreibenden zu berücksichtigen, damit diese tatsächlich wirkungsvoll sind.
Zusammenfassend lässt sich sagen, dass in Kapitel 3 gezeigt werden konnte, was die Ursachen für bestehende Privatsphärerisiken sind und welche Hürden Webseitenbetreibende bei der Behebung überwinden müssen. Dabei wird auch deutlich, dass die Hürden stark vom Kontext der Webseitenbetreibenden abhängen. Dieser kann sehr unterschiedlich sein und entsprechend müssen effektive Unterstützungsmaßnahmen angepasst werden.

5.2 Zusammenfassung und Beitrag von Kapitel 4 (Ziel 3 & 4)

In Kapitel 4 wurde die Herausforderung der Webseitenbetreibenden untersucht, die Entstehung neuer Privatsphärerisiken auf ihren Webseiten zu vermeiden. Als Untersuchungsbeispiel für ein Privatsphärerisiko dienten Cookie-Einwilligungserklärungen mit Gestaltungselementen, die Nutzende zur Zustimmung zu Cookies verleiten – sogenannten *Deceptive Designs*. Ziel war es zum einen, ein besseres Verständnis für die Herausforderung der Webseitenbetreibenden zu entwickeln, dieses Privatsphärerisiko zu vermeiden (Ziel 3), und zum anderen sollte aufgezeigt werden, wie Webseitenbetreibende darin unterstützt werden können, die Entstehung von Privatsphärerisiken auf ihren Webseiten zu vermeiden (Ziel 4). Um diese Ziele zu adressieren, wurden zwei Studien durchgeführt: Dazu wurden zunächst mit Studie 2a und 2b zwei aufeinanderfolgende Online-Experimente durchgeführt. Zunächst wurde die Perspektive der Nutzenden ($N = 376$) untersucht. Dazu interagierten Nutzende mit einem fiktiven Onlineshop, der für die unterschiedlichen Experimentalgruppen verschiedene Cookie-Einwilligungserklärungen enthielt. Im Anschluss wurden Nutzende u. a. zu ihrer Bewertung und zu ihren Präferenzen hinsichtlich der Cookie-Einwilligungserklärungen befragt. In Studie 2b wurden Webseitenbetreibende ($N = 195$) u. a. zu ihren Präferenzen bezüglich der Gestaltung von Cookie-Einwilligungserklärungen befragt. Außerdem wurden sie gebeten, eine von vier möglichen Cookie-Einwilligungserklärungen auszuwählen, wobei die Experimentalgruppe zusätzlich Informationen über die Nutzendenpräferenz sowie die Cookie-Zustimmungsrate (Ergebnisse aus Studie 2a) erhielt. Zur Erstellung von Einwilligungserklärungen greifen Webseitenbetreibende immer häufiger auf die Vorlagen von CMPs zurück. Um zu untersuchen, inwiefern Webseitenbetreibende mit diesen Vorlagen Einwilligungserklärungen ohne Privatsphärerisiken (*Deceptive Designs*) generieren können, wurden im Rahmen der Studie 3 die Vorlagen von 15 populären CMPs analysiert.
Die Ergebnisse des Online-Experiments mit Nutzenden zeigen, dass die Gestaltung von Einwilligungserklärungen einen Einfluss auf die Zustimmungsrate hat. Enthielten die Einwilligungserklärungen *Deceptive Designs*, akzeptierten mehr Nutzende alle Cookies, obwohl sie Gestaltungsvarianten präferierten, die keine *Deceptive Designs* enthalten. Webseitenbetreibende waren sich der Präferenzen der Nutzenden bezüglich der Gestaltung von Einwilligungserklärungen bewusst und schätzten diese korrekt ein. Jedoch wählte nur ein Teil der Webseitenbetreibenden entsprechende Einwilligungserklärungen aus. Einwilligungserklärungen mit *Deceptive Designs* wurden häufiger von Webseitenbetreibenden gewählt, die mit den durch Cookies gespeicherten Daten Einnahmen generieren. Dabei scheint die Popularität der Webseite eine untergeordnete Rolle zu spielen. Zentraler ist, ob das Geschäftsmodell bzw. die Werte der Organisation hinter der Webseite den Schutz der Privatsphäre der

Nutzenden bestärken oder nicht. Es konnte nicht gezeigt werden, dass die Bereitstellung von Informationen über die Nutzendenpräferenz bzw. das Nutzungsverhalten eine wirkungsvolle Maßnahme ist, um Webseitenbetreibende dazu zu bringen, Privatsphärerisiken zu vermeiden. Die Analyse der Vorlagen der CMPs zeigt, dass es für Webseitenbetreibende nur eingeschränkt möglich ist, damit Einwilligungserklärungen ohne *Deceptive Designs* zu erstellen. CMPs tragen daher möglicherweise stark zur Entstehung von Privatsphärerisiken auf Webseiten bei.

5.3 Zukünftige Forschung

Durch die vorliegende Arbeit wird ein erster explorativer Blick auf die bisher wenig untersuchte Gruppe der Webseitenbetreibenden ermöglicht. Es wurden deren Hintergründe, Interessen und Motivationen aufgezeigt sowie die Ursachen für Privatsphärerisiken und die Hürden bei deren Behebung identifiziert. Damit schafft diese Arbeit eine Reihe an Anknüpfungspunkten für die zukünftige Forschung, auf die im Folgenden eingegangen wird.

5.3.1 Webseitenbetreibende besser verstehen

Die Gruppe der Webseitenbetreibenden systematisch untersuchen: In der vorliegenden Arbeit wurden die Hintergründe von Webseitenbetreibenden anhand von drei Beispiel-Personas dargestellt. Inwiefern diese für die Gruppe von Webseitenbetreibend repräsentativ sind, ist jedoch unklar. In der zukünftigen Forschung sollten die Hintergründe von Webseitenbetreibenden systematisch untersucht werden. Dazu sollten Webseitenbetreibende über möglichst viele unterschiedliche Kanäle und Wege kontaktiert werden, um deren vielfältigen Hintergründen gerecht zu werden. Als mögliche Kanäle bieten sich Internetforen, direkte Ansprache über Nachrichten sowie indirekte Ansprache über Interessens- oder Berufsverbände an. Folgende Fragen gilt es dabei zu klären: Welche demographischen Daten haben die Webseitenbetreibenden? Warum betreiben sie eine Webseite? Welche Einstellungen haben sie bezüglich der Privatsphäre und wie ist ihr technisches und ihr Privatsphärewissen ausgeprägt?

Die Gruppe der Webseitenbetreibenden global untersuchen: In dieser Arbeit wurden ausschließlich in Deutschland tätige Webseitenbetreibende berücksichtigt. Webseitenbetreibende, die in anderen Ländern tätig sind, müssen gegebenenfalls andere datenschutzrechtliche Anforderungen erfüllen, womit andere Herausforderungen einhergehen können. Des Weiteren kann es sein, dass kulturelle Unterschiede zwischen Webseitenbetreibenden bestehen, die in verschiedenen Ländern leben. Die Forschung deutet daraufhin, dass Nutzende in Deutschland größere Privatsphärebedenken haben als z. B. Nutzende in den USA (Krasnova & Veltri, 2010). Daran schließt sich die Frage an, inwiefern Webseitenbetreibende aus verschiedenen Ländern ein unterschiedliches Bewusstsein und unterschiedliche Interessen bezüglich des Schutzes der Privatsphäre ihrer Nutzenden haben.

Die Gruppe der Webseitenbetreibenden im Detail verstehen: Aufbauend auf der systematischen Untersuchung der Webseitenbetreibenden bietet es sich an, Teilgruppen von Webseitenbetreibenden näher zu untersuchen, um ihre Herausforderungen im Detail zu verstehen. Zum Beispiel konnte in dieser Arbeit bereits gezeigt werden, dass Privatpersonen, die eine Webseite betreiben, mit anderen Herausforderungen konfrontiert sind als Webseitenbetreibende, die mit der Webseite ihr kleines Unternehmen repräsentieren. Eine in dieser Arbeit wiederholt auftauchende Teilgruppe sind Webseitenbetreibende, die die Webseite im Rahmen ihres Engagements in einem Verein betreiben. In

Deutschland gibt es über 600 000 eingetragene Vereine, von denen potenziell viele eine Webseite besitzen (Priemer, 2020).

Webseitenbetreibende als Individuen besser verstehen: In dieser Arbeit lag ein starker Fokus darauf, die Webseitenbetreibenden als Gruppe zu verstehen. Aus psychologischer Perspektive kann es von Interesse sein, Webseitenbetreibende auf Individualebene zu untersuchen. In dieser Arbeit gibt es erste Hinweise darauf, dass z. B. die Privatsphäremotivation ein möglicher Einflussfaktor ist, ob Webseitenbetreibende Privatsphärerisiken beheben. Es bietet sich an, motivationale Aspekte näher zu untersuchen. Zum Beispiel kann die Frage gestellt werden, inwiefern die Motivation der Webseitenbetreibenden, ihre eigene Privatsphäre zu schützen, im Zusammenhang mit der Motivation steht, die Privatsphäre anderer Nutzender zu schützen. Die Ergebnisse dieser Arbeit deuten auch daraufhin, dass Webseitenbetreibende zum Teil damit überfordert sind, Privatsphärerisiken zu beheben. Es könnte also interessant sein, die Selbstwirksamkeitserwartung von Webseitenbetreibenden zu untersuchen, um besser zu verstehen, wie solche individuellen Faktoren zu Privatsphärerisiken auf Webseiten beitragen. In der bisherigen Forschung zu Nutzenden wurde bereits gezeigt, dass psychologische Bedürfnisse, z. B. das Bedürfnis nach Sicherheit oder Kompetenzerleben, bei der Gestaltung interaktiver Systeme berücksichtigt werden sollten. Erstellen oder warten Webseitenbetreibende eine Webseite, werden sie dabei genau genommen auch zu Nutzenden eines Systems. Auch in diesem Kontext könnte es interessant sein, relevante psychologische Bedürfnisse von Webseitenbetreibenden zu identifizieren, um besser zu verstehen, ob und wie deren Befriedigung zu privatsphäreförderlichem Verhalten beiträgt.

5.3.2 Herausforderungen der Webseitenbetreibenden untersuchen

Herausforderungen der Webseitenbetreibenden systematisch untersuchen: In dieser Arbeit wurden die Herausforderungen der Webseitenbetreibenden exemplarisch und explorativ an zwei konkreten Beispielen untersucht. In der zukünftigen Forschung sollten Herausforderungen bezüglich des Schutzes der Privatsphäre von Nutzenden systematisch untersucht werden. Dies würde es unter anderem erlauben, besser zu verstehen, welche Herausforderungen von besonderer Priorität sind. Dazu könnte zunächst mit einem qualitativen und explorativen Ansatz, z. B. mithilfe von Interviews mit Webseitenbetreibenden, der Möglichkeitsraum der Herausforderungen aufgespannt werden. Im Anschluss ließe sich die Bewertung sowie die Prävalenz der identifizierten Herausforderungen z. B. mithilfe einer Umfrage quantifizieren.

Weitere Herausforderungen untersuchen: Mit der Behebung der IP-Anonymisierung von Google Analytics wurde in dieser Arbeit nur ein Beispiel untersucht, das zum Zeitpunkt der Studie einen DSGVO-Verstoß darstellte. In der DSGVO und im TTSDG werden jedoch eine Reihe weiterer Anforderungen gestellt, die Webseitenbetreibende erfüllen müssen. Zum Beispiel haben Nutzende nach dem Auskunftsrecht (Art. 15 DSGVO) das Recht, von Webseitenbetreibenden Auskunft über potenziell erhobene Daten zu erhalten. Wie und ob Webseitenbetreibende diesem Recht nachkommen und welche Hürden sie dabei überwinden müssen, gilt es, in der zukünftigen Forschung zu klären.

5.3.3 Entwicklung und Evaluation von Unterstützungsmaßnahmen für Webseitenbetreibende

Entwicklung und Evaluation von Unterstützungsmaßnahmen für verschiedene Webseitenbetreibende: In dieser Arbeit wurden Empfehlungen für konkrete Maßnahmen zur Unterstützung von Webseitenbetreibenden bei der Behebung von Privatsphärerisiken vorgeschlagen. Dabei wurden einzelne Maßnahmen wie Benachrichtigungen bereits evaluiert. In der zukünftigen Forschung gilt es nun, weitere Maßnahmen wie Informationskampagnen zu evaluieren. Des Weiteren müssen Maßnahmen an die Bedürfnisse verschiedener Webseitenbetreibenden angepasst und entsprechend evaluiert werden. Zum Beispiel könnten in der zukünftigen Forschung gezielt Webseitenbetreibende mit kleinen Betrieben über deren Berufsverbände durch Benachrichtigungen für Privatsphärerisiken sensibilisiert werden.

Privatsphärefreundliche Alternativen entwickeln: Webseitenbetreibende sind häufig auf die Dienste von Drittanbietern angewiesen, um Funktionalitäten auf ihren Webseiten zu ermöglichen. Selbst wenn es in ihrem Interesse ist, die Privatsphäre der Nutzenden zu schützen, sehen sie teilweise keine Alternativen. Diese gilt es, zu entwickeln bzw. weiterzuentwickeln und den Webseitenbetreibenden bereitzustellen. Dazu gehören beispielsweise privatsphärefreundliche Vorlagen für Einwilligungserklärungen.

Anpassung von Unterstützungsmaßnahmen für andere Gruppen auf Webseitenbetreibende: Die S&P-Forschung bietet bereits eine Vielzahl an Lösungen, um Nutzende dabei zu unterstützen, ihre Privatsphäre besser zu schützen (Stöver et al., 2020, z. B. 2021). Es könnte sinnvoll sein, diese Lösungen dahingehen zu untersuchen, ob sie sich auch auf die Bedürfnisse von Webseitenbetreibenden übertragen und anpassen lassen. Eine Möglichkeit stellt dabei ein sogenannter Privatsphäreassistent dar (Stöver et al., 2020). Für Nutzende hat dieser die Funktion, deren Privatsphäreeinstellungen zu kennen und sie dabei zu unterstützen, diese in ihrem digitalen Alltag umzusetzen (Stöver et al., 2020). Für Webseitenbetreibende könnte so ein Assistent die Funktion übernehmen, diese bei der Erstellung und dem Betrieb privatsphärefreundlicher Webseiten zu unterstützen. Zum Beispiel könnte der Assistent auf bestehende Privatsphärerisiken auf der Webseite aufmerksam machen und Alternativen anbieten. Durch neue Rechtsprechungen und sich wandelnde Technologien ändern sich die Anforderungen an eine privatsphärefreundliche Webseite ständig. Der Privatsphäreassistent für Webseitenbetreibende könnte die Webseite also regelmäßig bezüglich der aktuellen Rechtsprechung und der technologischen Entwicklung prüfen und den Webseitenbetreibenden bei Handlungsbedarf konkrete Hinweise mit Lösungsvorschlägen mitteilen.

5.4 Implikationen für Praxis

Die Ergebnisse dieser Arbeit zeigen, dass Webseitenbetreibende einen großen Unterstützungsbedarf haben, um bestehende Privatsphärerisiken auf ihren Webseiten zu beheben und die Entstehung neuer Privatpshärerisiken zu vermeiden. Daraus ergeben sich eine Reihe an Implikationen bzw. Handlungsbedarfe für die Praxis. Damit sind potenzielle eine Vielzahl an Akteur:innen gemeint, denn das Thema der Privatsphäre ist so vielschichtig, dass Lösungsansätze auf verschiedenen Ebenen ansetzen müssen. Die im Folgenden vorgestellten Implikationen richten sich also an Datenschutzbehörden und Datenschutzbeauftragte, Medien, Politik sowie Interessensvertretungen einzelner Webseitenbetreibende, wie Berufsverbände. Diese Arbeit hat außerdem gezeigt, dass die Hintergründe

von Webseitenbetreibenden vielfältig sind, entsprechend müssen sie über diverse Kanäle ihren Bedürfnissen entsprechend adressiert werden. Das Ziel sollte sein Webseitenbetreibenden dazu zu befähigen bewusste Entscheidungen bezüglich des Schutzes der Privatsphäre ihrer Nutzenden treffen und demnach auch handeln zu können. Dazu bieten sich mehrere Ansätze an, die aus den Erkenntnissen dieser Arbeit abgeleitet und im Folgenden vorgestellt werden:

Allgemeines Bewusstsein für Privatsphärerisiken bei der Erstellung von Webseiten stärken: Die Ergebnisse aus Kapitel 3 legen nahe, dass eine zentrale Ursache für bestehende Privatsphärerisiken auf Webseiten fehlendes Bewusstsein der Webseitenbetreibenden ist. Webseitenbetreibenden sollten dafür sensibilisiert werden, dass sie bei der Gestaltung einer Webseite potenziell die Privatsphäre der Nutzenden einschränken. Dies kann zum Beispiel dadurch geschehen, dass Webseitenbetreibenden aufzeigt wird, welche konkreten Konsequenzen für ihre Privatsphäre Nutzende beim Besuch der entsprechenden Webseite fürchten müssen. Dabei ist es jedoch wichtig sowohl in der Art als auch im Weg der Ansprache die vielfältigen Hintergründe von Webseitenbetreibenden zu berücksichtigen. Im Gegensatz zu Beispielsweiße Software oder App Entwickler:innen verfügen nicht alle Webseitenbetreibenden über ein fundiertes technisches Wissen. Deshalb muss zum Beispiel die Darstellung oder Formulierung entsprechender Maßnahmen auch für technische Laien verständlich sein.

Webseitenbetreibenden konkrete Privatsphärerisiken zusammen mit Handlungsmöglichkeit aufzeigen: Die Ergebnisse der Arbeit zeigen, dass Webseitenbetreibende häufig nicht über umfangreiche zeitliche Kapazitäten verfügen sich ihrer Webseite und erst recht nicht Privatsphäre Themen zu widmen. Gleichzeitig konnte gezeigt werden, dass die Benachrichtigung über ein bestehendes Privatsphärerisiko mit einer entsprechenden Anleitung zur Behebung des Risikos eine effektive Maßnahme ist. Daraus leitet sich die Empfehlung ab, Webseitenbetreibende über konkret bestehende Risiken auf ihren Webseiten aufmerksam zu machen. Das kann z. B. durch Benachrichtigungen oder Prüftools geschehen. Um tatsächlich eine Änderung hervorzurufen, ist es jedoch essenziell, den Webseitenbetreibenden aufzuzeigen, wie sie das Problem konkret lösen können. Das kann entweder durch Anleitungen in Form von Checklisten oder Videos oder durch persönlichen Support geschehen.

Webseitenbetreibende im Entscheidungsprozess unterstützen: Aus früherer Forschung ist bekannt, dass Webseitenbetreibende meist auf Standarddienste für ihre Webseiten zurückgreifen. Drittanbieter wie CMPs werben teilweise damit, die Privatsphäre der Nutzenden zu schützen. Die Ergebnisse der Arbeit zeigen jedoch, dass diese Webseitenbetreibende vielmehr dazu verleiten, die Privatsphäre der Nutzenden einzuschränken. Für Webseitenbetreibende kann es schwer sein, die tatsächliche Intention von Drittanbietern hinsichtlich Privatsphäreaspekten korrekt einzuschätzen und die Implikationen für die Privatsphäre der Nutzenden abzuschätzen, wenn sie die Dienste von Drittanbietern einsetzen. Hier kann es sinnvoll sein, den Webseitenbetreibenden mit transparenzfördernden Maßnahmen eine informierte Entscheidung bei der Auswahl eines Drittanbieterdienstes zu ermöglichen. Eine Möglichkeit könnten sogenannte Privacy Icons sein, die bereits für Nutzende erforscht wurden (z. B. Stöver et al., 2021). Angewandt für Webseitenbetreibende könnten diese Icons angeben, welche Privatsphärerisiken einzelne Drittanbieter beinhalten, und damit eine Entscheidungsgrundlage für Webseitenbetreibende bieten.

Webseitenbetreibende entlasten: Die Ergebnisse der Arbeit zeigen, dass Webseitenbetreibende, insbesondere diejenigen, die kleine Webseiten betreiben, damit überfordert sind, die Privatsphäre ihrer Nutzenden zu schützen. Ein Ansatz, um Webseitenbetreibende zu entlasten, kann sein, Drittanbieterdienste hier mehr in die Verantwortung zu ziehen. Das kann z. B. durch eine stärkere Kontrolle der Angebote der Drittanbieter dahingehend, ob diese den Privacy-by-Design Prinzipien folgen, geschehen. Außerdem sollten Drittanbieter daran gehindert werden, falsche Versprechungen zu machen: Wenn es nicht ihre Intention ist, die Privatsphäre der Nutzenden zu schützen, sollten sie dies nicht anpreisen dürfen.

5.5 Schlussfolgerung

Ursprünglich wurden Webseiten von Berners-Lee erfunden, um den Austausch von Informationen zwischen Forschenden zu ermöglichen. Heutzutage werden Webseiten auch genutzt, um mit ihnen bzw. mit den darüber erhobenen Daten der Nutzenden Geld zu verdienen. Ein Beispiel dafür sind Nachrichten-Webseiten, die in der Kritik stehen, sich durch Einnahmen aus exzessivem Tracking zu finanzieren. Gleichzeitig ist es heutzutage für die meisten Menschen, die über minimales technisches Wissen sowie einen Computer mit Internetzugang verfügen, möglich, mithilfe von Vorlagen eine Webseite zu erstellen. Das Erstellen von Webseiten kann als Mittel der digitalen Mitbestimmung genutzt werden, mit dem Menschen Informationen mit der Öffentlichkeit teilen und für Themen einstehen können. Die Ergebnisse dieser Arbeit bestärken diese Annahmen, indem sie zeigen, dass Webseitenbetreibende vielfältige Hintergründe haben und ihre Webseiten aus den unterschiedlichsten Beweggründen betreiben. Gleichzeitig tragen Webseitenbetreibende die Verantwortung mit, die Privatsphäre von Nutzenden zu schützen, denn sie können mit ihren Entscheidungen – z. B. mit der Entscheidung, Dienste von gewissen Drittanbietern auf ihren Webseiten zu integrieren – Einfluss darauf nehmen, ob und welche Daten von Nutzenden gesammelt und weitergeben werden. Die Erkenntnisse dieser Arbeit zeigen, dass Webseitenbetreibende einen großen Unterstützungsbedarf haben, um bestehende Privatsphärerisiken auf ihren Webseiten zu beheben und die Entstehung von neuen Privatsphärerisiken zu vermeiden. Es gilt, entsprechende Maßnahmen den vielfältigen Hintergründen der Webseitenbetreibenden anzupassen. Maßnahmen, die bereits für andere Personengruppen, die Systeme entwickeln und betreiben, evaluiert wurden, scheinen nur bedingt für Webseitenbetreibende anwendbar, denn diese unterscheiden sich in mehreren Aspekten voneinander. Zum Beispiel verfügen Webseitenbetreibende nur teilweise über fundiertes technisches Wissen. Auch ist es notwendig, den Fokus auf die Gruppe der Webseitenbetreibenden zu lenken und diese konkret zu unterstützen, da Webseitenbetreibe einen essenziellen Beitrag zum Schutz der Privatsphäre der Nutzenden leisten können. Es gilt also, sie zu befähigen, bewusste Entscheidungen bezüglich der Privatsphäre der Nutzenden treffen und entsprechend handeln zu können.

Literaturverzeichnis

Abbate, J. (2010). Privatizing the internet: Competing visions and chaotic events, 1987–1995. *IEEE Annals of the History of Computing*, *32*(1), 10–22.

Acar, Y., Fahl, S., & Mazurek, M. L. (2016). You are not your developer, either: A research agenda for usable security and privacy research beyond end users. *2016 IEEE Cybersecurity Development (SecDev)*, 3–8.

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2018). Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys*, *50*(3), 1–41. https://doi.org/10.1145/3054926

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40–46. https://doi.org/10.1145/322796.322806

AdOpt. (o. J.). *AdOpt—Plataforma de Adequação a LGPD - AdOpt*. Abgerufen 23. März 2022, von https://goadopt.io/en/

Agrawal, N., Binns, R., Van Kleek, M., Laine, K., & Shadbolt, N. (2021). Exploring Design and Governance Challenges in the Development of Privacy-Preserving Computation. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3411764.3445677

Alomar, N., & Egelman, S. (2022). Developers Say the Darnedest Things: Privacy Compliance Processes Followed by Developers of Child-Directed Apps. *Proceedings on Privacy Enhancing Technologies*, *4*, 250–273.

Altman, I. (1977). Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues*.

Arias-Cabarcos, P., Khalili, S., & Strufe, T. (2022). „Surprised, Shocked, Worried": User Reactions to Facebook Data Collection from Third Parties. *arXiv preprint arXiv:2209.08048*.

Armstrong, M. (2021, August 6). *How Many Websites Are There?* https://www.statista.com/chart/19058/number-of-websites-online/

Balebako, R., Marsh, A., Lin, J., Hong, J., & Faith Cranor, L. (2014). The Privacy and Security Behaviors of Smartphone App Developers. *Proceedings 2014 Workshop on Usable Security*. Workshop on Usable Security, San Diego, CA. https://doi.org/10.14722/usec.2014.23006

Bermejo Fernandez, C., Chatzopoulos, D., Papadopoulos, D., & Hui, P. (2021). This Website Uses Nudging: MTurk Workers' Behaviour on Cookie Consent Notices. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW2), 1–22. https://doi.org/10.1145/3476087

BfDI. (o. J.). *Einwilligung*. Der Bundesbeauftrage für Datenschutz und Informationsfreiheit. Abgerufen 15. Januar 2023, von https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Datenschutz/Einwilligung.html

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., & Shadbolt, N. (2018). Third Party Tracking in the Mobile Ecosystem. *Proceedings of the 10th ACM Conference on Web Science*, 23–31. https://doi.org/10.1145/3201064.3201089

Binns, R., Zhao, J., Kleek, M. V., & Shadbolt, N. (2018). Measuring Third-party Tracker Power across Web and Mobile. *ACM Transactions on Internet Technology*, *18*(4), 1–22. https://doi.org/10.1145/3176246

Bocksch, R. (2022, Juni 10). *PayPal ist die Nummer Eins der Online-Bezahldienste*. Statista. https://de.statista.com/infografik/23357/anteil-der-befragten-die-diese-online-bezahldienste-nutzen/

Bollinger, D., Kubicek, K., Cotrini, C., & Basin, D. (2022). Automating Cookie Consent and GDPR Violation Detection. *31st USENIX Security Symposium (USENIX Security 22)*, 1–18. https://www.usenix.org/conference/usenixsecurity22/presentation/bollinger

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), 77–101.

Brignull, H. (o. J.). *Deceptive Design—User interfaces crafted to trick you*. Abgerufen 28. März 2022, von https://www.deceptive.design

Buchner, A., Erdfelder, E., Faul, F., & Lang, A.-G. (2014). *G*Power 3.1.9.2* (3.1). https://www.psychologie.hhu.de/arbeitsgruppen/allgemeine-psychologie-und-arbeitspsychologie/gpower

Bundesministerium der Verteidigung. (2023). *Cyber-Sicherheitsrat*. 12.01.2023

Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV). (2022). *Impressumspflicht*. https://www.bmuv.de/themen/verbraucherschutz-im-bmuv/digitaler-verbraucherschutz/impressumspflicht

Canali, D., Balzarotti, D., & Francillon, A. (2013). The role of web hosting providers in detecting compromised websites. *Proceedings of the 22nd International Conference on World Wide Web*, 177–188. https://doi.org/10.1145/2488388.2488405

CCM19. (o. J.). *Was Sie schon immer über Cookie Banner wissen (s)wollten!* Abgerufen 23. März 2022, von https://www.ccm19.de/cookie-banner.html

CERN. (2023). *The birth of the Web*. https://home.cern/science/computing/birth-web

Çetin, O., Ganán, C., Altena, L., Tajalizadehkhoob, S., & van Eeten, M. (2018). Let me out! Evaluating the effectiveness of quarantining compromised users in walled gardens. *14th Symposium on Usable Privacy and Security (SOUPS 2018)*, 251–263.

Çetin, O., Ganán, C., Korczynski, M., & van Eeten, M. (2017). Make Notifications Great Again: Learning How to Notify in the Age of Large-Scale Vulnerability Scanning. *Workshop on the Economics of Information Security (WEIS)*, 23.

Chowdhury, P. D., Hallett, J., Patnaik, N., Tahaei, M., & Rashid, A. (2021). Developers Are Neither Enemies Nor Users: They Are Collaborators. *2021 IEEE Secure Development Conference (SecDev)*, 47–55. https://doi.org/10.1109/SecDev51306.2021.00023

Clickworker GmbH. (2022). *AI Training Data and other Data Management Services*. https://www.clickworker.com/

Cookiebot. (o. J.). *Ist meine Webseite datenschutz-konform?* Abgerufen 23. März 2022, von https://www.cookiebot.com/de/

CookieHub ehf. (o. J.). *Cookie Consent Management-Plattform*. Abgerufen 23. März 2022, von https://www.cookiehub.com/de

CookieYes. (o. J.). *Consent Management Platform (CMP): How Does it Work?* Abgerufen 23. März 2022, von https://www.cookieyes.com/blog/consent-management-platform/

Crownpeak Technology, Inc. (o. J.). *Digital Experience Platform & Enterprise CMS*. Abgerufen 23. März 2022, von https://www.crownpeak.com//

Dambra, S., Sanchez-Rola, I., Bilge, L., & Balzarotti, D. (2022). When Sally Met Trackers: Web Tracking From the Users' Perspective. *31st USENIX Security Symposium (USENIX Security 22)*, 2189–2206.

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). We Value Your Privacy ... Now

Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. *Network and Distributed System Security Symposium (NDSS 2019)*. https://doi.org/10.14722/ndss.2019.23378

Döring, N., & Bortz, J. (2016). *Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften* (5. vollständig überarbeitete, aktualisierte und erweiterte Auflage). Springer. https://doi.org/10.1007/978-3-642-41089-5

DSGVO, (2016). https://dejure.org/gesetze/DSGVO/1.html

Durumeric, Z., Li, F., Kasten, J., Amann, J., Beekman, J., Payer, M., Weaver, N., Adrian, D., Paxson, V., Bailey, M., & Halderman, J. A. (2014). The Matter of Heartbleed. *Proceedings of the 2014 Internet Measurement Conference*, 475–488. https://doi.org/10.1145/2663716.2663755

Englehardt, S., & Narayanan, A. (2016). Online Tracking: A 1-million-site Measurement and Analysis. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1388–1401. https://doi.org/10.1145/2976749.2978313

European Data Protection Supervisor. (2022a). *Datenschutz*. https://edps.europa.eu/data-protection/data-protection_de

European Data Protection Supervisor. (2022b). *Über den EDSB*. https://edps.europa.eu/ueber/about-us_de

Fachverband deutscher Webseiten-Betreiber. (2017). *Webseitenbetreiber*. https://fdwb.de/webseitenbetreiber/

Franke, T., Attig, C., & Wessel, D. (2019). A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human–Computer Interaction*, *35*(6), 456–467. https://doi.org/10.1080/10447318.2018.1456150

G2. (o. J.). *Best Consent Management Platforms*. Abgerufen 28. März 2022, von https://www.g2.com/categories/consent-management-platform-cmp

Ghostery, Inc. (2022). *What is web tracking & How can I browse safely?* https://www.ghostery.com/blog/what-is-web-tracking-how-can-i-browse-safely

Ginosar, A., & Ariel, Y. (2017). An analytical framework for online privacy research: What is missing? *Information & Management*, *54*(7), 948–957. https://doi.org/10.1016/j.im.2017.02.004

Google. (o. J.). *Google Fonts*. Fonts Knowledge. Abgerufen 12. Januar 2023, von https://fonts.google.com/knowledge

Google. (2020). *IP Anonymization (or IP masking) in Universal Analytics—Analytics Help*. https://support.google.com/analytics/answer/2763052?hl=en

Google. (2023). *Google Ads: Definition*. https://support.google.com/google-ads/answer/6319?hl=de

Gradow, L., & Greiner, R. (2021). *Quick Guide Consent-Management*. Springer Gabler.

Graßl, P., Schraffenberger, H., Zuiderveen Borgesius, F., & Buijzen, M. (2021). Dark and Bright Patterns in Cookie Consent Requests. *Journal of Digital Social Research*, *3*(1), 1–38. https://doi.org/10.33621/jdsr.v3i1.54

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (S. 1–14). Association for Computing Machinery. https://doi.org/10.1145/3173574.3174108

Gulati, S., Sousa, S., & Lamas, D. (2019). Design, development and evaluation of a human-computer trust scale. *Behaviour & Information Technology*, *38*(10), 1004–1015. https://doi.org/10.1080/0144929X.2019.1656779

Guo, F. Y., Shamdasani, S., & Randall, B. (2011). Creating effective personas for product design: Insights from

a case study. *International Conference on Internationalization, Design and Global Development*, 37–46.

Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S., & Balissa, A. (2018). Privacy by designers: Software developers' privacy mindset. *Empirical Software Engineering*, *23*(1), 259–289. https://doi.org/10.1007/s10664-017-9517-1

Hemmerich, W. (2023). *StatistikGuru: Bonferroni-Korrektur*. StatistikGuru.

Hennig, A., Dietmann, H., Lehr, F., Mutter, M., Volkamer, M., & Mayer, P. (2022). "Your Cookie Disclaimer is Not in Line with the Ideas of the GDPR. Why?". In N. Clarke & S. Furnell (Hrsg.), *Human Aspects of Information Security and Assurance* (Bd. 658, S. 218–227). Springer International Publishing. https://doi.org/10.1007/978-3-031-12172-2_17

Hennig, A., Neusser, F., Pawelek, A. A., Herrmann, D., & Mayer, P. (2022). Standing out among the daily spam: How to catch website owners' attention by means of vulnerability notifications. *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, 1–8. https://doi.org/10.1145/3491101.3519847

Hils, M., Woods, D. W., & Böhme, R. (2020). Measuring the emergence of consent management on the web. *Proceedings of the ACM Internet Measurement Conference*, 317–332.

HmbBfDI. (2021, November 30). *Das TTDSG*. Datenschutz-Hamburg.de. https://datenschutz-hamburg.de/pages/ttdsg/

IAB, E. (o. J.). *Transparency & Consent Framework – Policies Version 2020-08-24.3.2*. IAB Europe. Abgerufen 28. März 2022, von www.iabeurope.eu

IBM. (2020). *SPSS Software* (Version 28). https://www.ibm.com/analytics/spss-statistics-software

Kampanos, G., & Shahandashti, S. F. (2021). Accept All: The Landscape of Cookie Banners in Greece and the UK. In A. Jøsang, L. Futcher, & J. Hagen (Hrsg.), *ICT Systems Security and Privacy Protection* (S. 213–227). Springer International Publishing.

Kant, T. (2021). Identity, Advertising, and Algorithmic Targeting: Or How (Not) to Target Your "Ideal User". *MIT Case Studies in Social and Ethical Responsibilities of Computing*. https://doi.org/10.21428/2c646de5.929a7db6

Karaj, A., Macbeth, S., Berson, R., & Pujol, J. M. (2019). WhoTracks .Me: Shedding light on the opaque world of online tracking. *ArXiv Preprint ArXiv:1804.08959*. http://arxiv.org/abs/1804.08959

Kaur, M., van Eeten, M., Janssen, M., Borgolte, K., & Fiebig, T. (2021). Human Factors in Security Research: Lessons Learned from 2008-2018. *ArXiv Preprint ArXiv:2103.13287*. http://arxiv.org/abs/2103.13287

Kevel. (o. J.). *Consent Management Platform (CMP) Tracker*. Abgerufen 28. März 2022, von https://www.kevel.com/cmp

Krasnova, H., & Veltri, N. F. (2010). Privacy calculus on social networking sites: Explorative evidence from Germany and USA. *Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS 2010)*, 1–10. https://doi.org/10.1109/HICSS.2010.307

Krisam, C., Dietmann, H., Volkamer, M., & Kulyk, O. (2021). Dark Patterns in the Wild: Review of Cookie Disclaimer Designs on Top 500 German Websites. In *European Symposium on Usable Security 2021* (S. 1–8). Association for Computing Machinery. https://doi.org/10.1145/3481357.3481516

Lackes, R., Siepermann, M., Kollmann, T., & Sjurts, I. (2018). *World Wide Web (WWW)*. https://wirtschaftslexikon.gabler.de/definition/world-wide-web-www-49260

Landgericht Dresden, Pub. L. No. Urteil v. 11.01.2019-Az.: 1a O 1582/18 (2019). https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=LG%20Dresden&Datum=2019-01-

11&Aktenzeichen=1a%20O%201582%2F18

Laufer, R., & Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of social Issues*, *33*(3).

Leiner, D. J. (2014). *SoSci Survey* (Version 2.5. 00-i, Bd. 30). https://www. soscisurvey. de

Lenz, C., Garling, K., Manz, R., & Hecht, A. (2022, Februar 22). *Haftung bei der Weitergabe dynamischer IP-Adressen über Google Fonts*. dhpg. https://www.dhpg.de/de/newsroom/blog/haftung-weitergabe-ip-adressen-ueber-google-fonts

Leon, P. G., Cranor, L. F., McDonald, A. M., & McGuire, R. (2010). Token attempt: The misrepresentation of website privacy policies through the misuse of p3p compact policy tokens. *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society*, 93–104. https://doi.org/10.1145/1866919.1866932

Li, F., Durumeric, Z., Czyz, J., Karami, M., Bailey, M., McCoy, D., Savage, S., & Paxson, V. (2016). You've Got Vulnerability: Exploring Effective Vulnerability Notifications. *25th USENIX Security Symposium (USENIX Security 16)*, 1033–1050.

Li, F., Ho, G., Kuan, E., Niu, Y., Ballard, L., Thomas, K., Bursztein, E., & Paxson, V. (2016). Remedying Web Hijacking: Notification Effectiveness and Webmaster Comprehension. *Proceedings of the 25th International Conference on World Wide Web - WWW '16*, 1009–1019. https://doi.org/10.1145/2872427.2883039

Libert, T., & Nielsen, R. K. (2018). *Third-Party Web Content on EU News Sites: Potential Challenges and Paths to Privacy Improvement*. https://timlibert.me/pdf/Libert_Nielsen-2018-Third_Party_Content_EU_News_GDPR.pdf

Maass, M., Stöver, A., Pridöhl, H., Bretthauer, S., Herrmann, D., Hollick, M., & Spiecker, I. (2021). Effective Notification Campaigns on the Web: A Matter of Trust, Framing, and Support. *30th USENIX Security Symposium (USENIX Security 21)*, 2489–2506.

Maass, M., Wichmann, P., Pridöhl, H., & Herrmann, D. (2017). Privacyscore: Improving privacy and security via crowd-sourced benchmarks of websites. *Annual Privacy Forum*, 178–191.

Machuletz, D., & Böhme, R. (2020). Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. *Proceedings on Privacy Enhancing Technologies*, *2020*(2), 481–498. https://doi.org/10.2478/popets-2020-0037

Mager, S., & Kranz, J. (2021). On the Effectiveness of Overt and Covert Interventions in Influencing Cookie Consent: Field Experimental Evidence. *Proceedings of the 2021 International Conference on Information Systems (ICIS)*. https://aisel.aisnet.org/icis2021/cyber_security/cyber_security/5

Marky, K., Voit, A., Stöver, A., Kunze, K., Schröder, S., & Mühlhäuser, M. (2020). "I don't know how to protect myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, 1–11. https://doi.org/10.1145/3419249.3420164

Marky, K., Zimmermann, V., Stöver, A., Hoffmann, P., Kunze, K., & Mühlhäuser, M. (2020). All in One! User Perceptions on Centralized IoT Privacy Settings. *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–8. https://doi.org/10.1145/3334480.3383016

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), 1–32. https://doi.org/10.1145/3359183

Mathur, A., Kshirsagar, M., & Mayer, J. (2021). What Makes a Dark Pattern... Dark?: Design Attributes, Normative Considerations, and Measurement Methods. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–18. https://doi.org/10.1145/3411764.3445610

Matomo. (o. J.). matomo.org.

Matte, C., Bielova, N., & Santos, C. (2020). Do Cookie Banners Respect my Choice? : Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. *2020 IEEE Symposium on Security and Privacy (SP)*, 791–809. https://doi.org/10.1109/SP40000.2020.00076

Metzger, J., Lackes, R., Siepermann, M., Kollmann, T., & Sjurts, I. (2018). *Definition: Was ist „Internet"?* https://wirtschaftslexikon.gabler.de/definition/internet-37192

Mhaidli, A. H., Zou, Y., & Schaub, F. (2019). ``We Can't Live Without Them!'' App Developers' Adoption of Ad Networks and Their Considerations of Consumer Risks. *15th Symposium on Usable Privacy and Security (SOUPS 2019)*, 225–244.

Microsoft. (2007). *OneDrive* (22.238.1114.0002). https://www.microsoft.com/de-de/microsoft-365/onedrive/online-cloud-storage

Microsoft. (2018). *Microsoft Excel* (2019 (16.0)). https://office.microsoft.com/excel

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3313831.3376321

Nurgalieva, L., Frik, A., & Doherty, G. (2021). WiP: Factors Affecting the Implementation of Privacy and Security Practices in Software Development: A Narrative Review. *Proceedings of the 8th Annual Symposium on Hot Topics in the Science of Security (HotSoS 2021)*.

Pennsylvania State University, Xu, H., Dinev, T., Florida Atlantic University, Smith, J., Miami University, Hart, P., & Florida Atlantic University. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems*, *12*(12), 798–824. https://doi.org/10.17705/1jais.00281

Pew Research Center. (2019). *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*.

Priemer, J. (2020, April). *ZiviZ-Survey: Vereine*. https://www.ziviz.de/ziviz-survey/vereine

Pruitt, J., & Grudin, J. (2003). Personas: Practice and theory. *Proceedings of the 2003 Conference on Designing for User Experiences*, 1–15.

Purcell, K., Brenner, J., & Rainie, L. (2023). *Search Engine Use 2012*. Pew Research Center's Internet & American Life Project.

Reuter, C., Iacono, L. L., & Benlian, A. (2022). A quarter century of usable security and privacy research: Transparency, tailorability, and the road ahead. *Behaviour & Information Technology*, *41*(10), 2035–2048. https://doi.org/10.1080/0144929X.2022.2080908

Samat, S., Acquisti, A., & Babcock, L. (2017). Raise the Curtains: The Effect of Awareness About Targeting on Consumer Attitudes and Purchase Intentions. *13th Symposium on Usable Privacy and Security (SOUPS 2017)*, 299–319.

Sauro, J. (2015). SUPR-Q: A Comprehensive Measure of the Quality of the Website User Experience. *Journal of Usability Studies*, *10*(2), 19.

Shiller, B. R. (2020). Approximating purchase propensities and reservation prices from broad consumer tracking.

International Economic Review, *61*(2), 847–870. https://doi.org/10.1111/iere.12442

Singh, A. K., Upadhyaya, N., Seth, A., Hu, X., Sastry, N., & Mondal, M. (2022). What Cookie Consent Notices Do Users Prefer: A Study In The Wild. *Proceedings of the 2022 European Symposium on Usable Security*, 28–39. https://doi.org/10.1145/3549015.3555675

SmartLife - Online UG. (o. J.). *Cookie-Banner-Generator*. Abgerufen 23. März 2022, von https://www.smartlife-online.de/cb/

Smith, Jeff, Dinev, Tamara, & Xu, Heng. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989. https://doi.org/10.2307/41409970

Soe, T. H., Nordberg, O. E., Guribye, F., & Slavkovik, M. (2020). Circumvention by design—Dark patterns in cookie consent for online news outlets. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society* (S. 1–12). ACM. https://dl.acm.org/doi/10.1145/3419249.3420132

Stock, B., Pellegrino, G., Li, F., Backes, M., & Rossow, C. (2018). Didn't You Hear Me? - Towards More Successful Web Vulnerability Notifications. *Network and Distributed System Security Symposium (NDSS 2018)*. Network and Distributed System Security Symposium, San Diego, CA. https://doi.org/10.14722/ndss.2018.23171

Stock, B., Pellegrino, G., Rossow, C., Johns, M., & Backes, M. (2016). Hey, You Have a Problem: On the Feasibility of Large-Scale Web Vulnerability Notification. *25th USENIX Security Symposium (USENIX Security 16)*, 1015–1032. https://doi.org/10.1111/j.1151-2916.1918.tb17817.x

Story, P., Smullen, D., Yao, Y., Acquisti, A., Cranor, L. F., Sadeh, N., & Schaub, F. (2021). Awareness, Adoption, and Misconceptions of Web Privacy Tools. *Proceedings on Privacy Enhancing Technologies*, *2021*(3), 308–333. https://doi.org/10.2478/popets-2021-0049

Stöver, A., Gerber, N., Cornel, C., Henz, M., Marky, K., Zimmermann, V., & Vogt, J. (2022). *Website operators are not the enemy either—Analyzing options for creating cookie consent notices without dark patterns*. https://doi.org/10.18420/MUC2022-MCI-WS01-458

Stöver, A., Gerber, N., Kaushik, S., Mühlhäuser, M., & Marky, K. (2021). Investigating Simple Privacy Indicators for Supporting Users when Installing New Mobile Apps. *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–7. https://doi.org/10.1145/3411763.3451791

Stöver, A., Gerber, N., Pridöhl, H., Maass, M., Bretthauer, S., Spiecker gen. Döhmann, I., Hollick, M., & Herrmann, D. (2023). How Website Owners Face Privacy Issues: Thematic Analysis of Responses from a Covert Notification Study Reveals Diverse Circumstances and Challenge. *Proceedings on Privacy Enhancing Technologies*, *3*(2).

Stöver, A., Kretschmer, F., Cornel, C., & Marky, K. (2020). *Work in Progress: How I met my Privacy Assistant – A User-Centric Workshop*. https://doi.org/10.18420/MUC2020-WS119-005

Süddeutsche Zeitung. (o. J.). *Datenschützer starten Beschwerdewelle gegen Cookie-Banner*. Abgerufen 28. März 2022, von https://www.sueddeutsche.de/service/internet-datenschuetzer-starten-beschwerdewelle-gegen-cookie-banner-dpa.urn-newsml-dpa-com-20090101-210531-99-801337

Tahaei, M., Frik, A., & Vaniea, K. (2021a). *Deciding on Personalized Ads: Nudging Developers About User Privacy* (S. 573–596) [Data set]. https://doi.org/10.7488/DS/3045

Tahaei, M., Frik, A., & Vaniea, K. (2021b). Privacy champions in software teams: Understanding their motivations, strategies, and challenges. *Proceedings of the 2021 CHI Conference on Human Factors in*

Computing Systems, 1–15.

Tahaei, M., Li, T., & Vaniea, K. (2022). Understanding Privacy-Related Advice on Stack Overflow. *Proceedings on Privacy Enhancing Technologies*, *2022*(2), 114–131. https://doi.org/10.2478/popets-2022-0038

Tahaei, M., Ramokapane, K. M., Li, T., Hong, J. I., & Rashid, A. (2022). Charting App Developers' Journey Through Privacy Regulation Features in Ad Networks. *Proceedings on Privacy Enhancing Technologies*, *2022*(3), 33–56. https://doi.org/10.56553/popets-2022-0061

Toth, M., Bielova, N., & Roca, V. (2022). On dark patterns and manipulation of website publishers by CMPs. *Proceedings on Privacy Enhancing Technologies*, *2022*(3), 478–497. https://doi.org/10.56553/popets-2022-0082

Utz, C., Amft, S., Degeling, M., Holz, T., Fahl, S., & Schaub, F. (2022). *Privacy Rarely Considered: Exploring Considerations in the Adoption of Third-Party Services by Websites* (arXiv:2203.11387). arXiv. http://arxiv.org/abs/2203.11387

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 973–990. https://doi.org/10.1145/3319535.3354212

Vasek, M., & Moore, T. (2012). Do Malware Reports Expedite Cleanup? An Experimental Study. *Proceedings of the 5th Workshop on Cyber Security Experimentation and Test*, 1–8. https://doi.org/10.1016/j.egypro.2011.02.120

VERBI Software, Berlin, Germany. (2020). *MAXQDA 2020 [computer software]* (4.2). maxqda.com

Walther, B. (2021, Februar). *Eine (kurze) Einführung in G*Power*. https://bjoernwalther.com/eine-kurze-einfuehrung-in-gpower/

Web.de. (o. J.). Abgerufen 13. Januar 2023, von https://web.de

Weinshel, B., Wei, M., Mondal, M., Choi, E., Shan, S., Dolin, C., Mazurek, M. L., & Ur, B. (2019). Oh, the Places You've Been! User Reactions to Longitudinal Transparency About Third-Party Web Tracking and Inferencing. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 149–166. https://doi.org/10.1145/3319535.3363200

Westin, A. F. (1968). *Privacy And Freedom* (Bd. 166). Washington and Lee Law Review.

Zeng, E., Li, F., Stark, E., & Felt, A. P. (2019). Fixing HTTPS Misconfigurations at Scale: An Experiment with Security Notifications. *WEIS 2019*.

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, *131*, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
CMP	Consent Management Platform
DSGVO	Datenschutz-Grundverordnung
EDSB	Europäischen Datenschutzbeauftragen
EU	Europäische Union
IP	Internet Protocol
IT	Informationstechnik
LG	Landesgericht
lit.	Litera
o. S.	ohne Seite
P	Person
R	Rückmeldung
S&P	Security and Privacy
TCP	Transmission Control Protocol
TTSDG	Telekommunikation-Telemedien-Datenschutz-Gesetz
VPN	Virtual Private Network
WWW	World Wide Web
z. B.	zum Beispiel
Q	Question

Anhang

Anhang A
Studie 1 – Studienmaterial

Einleitung: Liebe Teilnehmerin, lieber Teilnehmer, vielen Dank, dass Sie an dieser 5-minütigen Befragung teilnehmen. Damit unterstützten Sie ein gemeinsames Forschungsprojekt der TU Darmstadt, Universität Bamberg und Goethe Universität Frankfurt zum Thema Datenschutz. Weitere Informationen zum Datenschutz dieser Befragung finden Sie hier: Erläuterungen zur Studie und zum Datenschutz [Link zu Einverständniserklärung] [Ich habe die Erläuterungen zur Studie gelesen und bin damit einverstanden, an der genannten Studie teilzunehmen. Ich erkläre mich einverstanden, dass die im Rahmen der Studie erhobenen Daten zu wissenschaftlichen Zwecken ausgewertet und in anonymisierter Form gespeichert und veröffentlicht werden können. Ich bin mir darüber bewusst, dass meine Teilnahme freiwillig erfolgt und ich den Versuch jederzeit und ohne die Angabe von Gründen abbrechen kann. | Ich bin nicht einverstanden]

Q1: Anfang Juli haben wir Ihnen diese Benachrichtigung geschickt. Haben Sie diese Benachrichtigung gelesen? [Anzeige der Benachrichtigung entsprechend der Versuchsgruppe]
[Ja |Nein | Ich weiß es nicht]

Q2: Was war Ihr erster Eindruck von unserer Benachrichtigung?

- Die Benachrichtigung macht einen vertrauenswürdigen Eindruck. [Trifft nicht zu | Trifft eher nicht zu | Trifft eher zu | Trifft zu | Keine Angabe]
- Anhand der Benachrichtigung konnte ich das Problem der fehlenden IP-Anonymisierung nachvollziehen. [Trifft nicht zu | Trifft eher nicht zu | Trifft eher zu | Trifft zu | Keine Angabe]

Q3: Bitte beschreiben Sie kurz, welche Aspekte der Benachrichtigung dazu geführt haben, dass Sie ihr vertraut haben. [offene Antwort]

Q4: Bitte beschreiben Sie kurz, welche Aspekte der Benachrichtigung dazu geführt haben, dass Sie ihr NICHT/WENIGER vertraut haben. [offene Antwort]

Q5: Haben Sie das Problem der fehlenden IP-Anonymisierung von Google Analytics auf Ihrer Webseite vor dem 27.09.2019 behoben? [ja | Nein | weiß ich nicht | Seite wurde komplett abgeschaltet]

Q6: Optional: Da das Problem der fehlenden IP-Anonymisierung bereits auf Ihrer Webseite behoben wurde: welche der folgenden Aussagen trifft am ehesten auf Sie zu? [Ich habe das Problem ohne Hilfe selbst behoben. | Ich habe das Problem mit Hilfe selbst behoben. | Ich habe das Problem/die Angelegenheit an Kollegen meiner Organisation weitergeleitet. | Ich habe meinen externen Dienstleister aufgefordert das Problem zu beheben. | Ich habe einen neuen Dienstleister damit beauftragt das Problem zu beheben. | Sonstiges: [offene Antwort]]

Q7: Können Sie sich vorstellen, was Gründe dafür sein könnten, weshalb Sie die IP-Anonymisierung von Google Analytics auf Ihrer Webseite bis zum 27.09.2019 nicht aktiviert war? [Problem war nicht bekannt | Fehlendes Wissen, wie Problem gelöst werden kann | Fehlende Zeit |Problem hat keine Priorität | Benachrichtigung schien mir nicht seriös | Sonstiges: [offene Antwort]]

Q8: Wussten Sie VOR unserer Benachrichtigung, dass Sie Google Analytics auf Ihrer Webseite verwenden? [Ja | Nein]

Q9: Hatten Sie VOR unserer Benachrichtigung schon von der Funktion zur IP-Anonymisierung gehört? [Ja und ich kannte den Zweck |Ja, ich wusste aber nicht genau, was das ist |Nein]

Q10: Wussten Sie VOR unserer Benachrichtigung von der fehlenden IP-Anonymisierung von Google Analytics auf Ihrer Webseite? [Wenn ja: Was waren Ihrer Meinung nach Gründe für die fehlende IP-Anonymisierung? [offene Antwort] |Nein]

Q11: Während unserer Studie (Juli bis September 2019) wurde in verschiedenen Medien über ein Urteil des LG Dresden berichtet, das besagt, dass die Aktivierung der IP-Anonymisierung bei Google Analytics für einen rechtskonformen Betrieb erforderlich ist. Welche der Aussagen trifft auf Sie zu? (Mehrfachantwort möglich) [Das Urteil war ausschlaggebend dafür, die IP-Anonymisierung zu aktivieren. | Die IP-Anonymisierung wurde UNABHÄNGIG vom Urteil aktiviert. | Ich habe bisher noch nichts von dem Urteil gehört. | Sonstiges: [offene Antwort]]

Q12: In unserer Benachrichtigung haben wir Sie auf das „Check Google Analytics“-Tool der Universität Bamberg hingewiesen. Wie hilfreich fanden Sie das „Check Google Analytics“- Tool der Universität Bamberg? [Gar nicht hilfreich - Sehr hilfreich (5-Punkt-Likert-Skala)] [Ich habe das Tool nicht | Verwendet Ich kenne das Tool nicht]

Q13: Welche der folgenden Check-Tools sind Ihnen bekannt bzw. haben Sie bereits verwendet? [Qualys SSL Check [Bekannt | Bekannt + Verwendet | Unbekannt] Webkoll [Bekannt | Bekannt + Verwendet | Unbekannt] Mozilla Observatory [Bekannt | Bekannt + Verwendet | Unbekannt] HTBridge [Bekannt | Bekannt + Verwendet | Unbekannt] Immuniweb [Bekannt | Bekannt + Verwendet | Unbekannt] Sonstige [offene Antwort] [Bekannt | Bekannt + Verwendet | Unbekannt]]

Q14: Würden Sie auch in Zukunft gerne Benachrichtigungen über Datenschutzprobleme auf Ihrer Webseite erhalten? [ja | nein]

Q15: Auf welche Art und Weise würden Sie gerne auf Datenschutzprobleme hingewiesen werden? [Email | Brief | Anruf | Blogposts | Sonstiges: [offene Antwort]]

Q16: Wären Sie bereit für solche Benachrichtigungen zu zahlen? [Ja | Nein]

Q17: Wie viele Mitarbeitende hat Ihre Firma oder Organisation? [offene Antwort]

Q18: Wer ist in Ihrer Organisation für die Betreuung der Webseite zuständig? [Mitarbeitende in der Organisation (bitte geben Sie an, wie viele Mitarbeitende dafür zuständig sind)? [offene Antwort]] | Webseitenbetreuung durch eine externe Agentur]

Q19: Möchten Sie uns noch etwas mitteilen? Zum Beispiel etwas, das wir bei zukünftigen Benachrichtigungen berücksichtigen sollten. [offene Antwort]

Anhang B
Studie 2a – Studienmaterial

Einleitung: Wir interessieren uns für Ihre Meinung zu einem neuen Onlineshop „WARM OUTDOOR WEAR“. Der Shop vertreibt [hochwertige Outdoor-Bekleidung zu fairen Preisen]. Vielen Dank für Ihre Unterstützung!

- Bitte lesen Sie sich folgenden Instruktionen sorgfältig durch:
- Im Folgenden finden Sie einen Link zu einer Demo-Version des Onlineshops.
- Bitte nehmen Sie sich etwas Zeit und schauen Sie sich die Website in Ruhe an.
- Schauen Sie sich auch die Produkte an und entscheiden Sie sich bitte für das Produkt, welches Sie am ehesten kaufen würden. Merken/Notieren Sie sich bitte Ihre Entscheidung.
- Im Anschluss kehren Sie bitte über den „ZURÜCK ZUR BEFRAGUNG“ zu dieser Befragung zurück, wenn Sie sich in Ruhe umgesehen haben (spätestens nach 5 Minuten werden Sie automatisch zurückgeleitet). Wir werden Sie dann um Ihr Feedback zu dem Onlineshop bitten.

[Link zum Onlineshop]

Q1-Q8: User Experience Percentile Rank Questionnaire (Sauro, 2015)– deutsche Übersetzung

Q9-Q15: Human Computer Trust Scale (Gulati et al., 2019)– deutsche Übersetzung

Q16-Q27: Privacy Scale (Xu, 2011) – deutsche Übersetzung

Q28: Als Sie den Onlineshop „WARM OUTDOOR WEAR“ besucht haben, wurde Ihnen möglicherweise ein Cookie Consent Banner anzeigt. Bitte klicken Sie die zutreffende Aussage an

- Mir wurde kein Cookie Banner angezeigt
- Ich erinnere mich nicht, ob mir ein Cookie Banner angezeigt wurde.
- Mir wurde ein Cookie Banner anzeigt: Falls zutreffend →
    - Cookie Banner 1 [Abbildung 11]
    - Cookie Banner 2 [Abbildung 12]
    - Cookie Banner 3 [Abbildung 13]
    - Cookie Banner 4 [Abbildung 14]
    - Ich erinnere mich nicht, wie der Cookie Banner aussah

Q29: Es gibt verschiedene Möglichkeiten Cookie Banner zu gestalten. Bitte bewerten Sie die folgenden Möglichkeiten mithilfe von Schulnoten (1 = finde ich sehr gut; 6 = finde ich überhaupt nicht gut).

- Cookie Banner 1 [Abbildung 11]
- Cookie Banner 2 [Abbildung 12]
- Cookie Banner 3 [Abbildung 13]
- Cookie Banner 4 [Abbildung 14]

Q30: Bitte wählen Sie den Cookie Banner aus, der Ihnen am besten gefällt:

- Cookie Banner 1 [Abbildung 11]
- Cookie Banner 2 [Abbildung 12]
- Cookie Banner 3 [Abbildung 13]
- Cookie Banner 4 [Abbildung 14]

Q31: Wieso haben Sie sich für diesen Cookie Banner entschieden? [offene Antwort]

Q32: Bitte wählen Sie den Cookie Banner aus, der Ihnen am wenigsten gefällt:

- Cookie Banner 1 [Abbildung 11]
- Cookie Banner 2 [Abbildung 12]
- Cookie Banner 3 [Abbildung 13]
- Cookie Banner 4 [Abbildung 14]
- Kein Cookie Banner (Website setzt Cookies ein, ohne Nutzer zu informieren/Wahl zu geben)

Q33: Wieso haben Sie sich für diesen Cookie Banner entschieden? [offene Antwort]

Q34: Websitebetreibende sind verantwortlich Cookie Banner für Ihre Website auszuwählen. Was denken Sie, welcher Cookie Banner würde einem Websitebetreibenden am besten gefallen?

- Cookie Banner 1 [Abbildung 11]
- Cookie Banner 2 [Abbildung 12]
- Cookie Banner 3 [Abbildung 13]
- Cookie Banner 4 [Abbildung 14]
- Kein Cookie Banner (Website setzt Cookies ein, ohne Nutzer zu informieren/Wahl zu geben)

Q35: Wieso haben Sie sich für diesen Cookie Banner entschieden? [offene Antwort]

Aufklärung: Vielen Dank für Ihre Teilnahme an der Studie. Das eigentliche Ziel der Studie war zu untersuchen, welchen Einfluss verschiedene Cookie Banner auf die Bewertung eines Onlineshops haben. Falls Sie Fragen zur Studie haben oder an den Ergebnissen interessiert sind, melden Sie sich gerne per Mail bei Alina Stöver (stoever@psychologie.tu-darmstadt.de). Falls Sie weitere Anmerkungen oder Feedback zur Studie haben, können Sie es gerne hier eintragen: [offenes Antwortfeld]

Anhang C
Studie 2b – Studienmaterial

Q1: Es gibt verschiedene Möglichkeiten Cookie Disclaimer zu gestalten. Bitte bewerten Sie die folgenden Möglichkeiten mithilfe der Skala von "Gefällt mir gar nicht" bis "Gefällt mir sehr gut"

- Cookie Banner 1 [Abbildung 11]
- Cookie Banner 2 [Abbildung 12]
- Cookie Banner 3 [Abbildung 13]
- Cookie Banner 4 [Abbildung 14]

Q2: Es gibt verschiedene Möglichkeiten Cookie Disclaimer zu gestalten. Was denken Sie, welcher Disclaimer Besucher:innen Ihrer Webseite am besten gefällt?

- Cookie Banner 1 [Abbildung 11]
- Cookie Banner 2 [Abbildung 12]
- Cookie Banner 3 [Abbildung 13]
- Cookie Banner 4 [Abbildung 14]

Q3: Wieso haben Sie sich für diesen Cookie Banner entschieden? [offene Antwort]

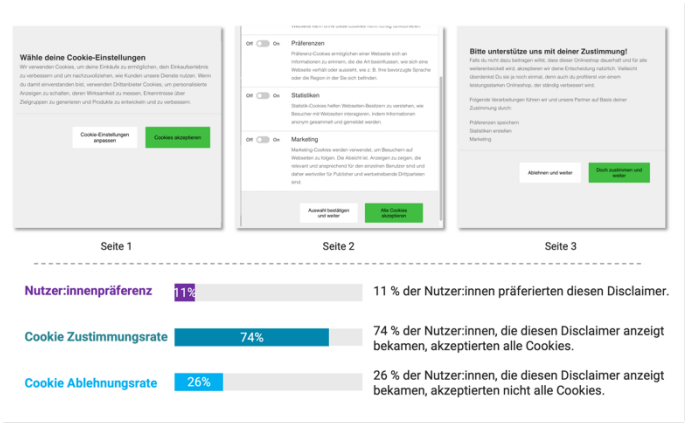
→ Zufällige Zuordnung zu Gruppe 1 oder 2

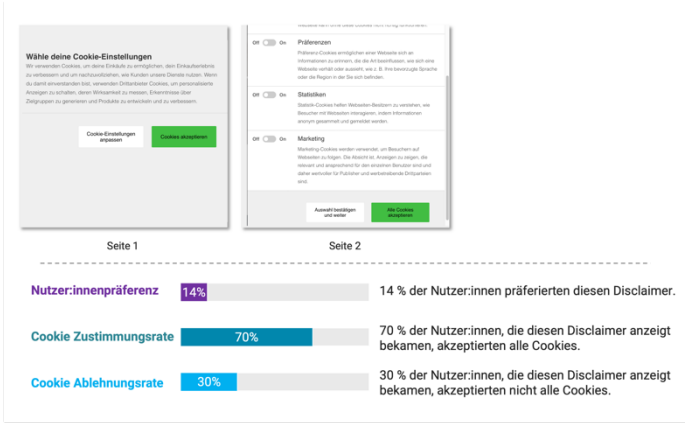
Q4.Gruppe 1 (ohne Info): Bitte wählen Sie den Cookie Disclaimer aus, der Ihnen als Webseitenbetreiber:in am besten gefällt (unabhängig davon, welcher Disclaimer möglicherweise den Besucher:innen Ihrer Website gefallen würde):

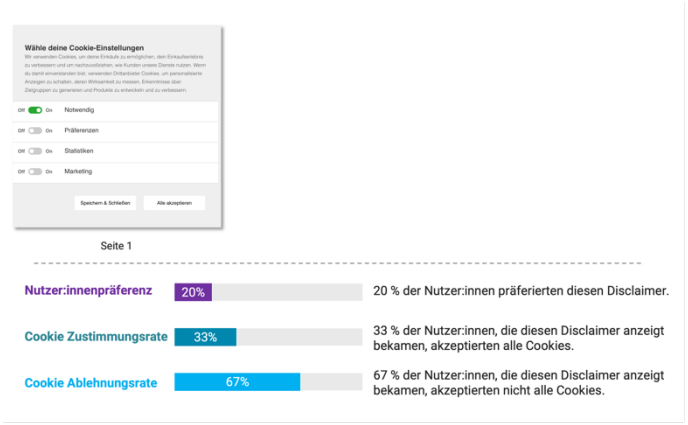
- Cookie Banner 1 [Abbildung 11]
- Cookie Banner 2 [Abbildung 12]
- Cookie Banner 3 [Abbildung 13]
- Cookie Banner 4 [Abbildung 14]

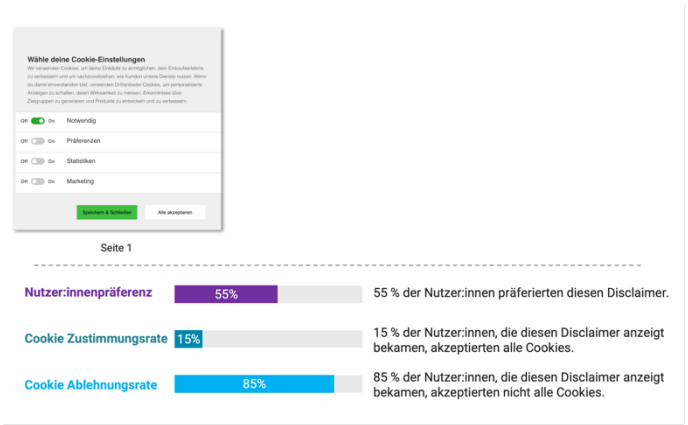
Q5.Gruppe 1: Wieso haben Sie sich für diesen Cookie Banner entschieden? [offene Antwort]

Q4. Gruppe 2 (mit Info): Bitte wählen Sie den Cookie Disclaimer aus, der Ihnen als Webseitenbetreiber:in am besten gefällt.









Q5. Gruppe 2: Wieso haben Sie sich für diesen Cookie Banner entschieden? [offene Antwort]

Demografie: Im Folgenden bitten wir Sie noch um einige Informationen zu Ihrer Person und zu Ihrer Website. Wenn Sie mehrere Webseiten betreiben, beziehen Sie sich bitte auf die Website mit den meisten monatlichen Seitenzugriffen.

Q6: Wie alt sind Sie?

- 18-24 Jahre
- 25-34 Jahre
- 35-49 Jahre
- 50-64 Jahre
- über 64 Jahre

Q7: Welchem Geschlecht ordnen Sie sich zu?

- Weiblich
- Männlich
- divers
- andere:
- Keine Angabe

Q8: Welche Art Webseite betreiben Sie? (z.B. Blog, Webshop, Unternehmensseite)

- [Offenes Antwortfeld]
- aktuell betreibe ich keine Webseite (habe dies jedoch in der Vergangenheit und/oder plane es zukünftig)
- aktuell betreibe ich keine Webseite (und habe dies auch in der Vergangenheit nicht und/oder plane es zukünftig nicht)

Q9: Welche Art Webseite betreiben Sie? (z.B. Blog, Webshop, Unternehmensseite). Bitte geben Sie weitere Informationen zu Ihrer Webseite an. [offene Antwort]

Q10: Zu welchem Zweck betreiben Sie Ihre Webseite? (z.B. persönliches Interesse, Unternehmensdarstellung) Bitte geben Sie weitere Informationen zu Ihrer Webseite an. [offene Antwort]

Q11: Welcher rechtliche Rahmen ist für Ihre Webseite relevant?

- Datenschutzgrundverordnung (DSGVO)
- Sonstiger:
- Weiß nicht

Q12: Wie viele Seitenzugriffe hat Ihre Website durchschnittlich im Monat?

- 0-99
- 100-999

- 1.000-9.999
- 10.000-99.999
- 100.00-999.999
- 1.000.000+
- Weiß nicht

Q13: Zu welchem Zweck setzen Sie Cookies auf Ihrer Webseite ein? [Mehrfachantwort möglich]

- Es werden keine Cookies eingesetzt
- Notwendig [Ja | Nein | Weiß nicht]
- Präferenzen [Ja | Nein | Weiß nicht]
- Marketing [Ja | Nein | Weiß nicht]

Q14: Generieren Sie/Ihre Organisation Einnahmen über Daten, die durch Cookies auf Ihrer Webseite gesammelt werden?

- Ja
- Nein
- Weiß nicht
- Keine Angabe

Q15: Wer hat auf Ihrer Website den aktuellen Cookie Disclaimer gestaltet?

- Selbst erstellt
- Consent Management Platform/Cookie Zustimmungstool (z.B. Cookiebot):
- Vorlage des Webseitenanbieters (z.B. WordPress):
- weiß nicht
- sonstiges:
- Es gibt keinen Disclaimer auf der Webseite

Aufklärung: Vielen Dank für Ihre Teilnahme an der Studie. Das Ziel der Studie war auch zu untersuchen, ob die Präsentation von zusätzlichen Informationen die Wahl eines Cookie Disclaimers beeinflusst. Falls Sie Fragen zur Studie haben oder an den Ergebnissen interessiert sind, melden Sie sich gerne per Mail bei Alina Stöver (stoever@psychologie.tu-darmstadt.de). Falls Sie weitere Anmerkungen oder Feedback zur Studie haben, können Sie es gerne hier eintragen: [offenes Antwortfeld]. Der Vollständigkeit halber erhalten Sie hier noch Informationen zu Cookie Consent Bannern: [Studieninfos aus der Gruppe 2]

Anhang D
Studie 3 – Studienmaterial

Tabelle 6. Liste der CMPs und deren Auflistung in den verschiedenen Quellen.

CMP	Quelle 1	Quelle 2	Quelle 3	Quelle 4	Quelle 5	Quelle 6	Status
2badvice	X						
AdOpt				X			X
Axeptio				X			X
CCM 19		X					X
Commanders Act						X	
consent manager	X	X				X	X
Main web solution		X					
Smart life		X					X
Cookie Script	X					X	X
Cookie Yes		X		X		X	X
Cookiebot by usercentrics	X	X	X	X	X	X	X
cookiefirst	X						
CookieHub	X			X			X
CookiePro				X			X
Crownpeak			X	X	X	X	
data privacy manager	X						
DataGrail				X			
Datenschutzgenerator		X					
Datev				X			
Didomi	X			X		X	
Ethyca				X			
Evidon/Crownpeak						X	
google funding Choices			X				
Iubenda	X	X	X	X		X	X
Ketch				X			
Liveramp	X		X			X	
Monsido				X			
Ogury						X	
onetrust			X	X	X	X	
Osano	X		X	X		X	
PiWik Pro		X		X		X	X
privacy policies		X					
privacy tools				X			
PrivacyUX for CCPA				X			
Quantcast	X		X	X	X	X	X
real cookie banner		X					X
salesforce identity				X			
secure Privacy				X			
securiti	X			X			
segment				X			
sourcepoint	X		X			X	
squarespace		X					
Termly.io				X			X
Transcend				X			
truendo	X						
TrustArc			X	X	X	X	
trustcommander	X						
uniconsent	X						
Usercentrics	X	X		X		X	
WS02 Identiy Server				X			

Anmerkung: Der Status bezieht sich darauf, ob es möglich war eine Cookie-Einwilligungserklärung kostenlos und ohne persönliche Kontaktaufnahme zu erstellen.

Quelle 1: Ergebnisse auf Seite 1-4 der Google-Suche im Inkognito-Modus für den Begriff "Consent Management Platform" am 10. März 2022.
Quelle 2: Ergebnisse auf Seite 1-4 unserer Google-Suche im Inkognito-Modus für den Begriff "Cookie Consent Notice" am 10. März 2022.
Quelle 3: Kevel. 2022. Consent Management Platform (CMP) 2022 Tracker. Abgerufen am 28. März 2022 von https://www.kevel.com/cmp/.
Quelle 4: Best Consent Management Platforms. Top 30 scored CMPs. Abgerufen am 28. März 2022 von

https://www.g2.com/categories/consentmanagement-platform-cmp.
Quelle 5: Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (Honolulu, HI, USA) (CHI '20).Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376321
Quelle 6: Lisa Gradow and Ramona Greiner. 2021. Quick Guide Consent-Management. Springer Gabler, Wiesbaden, Germany.

Studie 3 – Weitere Ergebnisse

Tabelle 7. Ergebnisse der analysierten Vorlagen von 15 CMPs.

CMP	Balanced möglich	Bright möglich	Obstruction enthalten	Interface Interference enthalten	Mind. 1 Deceptive Design
AdOpt	nein	nein	ja	nein	ja
Axeptio	ja	ja	nein	ja	ja
CCM 19	ja	ja	nein	ja	ja
Consent manager	ja	ja	nein	nein	nein
Smart life	uneindeutig	ja	uneindeutig	ja	ja
Cookie Script	nein	ja	nein	ja	ja
Cookie Yes	ja	ja	nein	ja	ja
Cookiebot	nein	ja	nein	ja	ja
CookieHub	ja	nein	nein	nein	nein
CookiePro	ja	nein	nein	nein	nein
Iubenda	ja	ja	nein	nein	nein
PiWik Pro	ja	ja	nein	nein	nein
Quantcast	ja	ja	nein	ja	ja
Real cookie banner (devowl)	uneindeutig	ja	nein	ja	ja
Termly.io	ja	nein	nein	nein	nein

Anmerkung: Die Tabelle orientiert sich an der Tabelle aus Stöver et al. (2022).