Gottfried Wilhelm
Leibniz Universität Hannover
Fakultät für Elektrotechnik und Informatik
Institut für Praktische Informatik
Fachgebiet Software Engineering

Konzeptionierung und prototypische Umsetzung von kontextuellen Privatsphäreerklärungen

Masterarbeit

im Studiengang Informatik

von

Felix Volodarskis

Prüfer: Prof. Dr. rer. nat. Kurt Schneider
Zweitprüferin: Dr. rer. nat. Jil Klünder
Betreuer: M. Sc. Wasja Brunotte, M. Sc. Jakob Richard Christian Droste

Hannover, 19.04.2023

Erklärung der Selbstständigkeit

Hiermit versichere ich, dass ich die vorliegende Masterarbeit selbständig und ohne fremde Hilfe verfasst und keine anderen als die in der Arbeit angegebenen Quellen und Hilfsmittel verwendet habe. Die Arbeit hat in gleicher oder ähnlicher Form noch keinem anderen Prüfungsamt vorgelegen.

Hannover, den 19.04.2023

Felix Volodarskis

Danksagung

An dieser Stelle möchte ich mich bei all denjenigen bedanken, die mich während der Ausarbeitung dieser Masterarbeit unterstützt und motiviert haben.

Zuerst möchte ich mich bei meinen Betreuern Wasja Brunotte und Jakob Richard Christian Droste bedanken, die mich kontinuierlich unterstützt haben und mir mithilfe von konstruktiver Kritik den Weg gewiesen haben.

Ebenfalls möchte ich mich bei Alexander Specht und Maike Ahrens für die ausführliche Pilotierung der Nutzerstudie bedanken.

Ein besonderer Dank gilt allen Teilnehmern, die an der Nutzerstudie teilgenommen haben, da ohne diese keine Ergebnisse vorgelegen hätten.

Abschließend möchte ich mich bei Kerim Balci, Marcel Konrad und Rafael Volodarskis für das Korrekturlesen bedanken.

Zusammenfassung

Heutzutage wird die Nutzung von Software als selbstverständlich angesehen. Durch die Nutzung dieser kann es zu Situationen kommen, in denen ein einseitiger Datenaustausch zugunsten von Unternehmen stattfindet. Zwar wurde durch die Europäische Union die sogenannte Datenschutz-Grundverordnung (DSGVO) verabschiedet, durch die die europäischen Bürger das „Recht auf Erklärung“ haben, jedoch wird dieses in der Praxis häufig durch Cookie-Banner oder Datenschutzbestimmungen umgesetzt. Beide Formen der Erklärungen können kritisiert werden. Die Cookie-Banner enthalten sogenannte „Dark Patterns“ und die Datenschutzbestimmungen sind nachweislich für die Benutzer schwer verständlich. Beide bereits umgesetzten Formen der Erklärung haben gemeinsam, dass Benutzer anhand dieser nur schwer verstehen können, was mit ihren eigenen Daten passiert. Die jeweiligen Hauptkritikpunkte können durch wissenschaftliche Ausarbeitungen belegt werden. Daraus folgt, dass ein informiertes Einverständnis seitens der Benutzer unwahrscheinlich ist.

Eine mögliche Lösung für das Problem sind die kontextuellen Privatsphäreerklärungen, die Kernpunkte bezüglich der Privatsphäre dem Benutzer in verständlicher Sprache übermitteln. Hierzu wird die Erklärbarkeit als nichtfunktionale Anforderung in dieser Arbeit näher betrachtet. Außerdem werden die kontextuellen Privatsphäreerklärungen im Anwendungskontext eines sozialen Mediums prototypisch umgesetzt und mit einem Fokus auf die Nutzbarkeit, der Verständlichkeit und der Angemessenheit einzelner Erklärungen analysiert. Dazu wurde eine Nutzerstudie mit insgesamt 62 Teilnehmern durchgeführt. Anhand der Ergebnisse ist sichtbar, dass die hier umgesetzten Privatsphäreerklärungen einen negativen Einfluss auf die Nutzbarkeit haben. Dennoch haben die Teilnehmer einen Nutzen in diesen gesehen. Weiterhin konnten die Teilnehmer inhaltliche Fragen bezüglich der Privatsphäreerklärungen beantworten und haben häufig eingeschätzt, dass sie diese verstanden haben. Außerdem haben die Teilnehmer Privatsphäreerklärungen, in denen es um ihre direkten Daten geht wie z.B. GPS-Daten häufig als relevant eingestuft.

Abstract

Nowadays, the use of software is taken for granted. Through the use of these, situations can arise in which a one-sided exchange of data takes place for the benefit of companies. Although the European Union has passed the so-called General Data Protection Regulation (GDPR), giving European citizens the „right to explanation“, but in practice this is frequently implemented through cookie banners or privacy notices. Both forms of explanations can be criticized. The cookie banners contain so-called „dark patterns“ and the privacy policies are demonstrably difficult for users to understand. Both types of explanations that are already implemented have in common that users find it difficult to understand what is happening with their own data. The main points of criticism in each case can be substantiated by scientific work. It follows that informed consent on the part of users is unlikely.

One possible solution to the problem are contextual privacy explanations, which convey key points regarding privacy to the user in understandable language. For this purpose, explainability is considered as a non-functional requirement in this thesis. Furthermore, the contextual privacy explanations are prototyped in the context of a social media platform and are implemented with a focus on usability, comprehensibility, and appropriateness of individual explanations. In order to analyze the privacy explanations, a user study was conducted with a total of 62 participants. Based on the results, it is visible that the privacy explanations implemented here have a negative influence on usability. Nevertheless, the participants saw a benefit in these. Furthermore, the participants were able to answer questions regarding the content of the privacy explanations and often assessed that they understood them. In addition, participants frequently rated privacy explanations involving their direct data, such as GPS data, as relevant.

Inhaltsverzeichnis

Kapitel 1

Einleitung

1.1 Motivation

In der heutigen Zeit, ist die Verwendung von Software sowohl im persönlichen als auch im beruflichen Umfeld kaum vermeidbar. Bei der Benutzung von Software jeder Art, wird seitens der Benutzer jedoch häufig der Fakt außen vor gelassen, dass indirekt Daten mit dem System geteilt werden können [10] [11]. Unter anderem können persönliche Interessen eines Benutzers anhand des Nutzerverhaltens ausgewertet und analysiert werden, um den Benutzer gezielt Werbung anzuzeigen. Dies stellt eine einseitige Beziehung zur Sammlung von privaten Daten dar, in der dem Benutzer häufig nicht klar ist, dass dieser gerade persönliche und sensible Daten freigibt. Eine Änderung dieser einseitigen Beziehung ist nicht in Sicht, da das Handeln mit Daten ein gewinnbringendes Geschäft ist [19]. Solch eine Praxis stellt jedoch einen Eingriff in die persönliche Privatsphäre dar und kann auf den Benutzer intransparent wirken.

Laut dem europäischen Datenschutzgesetz (DSGVO) [23], haben die Benutzer das Recht, über deren eigene Privatsphäre informiert zu werden, was häufig durch Nutzerbedingungen passiert, die sprachlich juristisch orientiert und schwierig erfassbar sind [44] [10]. Im digitalen Alltag kommt solch eine Konfrontation mit den Nutzungsbedingungen vor, aber durch die sprachliche Barriere, ist es für den Nutzer schwierig ein überlegtes Einverständnis zu geben. Außerdem konnte bereits gezeigt werden, dass ein großer Anteil an Benutzern diese Nutzungsbedingungen nicht lesen oder inhaltlich verstehen [35]. Damit dieser einseitige Datenaustausch zumindest informiert stattfinden kann, muss die sprachliche Barriere gemindert werden. Hierzu ist es wichtig, dass mit den Nutzern auf einem möglichst verständlichen sprachlichen Niveau kommuniziert wird.

1.2 Lösungsansatz

Zur Bewältigung dieses Problems hat im Rahmen dieser Arbeit eine Literaturrecherche und Einarbeitung in das Thema Erklärbarkeit stattgefunden. Dabei wurde der Einfluss auf die Nutzbarkeit beachtet und bereits existierende Lösungen wurden analysiert. Mithilfe der gefundenen Informationen wird ein Prototyp mit einem gewählten Anwendungskontext entwickelt. Dabei handelt es sich um einen Anwendungskontext, bei dem Missvertrauen seitens des Nutzers bezüglich der eigenen Privatsphäre bestehen kann.

In diesem Prototypen sind kontextuelle Privatsphäreerklärungen integriert, die sich strukturell an den Arbeiten von Brunotte [12] und Droste [21] orientieren. Inhaltlich sind sie an die Nutzungsbedingungen angepasst, die dem gewählten Anwendungskontext entsprechen. Allerdings sind die Privatsphäreerklärungen im Gegensatz zu den Nutzungsbedingungen in einfacher Sprache formuliert. Diese Privatsphäreerklärungen werden in verschiedenen Kontexten dem Benutzer angezeigt, so dass dieser die Erklärungen erhält, die im jetzigen Kontext relevant sind. Dies bedeutet, dass der Benutzer z.B. eine Erklärung darüber erhält welcher Hardwarezugriff benötigt wird sobald dieser dabei ist ein Bild hochzuladen.

Dieser Prototyp wurde in Rahmen einer Nutzerstudie mit 62 Teilnehmern getestet. Dadurch konnten Erkenntnisse bezüglich der Nutzbarkeit, des Verständnisses und der Ermessenheit der Privatsphäreerklärungen gewonnen werden.

1.3 Struktur der Arbeit

Diese Arbeit ist wie folgt strukturiert. In Kapitel 2 werden die Grundlagen, die zur Erarbeitung dieser Arbeit benötigt werden erläutert. Dabei wird die Erklärbarkeit und das Konzept der Privatsphäreerklärung näher betrachtet.

Darauf aufbauend wird in Kapitel 3 ein Konzept für die kontextuellen Privatsphäreerklärungen erarbeitet. In diesem Kapitel werden das Forschungsziel und die Forschungsfragen festgelegt. Außerdem wird die Struktur der Privatsphäreerklärungen mithilfe von bereits erarbeiteten Strukturen erstellt.

Das erarbeitete Konzept wird in Kapitel 4 in einem gewählten Anwendungskontext implementiert. Dabei wird der Prozess der Implementation vom Papier-Prototypen bis zur Web-Anwendung beschrieben. Weiterhin werden Kontexte für die Privatsphäreerklärungen im Anwendungskontext festgelegt.

Der fertige Prototyp wird mithilfe einer Nutzerstudie analysiert. Die Ergebnisse der Nutzerstudie werden in Kapitel 5 aufgelistet und evaluiert.

Daraufhin folgt die Intepretation der erhobenen Daten und die Limitierung der Ergebnisse in Kapitel 6.

Danach werden verwandte Arbeiten in Kapitel 7 präsentiert und mit dieser Arbeit verglichen.

Abschließend wird die Arbeit in Kapitel 8 zusammengefasst und es wird ein Ausblick auf zukünftige Möglichkeiten gegeben.

Kapitel 2

Grundlagen

2.1 Erklärbarkeit

In ihrer Studie haben Obar und Oeldorf-Hirsch [35] herausgefunden, dass 74% der 543 Teilnehmenden die Datenschutzrichtlinien und die Nutzungsbedingungen bei der Registrierung eines fiktiven sozialen Mediums übersprungen haben. Weiterhin sehen die Teilnehmer diese als eine Art „Belästigung“ an. Außerdem haben 98% der Teilnehmer übersehen, dass ihre Daten mit der NSA(National Security Agency) geteilt werden und dass der Preis zur Nutzung der fiktiven Plattform das erstgeborene Kind ist [35].

Dies zeigt, dass Benutzer sich häufig keine Gedanken darüber machen, was mit ihren hinterlassenen Daten passieren kann. Es wurde sogar häufig die Klausel übersehen, dass die Plattform etwas kostet.

Laut Chazette und Schneider [17] können Erklärungen in Software den Nutzern beim Treffen einer Entscheidung helfen. Außerdem kann die nichtfunktionale Anforderung der Erklärbarkeit dabei helfen das Bewusstsein bezüglich der persönlichen Privatsphäre zu stärken [10]. Weiterhin kann die Erklärbarkeit dabei helfen, dass Nutzer Vertrauen zum System aufbauen [26].

Daraus folgt, dass die Beachtung der Erklärbarkeit in solch einem System das Potential hat eine Lösung für das oben genannte Problem zu sein.

Chazette definiert in ihrer Dissertation Erklärbarkeit folgendermaßen [15]:

> „Erklärbarkeit ist die Fähigkeit oder der Akt, Informationen offenzulegen, die für einen Adressaten notwendig sind, um einen bestimmten Aspekt eines Systems in einem bestimmten Kontext zu verstehen, was durch die Bereitstellung von Erklärungen erreicht werden kann.“

Diese Definition beschriebt jedoch nicht die Erklärbarkeit als nichtfunktionale Anforderung, sondern stellt diese Definition lediglich eine „naive

Unterscheidung“ dar. Daher muss die Definition von erklärbaren Systemen herangezogen und betrachtet werden [15].

Ein erklärbares System wird von Chazette et al. [16] im Kontext von Requirement Engineering folgendermaßen definiert:

> „Ein System **S** ist in Bezug auf den Aspekt **X** von S relativ zu den Adressaten **A** im Kontext **C** erklärbar, wenn und nur wenn es eine Entität **E** (den Erklärer) gibt, die durch die Bereitstellung eines Informationskörpers **I** (die Erklärung von X) A ermöglicht, X von S im Kontext C zu verstehen.“

Zusammengefasst bedeutet es, dass ein System einen Erklärer enthält, der dem Benutzer das System anhand von eingebetteten Informationen erklärt. Außerdem ist erkennbar, dass die Definition eines erklärbaren Systems, die Definition der Erklärbarkeit erfüllt.

2.1.1 Auswirkung von Erklärbarkeit auf die Usability

Chazette und Schneider [17] haben den Einfluss auf die Usability durch die Erklärbarkeit untersucht. Hierbei haben $10,82\%$ der Teilnehmer angegeben, dass die Nutzung eines Systems durch Erklärungen erleichtert werden kann. Weiterhin haben $6,93\%$ der Teilnehmer das Gefühl, dass Erklärungen wie eine Art Tutorial funktionieren. Außerdem haben $5,19\%$ das Gefühl, dass die Erklärungen denen dabei geholfen haben schnellere Entscheidungen treffen zu können. Des Weiteren haben $2,16\%$ der Teilnehmer angegeben, dass Erklärungen Fehler beim Treffen einer Entscheidung vermeiden können. $0,87\%$ der Teilnehmer haben erwähnt, dass Erklärungen auch als Rückmeldung, dass das System korrekt funktioniert, dienen können [17]. Dies bedeutet, dass erklärbare Systeme einen positiven Effekt auf die Usability haben können.

Dennoch konnten auch negative Einflüsse gefunden werden. $15,82\%$ haben angegeben, dass die Nutzeroberfläche durch die Erklärungen überladen wirkt und dies von der eigentlichen Arbeitsfolge ablenken kann. $3,39\%$ haben angegeben, dass sie Sorgen bezüglich der Hardwarebelastung haben. $9,04\%$ meinten, dass die Erklärungen einen hohen zeitlichen Anspruch mit sich bringen [17].

Insgesamt betrachtet haben die Teilnehmer Vorteile für sich finden können. Die negativen Aspekte beziehen sich eher darauf, dass der Nutzer an der Stelle vom eigentlichen Ziel abgelenkt wird und selber aktiv werden muss. Dies erklärt auch die Tatsache, dass $19,77\%$ der Teilnehmer angegeben haben, dass sie die Erklärungen als Störfaktor wahrgenommen haben [17].

2.1.2 Transparenz als nichtfunktionale Anforderung

Leite und Capelli [27] haben die Transparenz in Software als nichtfunktionale Anforderung definiert. Hierbei haben sie folgende Definition erarbeitet [27]:

> Sofern die Informationen innerhalb eines Systems für die Benutzer **zugänglich**, **benutzerfreundlich**, **aussagekräftig**, **verständlich** und **überprüfbar** sind, gilt jenes System als transparent.

Diese Definition deckt sich mit der Definition aus Abschnitt 2.1 hinsichtlich der Verständlichkeit und der Zugänglichkeit.

Nach Chazette und Schneider [17] kann die in Abschnitt 2.1 beschriebene Erklärbarkeit bei der Erreichung der Transparenz helfen, da sie einen positiven Effekt auf die Transparenz haben kann, sofern die beinhalteten Informationen dem Nutzer verständlich vermittelt werden. Jedoch muss das von Chazette und Schneider [17] gefundene „double-Edged sword effect“ der Erklärbarkeit beachtet werden, weil Erklärungen an die Zielgruppe angepasst sein müssen. Bei zu viel Transparenz, wird seitens der Benutzer mehr Zeit zum Verständnis benötigt, was nicht gut für die Usability ist und dem Benutzer eher schaden könnte, weil dieser dadurch eventuell nichts versteht [17].

Dies bedeutet, dass die Inhalte vom Erklärer eines Systems möglichst an eine Zielgruppe gerichtet sein sollten und somit auch von dieser Zielgruppe verstanden werden sollten.

2.1.3 Understandability als nichtfunktionale Anforderung

Nach Leite und Capelli [27] ist die nichtfunktionale Anforderung Understandbility folgendermaßen definiert:

> Understandability bezieht sich auf die Verständlichkeit der Sprache oder des Gedankenganges.

Diese Definition deckt sich mit der Definition aus Abschnitt 2.1 bezüglich der Verständlichkeit. Außerdem heißt es in Abschnitt 2.1, dass die Erklärbarkeit bei der Treffung einer Entscheidung helfen kann, was mit dem Verständnis eines Gedankenganges vergleichbar ist.

Weiterhin heißt es laut Chazette und Schneider [17], dass Erklärungen „eine bessere Interpretierbarkeit“ bieten, was das Verständnis erleichtern kann.

2.2 Vertrauen und Vertrauenswürdigkeit

Laut Kästner et al. [26] kann die Erklärbarkeit zwar dabei helfen, dass die Nutzer dem System vertrauen, jedoch muss die Intention unterschieden werden.

Wenn ein System nicht vertrauenswürdig ist und der Entwickler somit schlicht auf das Vertrauen seitens der Nutzer hofft, so liegt hier ein Fall von „Vertrauen ohne Vertrauenwürdigkeit oder nicht garantiertes Vertrauen“ vor [26].

Dementsprechend muss strikt zwischen der Definition von einem vertrauenswürdigen System und Vertrauen seitens des Nutzers unterschieden werden:

> „Ein System **S** ist für den Nutzer **H** vertrauenswürdig in einem Kontext **C**, wenn und nur wenn
>
> (a) S in C ordnungsgemäß funktioniert und
>
> (b) H dazu berechtigt wäre (a) zu glauben. [26]“

> Wenn das System vom Nutzer **H** als vertrauenswürdig angesehen wird, so kann davon ausgegangen werden, dass das System von H als vertraulich angesehen wird [34].

Das bedeutet, dass die Vertrauenswürdigkeit eine Eigenschaft eines Systems sein kann, während das Vertrauen nur seitens des Nutzers bezüglich des Systems entstehen kann. Ein System muss sich das Vertrauen seitens des Nutzers also verdienen und das Vertrauen muss gerechtfertigt sein.

2.3 Privatsphäreerklärungen

Als Lösung des in Abschnitt 2.1 geschilderten Problems können die von Brunotte et al. [12] [16] definierten „Privatsphäreerklärungen“, die in einem Kontext mit Privatsphäre als Aspekt eingesetzt werden können, hilfreich sein.

2.3.1 Definition von Privatsphäreerklärungen

Brunotte et al. [12] verwenden die folgende Definition des Konzepts der Privatsphäreerklärungenzept:

„Eine Privatsphäreerklärung ist ein Informationskörper **I**, das ein System **S** dem Adressaten **A** im Kontext **C** zur Verfügung stellt, um den Zweck **P** für die Benutzung des Datenschutzaspekts **X** zu erklären."

In Anbetracht der in Abschnitt 2.1 enthaltenen Definition für die Erklärbarkeit, nimmt eine Privatsphäreerklärung mitsamt des Informationskörpers der Privatsphäreerklärung die Rolle der Entität bzw. die des Erklärers an.

Brunotte [12] konnte zeigen, dass Benutzer sich Gedanken um ihre Privatsphäre machen und die Vor- und Nachteile eines Dienstes abwägen, wenn es um die eigene Privatsphäre geht. Dies zeigt, dass seitens der Benutzer ein Interesse an Privatsphäreerklärungen besteht, da die Intention mehr über die eigene Privatsphäre zu erfahren vorliegt. Dieses Interesse bestätigt sich mit einer weiteren Beobachtung, denn $91,6\%$ der Teilnehmer sind an Privatsphäreerklärungen interessiert und stufen diese als nützlich ein, da die Teilnehmer durch diese Informationen über Datenpraktiken erhalten können, sofern diese sprachlich für den Benutzer verständlich sind und eine Verbindung zum aktuellen Kontext besteht [12]. Das heißt, dass z.B. in dem Szenario, in dem eine Person ein Bild erstellen und hochladen möchte, der Benutzer darüber aufgeklärt wird, welcher Zugriff benötigt wird und wieso dieser benötigt wird.

Diese Voraussetzungen stellen sicher, dass die enthaltenen Informationen innerhalb der Privatsphäreerklärungen für den Benutzer zugänglich sind. Weiterhin konnte gezeigt werden, dass das Bewusstsein bezüglich der eigenen Privatsphäre durch Privatsphäreerklärungen gefördert wird. Darüber hinaus können Privatsphäreerklärungen einen positiven Einfluss auf die Transparenz und die Vertrauenswürdigkeit eines Systems haben. Zudem wird dem Benutzer zu einer bewussteren Entscheidungsfindung durch die Privatsphäreerklärungen beholfen. Durch diese aufgezählten Eigenschaften ist es möglich, dass ein Benutzer dem System vertraut [12].

Insgesamt sind Privatsphäreerklärungen ein Konstrukt, das mit den Benutzern in verständlicher Sprache kommuniziert und dadurch Informationen bezüglich der Privatsphäre des Benutzers vermittelt.

Um einer Verwirrung vorzubeugen sei gesagt, dass das Wort „Erklärung" in der deutschen Sprache zwei Bedeutungen hat. Zum einen kann eine Erklärung eine Darlegung von Zusammenhängen sein und zum anderen kann eine Erklärung eine „offizielle Äußerung sein" [1]. In diesem Fall wird die erste Bedeutung der Erklärung verwendet, da es sich bei einer Privatsphäreerklärung um einen Informationskörper handelt, der den Benutzer Zusammenhänge erklären soll.

[1] `https://www.duden.de/rechtschreibung/Erklaerung`, zuletzt besucht am 18.04.2023

2.4 Privacy Paradox

Laut Olmstead und Smith sind 64% der befragten US-Bürger persönlich von einer Datenschutzverletzung betroffen und haben diese erlebt [36]. Nach Rainie möchten 61% der befragten US-Bürger mehr tun, um ihre Privatsphäre zu schützen [38]. Diese Daten zeigen, dass Personen sich Sorgen um ihre Privatsphäre machen und sich der Tatsache bewusst sind, dass ihre persönlichen Daten verarbeitet werden. Dennoch würden Nutzer laut Carrascal ihre Browserdaten für etwa 7 Euro verkaufen [14]. Diese Zweiteilung zwischen Bewusstsein über Privatsphäre und dem eigentlichen Verhalten wird „privacy paradox“ genannt [25].

Laut Barnes gibt es keine einfache Lösung für dieses Problem, jedoch könnte Aufklärung bezüglich der eigenen Privatsphäre einen positiven Einfluss auf das Bewusstsein über die Privatsphäre haben. Dabei ist das Bewusstsein bezüglich der eigenen Privatsphäre der Schlüssel zur Lösung [7].

Durch die Beobachtungen von Pentina et al. [37] kann die Definition des Privacy Paradox erweitert werden. Nämlich gibt es eine Art Schwelle zwischen Risiko und Nutzen, die vor der Benutzung einer Anwendung seitens des Benutzers evaluiert wird. Hierbei handelt es sich um die Privacy Calculus Theory [37].

Nach Pentina et al. [37] gibt es verschiedene Faktoren, die die Entscheidung welche Daten offengelegt werden beeinflussen können. Unter anderem konnte herausgefunden werden, dass z.B. in China diese Hinterfragung bezüglich der Offenlegung von Daten bei Anwendungen stattfindet, die nicht bereits genutzt werden und gesellschaftlich von weniger Relevanz sind, während dies bei bereits installierten und gesellschaftlich wichtigen Anwendungen wie WeChat, QQ und Baidu Mobile nicht gemacht wird. Der Grund hierfür könnte sein, dass chinesische Nutzer scheinbar ihre Daten lieber nur bei einem Unternehmen haben möchten als diese dann mehreren Unternehmen zur Verfügung zu stellen. Dies bedeutet, dass Anwendungen seltener hinterfragt werden, sobald ein „Informationsnutzen und ein sozialer Nutzen“ besteht [37].

Da die Privatsphäreerlärungen zur Aufklärung über die eigene Privatsphäre dienen und somit das Bewusstsein bezüglich der eigenen Privatsphäre stärken können, könnten diese in Anbetracht der Aussage von Barnes ebenso eine Lösung für den Privacy Calculus sein.

2.5 Dark Patterns in Software

Es existieren Software-Systeme, die so konzipiert sind, dass die Benutzer ihre Daten eher teilen, obwohl sie das nicht möchten. Diese Systeme können auch psychologische Tricks beinhalten, bei denen die Nutzer z.B. zum Kauf von Gegenständen verleitet werden. Solche manipulative Designmuster werden

von Experten zu der Kategorie Dark Patterns zugeordnet [20].

Chromik et al. [18] haben Dark Patterns im Kontext von Erklärbarkeit untersucht und herausgefunden, dass diese häufig so zum Einsatz kommen, dass Nutzer absichtlich für Profit getäuscht werden.

Da es bei dieser Arbeit darum geht den einseitigen Datenaustausch zwischen Benutzer und Unternehmen zu kommunizieren, sollten Dark Patterns möglichst nicht genutzt werden. Dies ist im Kontext der Privatsphäreerklärungen jedoch schwierig zu vermeiden, da die Nutzungsbedingungen nicht vollständig zitiert sein können und die Erklärung lediglich nur eine Teilmenge dieser enthält, was wiederum den Benutzer bei der Entscheidung beeinflussen kann [18].

2.5.1 Dark Patterns in Cookie Bannern

In Cookie Bannern (Consent Management Platforms), die beim ersten Besuch einer Webseite auftreten, konnten Nouwens et al. Dark Patterns feststellen [33]. Dafür haben sie die 10000 meistbesuchten Webseiten innerhalb des Vereinigten Königreiches (UK) untersucht. Laut Nouwens et al. müssen drei Bedingungen gelten damit das europäische Gesetz (DSGVO [23]) erfüllt ist [33]:

1. Die Einwilligung muss ausdrücklich erfolgen
2. Die Einwilligung aller Bedingungen muss genau so leicht sein wie das Ablehnen
3. Es soll keine voreingestellten Haken geben

Zusammenfassend muss das Akzeptieren auf freiwilliger Basis erfolgen, das Ablehnen soll dabei eine genau so einfache Option sein und die Nutzer müssen nicht dazu gezwungen sein sich durch mehrere Haken durchzuklicken.

Das Ergebnis dieser Studie ist, dass lediglich $11,8\%$ der getesteten Cookie Banner keine Dark Patterns enthalten [33]. Bei den Privatsphäreerklärungen lassen sich Dark Patterns bezüglich des Inhaltes nicht vermeiden, jedoch ist es möglich diese hier genannten Bedingungen zu erfüllen, so dass die Benutzer möglichst eine eigene Entscheidung treffen können.

Kapitel 3

Konzeption des Prototypen

Zur Entwicklung des Prototypen und der Nutzerstudie ist ein Konzept für die kontextuellen Privatsphäreerklärungen nötig. Hierfür wird zunächst ein Forschungsziel definiert. Daraufhin werden die Forschungfragen, die durch die Nutzerstudie beantwortet werden sollen erhoben und festgelegt. Anschließend werden die Anforderungen an die Privatsphäreerklärungen erhoben und begründet. Darauf aufbauend wird der benötigte Inhalt von Privatsphäreerklärungen bestimmt und erklärt.

3.1 Forschungsziel

Das Forschungsziel wurde mithilfe der Vorlage von Wohlin et al. [45] angefertigt.

> Es wird das entwickelte Konzept der kontextuellen Privatsphäreerklärungen analysiert, um die Wahrnehmung und Akzeptanz dieser zu bewerten mit Bezug auf Nutzbarkeit, Verständlichkeit und Erlernbarkeit aus der Sicht von Endbenutzern im Kontext einer Nutzerstudie, die online durchgeführt wird. Zusätzlich wird die Thinking-Aloud-Methode verwendet [29]. Bei der gesamten Durchführung ist der Experimentator anwesend.

3.2 Forschungsfragen

RQ1: Einfluss auf die Usability

Grundsätzlich hat die nichtfunktionale Anforderung der Erklärbarkeit einen Einfluss auf die sogenannte Usability [16]. Weiterhin stellen kontextuelle Privatsphäreerklärungen beim Durchführen einer Aufgabe einen weiteren Schritt dar, der eigentlich nicht üblich ist. Daher ist die Überprüfung,

ob es einen Einfluss gibt wichtig, da das Konzept neu ist. Außerdem ist es auch wichtig zu erfahren, ob die Privatsphäreerklärungen als störend wahrgenommen werden und ob Nutzer gegebenenfalls trotzdem einen Vorteil darin sehen. Somit ist die folgende Forschungsfrage zustande gekommen:

> **RQ1:** Welchen Einfluss haben kontextuelle Privatsphäreerklärungen auf die Usability?

RQ2: Verständnis der Privatsphäreerklärungen

Da es sich bei diesem Konzept der kontextuellen Privatsphäreerklärungen um ein neues Konzept handelt, ist es wichtig herauszufinden, ob diese Umsetzung für Nutzer inhaltlich verständlich ist und wie sie ihr eigenes inhaltliches Verständnis einschätzen. Außerdem ist es auch wichtig herauszufinden, ob die Benutzung der Privatsphäreerklärungen in der umgesetzten Form auch verständlich ist. Dadurch ist die folgende Forschungsfrage zustande gekommen:

> **RQ2:** Inwiefern ist das Konzept der kontextuellen Privatssphäreerklärungen für die Benutzer nachvollziehbar?

RQ3: Angemessenheit der Privatsphäreerklärungen

Es ist noch nicht klar, in welchem Kontext die Konfrontation der Nutzer mit den kontextuellen Privatsphäreerklärungen nötig ist. Da die Privatsphäreerklärungen bei der Nutzung einen weiteren Schritt darstellen, kann es passieren, dass diese als ein Hindernis wahrgenommen werden, falls die Konfrontation vom Nutzer als unangemessen eingeordnet wird. Deshalb ist es wichtig herauszufinden, für wie relevant die Nutzer eine Privatsphäreerklärung im gewählten Anwendungskontext empfinden. Dadurch ist die folgende Forschungsfrage zustande gekommen:

> **RQ3:** Unter welchen Umständen ist die Konfrontation der Nutzer mit den kontextuellen Privatsphäreerklärungen im gewählten Anwendungskontext angemessen?

3.3 Anforderungen an die kontextuellen Privatsphäreerklärungen

Mithilfe der Literatur, die ich in meinen Recherchen gefunden habe, und der vorausgegangenen Masterarbeit von Droste [21], ist es möglich Anforderungen an die kontextuellen Privatsphäreerklärungen zu erheben und das Konzept mit eigenen Ideen zu erweitern. Die nichtfunktionale Anforderung der **Erklärbarkeit** ist hierbei relevant, da es sich bei Privatssphäreerklärungen um ein Teil eines Systems handelt, das den Nutzern die Erhebung Ihrer Daten erklärt somit stellen diese eine Instanz dar, die den Nutzer dabei helfen das System zu verstehen [16] [12] [21]. Eine Grundannahme, die hierbei die Anforderung der Erklärbarkeit stützt, ist dass ein Großteil der Nutzer sich nicht mit juristischen Texten auseinander setzen will oder kann, da ihnen die fachliche Kompetenz fehlt oder die eigene Faulheit überwiegt [25]. Dieser Problematik könnte entgegengewirkt werden, indem bei den kontextuellen Privatsphäreerklärungen mit einfacher Sprache gearbeitet wird, die weder technischer noch rechtlicher Natur ist und somit für Nutzer möglichst einfach verständlich ist. Außerdem kann die nicht funktionale Anforderung der Erklärbarkeit einen Einfluss auf das **Vertrauen** haben, was eine wünschenswerte Eigenschaft ist, da das Vertrauen den Weg zur **Software-Transparenz** ebnen kann [12] [27].

Darauf folgt auch die Anforderung der **Verständlichkeit**. Die Erklärbarkeit gibt lediglich vor, dass das System sich dem Nutzer erklärt, jedoch ist damit noch nicht definiert, dass Nutzer verstehen für welche Tätigkeit die Privatsphäreerklärungen genutzt werden und unter welchen Bedingungen sie das Hauptsystem nutzen können [1]. Letzteres ist besonders dann wichtig, wenn der Benutzer dabei ist eine Entscheidung hinsichtlich einer Privatssphäreerklärung zu treffen, weil dem Benutzer erst dort erklärt wird, unter welchen Bedingungen dieser etwas verwenden darf.

Ein fundamentales Attribut für die **Nutzbarkeit** eines Systems ist die **Erlernbarkeit** eines Systems, da es generell wünschenswert ist, dass ein System leicht erlernbar ist [32]. Laut Nielsen ist ein System erlernbar, wenn es den Benutzer innerhalb kurzer Zeit ermöglicht ein angemessenes Niveau an Benutzerkenntnissen zu erreichen. Zudem versichert es, dass Benutzer unabhängig von Ihren Kenntnissen die Privatsphäreerklärungen bedienen können [24] [32].

Bei all den Anforderungen muss auch beachtet werden dass die Privatsphäreerklärungen bei den Nutzern nicht negativ auffallen, da diese ein weiterer Schritt beim Erreichen eines Ziels sind und dabei vom eigentlichen Ziel ablenken können. Außerdem muss auch darauf geachtet werden, dass in verständlicher Sprache mit den Nutzern kommuniziert wird, da dies ansonsten die Erreichung der Erklärbarkeit und der Verständlichkeit verhindert. Inhaltlich darf auch nichts ausgelassen werden, was für den Nutzer von

Relevanz ist, da dies, wie in Abschnitt 2.2 erwähnt dazu führt, dass ein nicht garantiertes Vertrauen vorliegt.

3.4 Inhalt der kontextuellen Privatsphäreerklärungen

Es existieren inhaltliche Anforderungen an Privatsphäreerklärungen, die in den folgenden vier Kategorien aufgeteilt sind [12] 3.1:

- Datennutzung
- Datenspeicherung
- Präsentationsform
- Vertraulichkeit

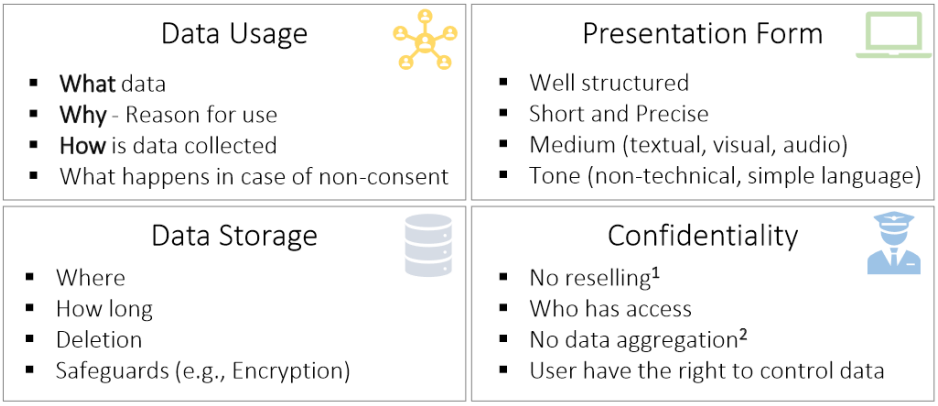

Abbildung 3.1: Inhaltliche Anforderungen an Privatsphäreerklärungen nach [12]

3.4.1 Datennutzung

Diese Kategorie beinhaltet die Nutzung der Nutzerdaten im Rahmen des Systems. Hierbei werden die Fragen „Welche Daten werden genutzt?“, „Wieso werden die Daten genutzt?“ und „Wie werden die Daten genutzt?“ beantwortet [12]. Zusätzlich beinhaltet diese Kategorie auch die Folgen des Ablehnens der Privatssphäreerklärung 3.1.

3.4.2 Datenspeicherung

Benutzer des Systems sollten wissen wo und wie lange die Daten gespeichert werden. Dafür sollten Privatsphäreerklärungen beinhalten ob die Daten lediglich temporär oder langfristig gespeichert werden. Zusätzlich müssen diese auch beinhalten welche Sicherheitsmaßnahmen ergriffen werden, um Datenschutzverletzungen zu vermeiden [12] 3.1.

3.4.3 Präsentationsform

Die Präsentationsform der Privatsphäreerklärungen muss für Benutzer einfach verständlich sein. Dafür relevant ist die Präsentationsform, die beinhaltet dass die Privatsphäreerklärungen strukturiert, kurz und präzise sind. Außerdem muss der Inhalt in einfacher Sprache präsentiert werden, was bedeutet dass technische Ausdrücke gemieden werden [12] 3.1.

3.4.4 Diskretion

Diskretion ist ein zentraler Punkt von persönlicher Privatsphäre. Dazu gehört die Offenlegung, ob Daten des Nutzers weiterverkauft werden und ob die Daten aggregiert werden. Außerdem müssen Nutzer die Kontrolle über ihre eigenen Daten behalten. Zum Beispiel sollten Nutzer innerhalb der Privatsphäreerklärungen die Möglichkeit dazu haben den Weiterverkauf ihrer Daten zu unterbinden [12] 3.1.

3.5 Struktur der kontextuellen Privatsphäreerklärungen

Die Struktur der Privatsphäreerklärungen orientiert sich an das Modell von Droste [21]. Hierbei ist der benötigte Inhalt der Privatsphäreerklärungen in fünf verschiedene Ebenen aufgeteilt. Diese Struktur wurde von Droste so definiert, da Nutzer existieren, für die einzelne Details von höherer Relevanz sind als für andere. So ist es für die Benutzer möglich tiefer in die Details zu gehen, falls diese es möchten [21].

3.5.1 Basis-Ebene

Die erste Ebene ist die Basis-Ebene, in der inhaltlich die Datenverarbeitung angesprochen wird. Folgende Punkte werden hierbei beachtet[21]:

- Welche Art von Daten verarbeitet werden
- Wie die Daten primär verarbeitet werden
- Mögliche Zweitverwendungen von Daten

- Die Konsequenzen des Ablehnens der Daten

Inhaltlich ist diese Ebene vergleichbar mit der Datennutzung, die bereits in Unterabschnitt 3.4.1 beschrieben ist. Im Vergleich dazu ist bei den hier konzipierten Privatsphäreerklärungen folgender Inhalt enthalten:

- Welcher Zugriff wird benötigt? (z.B. Hardwarezugriff auf die Kamera)
- Welche Konsequenzen hat das Ablehnen der Privatsphäreerklärung?
- Welche Daten werden genutzt?

3.5.2 Kontrastive-Ebene

Die zweite Ebene ist die kontrastive Ebene, in der den Nutzern mitgeteilt wird, was nicht mit Ihren Daten passiert [21]. In den hier konzipierten Privatsphäreerklärungen ist dies lediglich dahingehend integriert, dass dies in den Folgen des Ablehnens einer Privatssphäreerklärung enthalten ist.

3.5.3 Beispielsbasierte-Ebene

Die dritte Ebene ist die beispielsbasierte Ebene, bei der dem Nutzer anhand eines visuellen Beispiels dargestellt wird wie die Daten verarbeitet werden [21]. In Abbildung 3.2 ist eine Visualisierung aus dem finalen Prototypen dargestellt. Hierbei wird anhand des Pfeiles signalisiert, dass das gewählte GIF auf der rechts dargestellten Diskette landet. Hierbei ist die Diskette eine häufig gewählte Metapher dafür, dass etwas gespeichert wird.

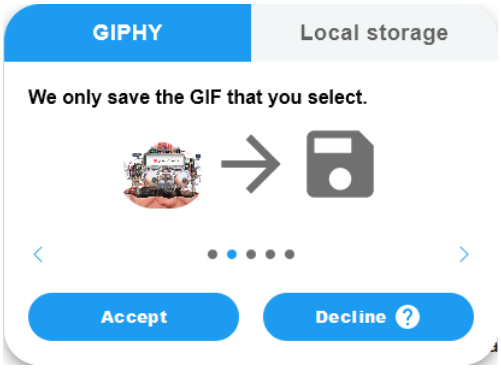

Abbildung 3.2: Beispielsbasierte Darstellung der Datenverarbeitung aus dem finalen Prototypen

3.5.4 Erklärung weiterer Details

Die in Unterabschnitt 3.5.1 angesprochene Basis-Ebene enthält zwar welche Daten erhoben werden, welche Konsequenzen das Ablehnen der Privatsphä-

reerklärung hat und welcher Zugriff benötigt wird, jedoch wird dabei nur oberflächlich auf die rechtliche Ebene eingegangen. Folgende Fragen müssen hierfür beantwortet werden [21]:

- Wo werden die Daten gespeichert?
- Wer hat Zugriff auf die Daten?
- Wie lange werden die Daten gespeichert?
- Wann werden die Daten anonymisiert?
- Welche Rechte hat der Benutzer?

Diese Ebene von Droste gleicht sich mit der Umsetzung im finalen Prototypen und ähnelt sich inhaltlich mit der in Unterabschnitt 3.4.4 beschriebenen Diskretion.

3.5.5 Drittanbieter

Laut der DSGVO haben die Benutzer das Recht zu erfahren mit welchen Drittanbieterdiensten die Daten geteilt werden. Hierzu müssen laut Droste folgende Information in der Privatsphäreerklärung enthalten sein:

- Mit welchen Drittanbietern werden die Daten geteilt?
- Verlinkung zu den einzelnen Drittanbieterdiensten.
- Wie werden die Daten durch Drittanbieter genutzt?

Diese Ebene ergänzt inhaltlich mit der in Unterabschnitt 3.5.4 angesprochenen Ebene. Zusammen ergeben sie die in Unterabschnitt 3.4.4 angesprochene Diskretion. Diese Ebene ist inhaltlich in den umgesetzten Privatssphäreerklärungen vorzufinden, jedoch führt die Verlinkung zum Drittanbieterdienst zu den Nutzungsbedingungen des entsprechenden Drittanbieters.

3.5.6 Was nicht garantiert wird

Diese Ebene stellt eine Ergänzung zu den bereits bestehenden Anforderungen dar. Es existieren Fälle, in denen Dienste keine Kontrolle darüber haben können, was mit den Daten, die öffentlich einsehbar sind, passiert. Unter anderem kann es auf einem sozialen Medium passieren, dass andere Nutzer eine lokale Kopie eines hochgeladenen Bildes erstellen. In diesem Fall kann das soziale Medium den Nutzer nur davor warnen, dass das Szenario im Rahmen des Möglichen ist. Ein Beispiel für solch eine Warnung ist in Abbildung 3.3 vorzufinden.

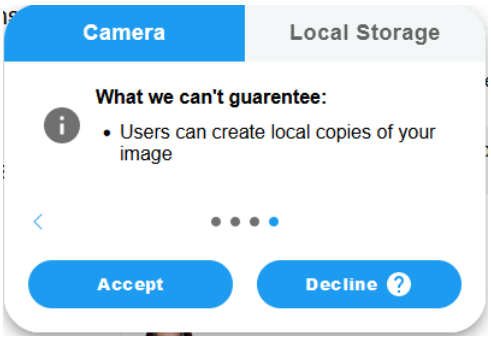

Abbildung 3.3: Beispielsbasierte Darstellung einer Warnung aus dem finalen Prototypen

Kapitel 4

Implementation des Prototypen

Zur Durchführung der Studie und Evaluation des Konzepts, ist ein funktionierender Prototyp nötig, der die Anforderungen an das Konzept erfüllt. Dafür wird zu Beginn des Kapitels die Wahl des Anwendungskontextes begründet. Daraufhin wird die Entwicklung des Papierprototypen beschrieben. Weiterhin wird die Implementation des finalen Prototypen mithilfe des Web Frameworks React [1] erklärt und mit dem ursprünglichen Papierprototypen verglichen.

4.1 Wahl des Anwendungskontextes

Vor der Entwicklung des Prototypen, musste ein Anwendungskontext festgelegt werden. Hierbei ist es wichtig, dass der Anwendungskontext für potentielle Studienteilnehmer bekannt ist und dass dieser den Teilnehmern ermöglicht, einen Bezug zur eigenen Privatsphäre herzustellen. Weiterhin ist es von Vorteil, wenn der Anwendungskontext möglichst leicht verständlich ist.

Dementsprechend eignet sich ein Nachbau des sozialen Mediums Twitter [2] als Anwendungskontext. Soziale Medien können mit der eigenen Privatsphäre in Verbindung gebracht werden, da auf diesen Plattformen auch sensible Daten geteilt werden. Außerdem ist die Nutzung eines sozialen Mediums fester Bestandteil des Alltags, wodurch die Studienteilnehmer seltener in Situationen geraten, die für sie unrealistisch wirken. Zusätzlich zählen soziale Medien zu den Quellen für Datenmakler [11].

[1] `https://reactjs.org/`, zuletzt besucht am 02.03.2023
[2] `https://twitter.com/home`, zuletzt besucht am 02.03.2023

4.2 Entwicklung des Papierprototypen

Bevor der finale Prototyp entwickelt werden kann, ist es wichtig eine Basis zu schaffen, auf dessen Grundlage der finale Prototyp aufbaut. Zudem ist es bei einem Papierprototypen einfacher schnell auf Änderungen zu reagieren, da hierfür keine aufwendige Entwicklung nötig ist. Dadurch ist es auch möglich mehrere Interaktionsmöglichkeiten auszuprobieren und darauf basierend Entscheidungen zu treffen [41]. Deshalb wurde zunächst ein Papierprototyp entwickelt. Für den Papierprototypen wurde die Software draw.io genutzt, da viele geometrische Formen nötig waren. Weiterhin ist es mit der Software möglich schnelle Änderungen einzuführen und auszuprobieren. Zur Nutzung des Papierprototypen wurde dieser ausgedruckt und die einzelnen Privatsphäreerklärungen wurden ausgeschnitten.

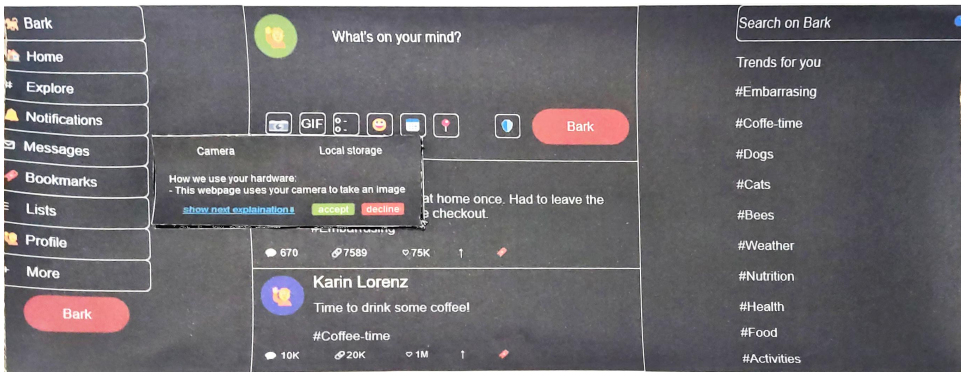

Abbildung 4.1: Finaler Papierprototyp

In Abbildung 4.1 ist der Papierprototyp abgebildet, der beim Designprozess entstanden ist und Privatsphäreerklärungen enthält. Dieser Papierprototyp ist ein Twitter-Klon namens „Bark“. Dabei handelt es sich bei der Namensgebung um eine Anlehnung an Twitter, dessen Name daher stammt, dass Vögel zwitschern bzw. auf Englisch heißt es „twitter“. Genau so ist es auch bei Hunden, dass sie bellen bzw. auf Englisch heißt es „bark“. Auf der Abbildung ist die Privatsphäreerklärung für die Kamerafunktionalität sichtbar, die angezeigt werden soll sobald auf das darüberliegende Kamerasymbol geklickt wird. Zudem wurden Posts mit zufällig generierten Namen und eine Trendleiste hinzugefügt, damit für die Nutzer des Prototypen eine Immersion entsteht. Weiterhin ist links neben dem Button mit der Aufschrift „Bark“ ein Button mit einem Schild-Symbol sichtbar, der zur Zurücksetzung der Privatsphäreerklärung zum Posten dienen soll. Da der Button zur Zurücksetzung der genannten Privatsphäreerklärung keine zentrale Funktion zur Bearbeitung des Posts enthält, ist ein räumlicher Abstand zwischen den

anderen Buttons entstanden, sodass diese Tatsache dem Nutzer mitgeteilt wird.

4.3 Verwendung des React Frameworks

Zur Umsetzung des funktionalen Prototypen wurde das Framework React verwendet. Eine besondere Eigenschaft des Frameworks ist die auf Komponenten basierende Entwicklung, die die Entwicklung einzelner Komponenten nacheinander ermöglicht. Zudem ist es auch möglich, den Zustand einzelner Komponenten zu verwalten [1]. Beide Eigenschaften ermöglichen ein einfaches Verwalten der kontextuellen Privatsphäreerklärungen im finalen Prototypen. Zudem ermöglicht React das Verwenden von bereits bestehenden Komponenten in Form von Bibliotheken. Eine Bibliothek, die im finalen Prototypen Verwendung findet, ist MUI (Material-UI)[3], das bereits vorgefertigte Komponenten im Stil der Material-UI von Google enthält [4]. Dies ermöglicht eine einfache Einbindung von Designelementen, die sowohl funktional als auch von der Ästhetik zu dem Prototypen passen. Zudem wurde die Bibliothek React-Router verwendet, um eine Weiterleitung auf einen Post zum Kommentieren zu ermöglichen [5].

4.4 Verwendung eines Templates

Als Grundlage für den Prototypen dient ein bereits existierender Twitter Klon [6]. Dieser Twitter-Klon enthält bereits einen optisch ähnlichen Designnachbau der Twitter-Oberfläche. Mit einer Anbindung an eine Datenbank, ist es mit diesem Klon auch bereits möglich selber Posts zu erstellen. Dies ist im Rahmen der Nutzerstudie nicht nötig, weshalb im finalen Prototypen die Posts nicht persistent sind und in einer Liste verwaltet werden.

4.5 Umsetzung des finalen Prototypen

Bei der Entwicklung des finalen Prototypen dient der in Abbildung 4.1 gezeigte Papierprototyp als Grundlage. Zur Umsetzung wurde erstmal die Möglichkeit zum Posten verändert. Hierzu wurde die im Template ursprünglich vorgesehene Anbindung zur Datenbank entfernt und mit einer lokalen Liste ersetzt. Daraufhin wurden die einzelnen Privatsphäreerklärungen mithilfe des Popover Komponenten, das aus der Material-UI Bibliothek stammt, an die dazugehörigen Buttons angebunden. Durch die Nutzung des

[3] `https://mui.com/`, zuletzt besucht am 02.03.2023

[4] `https://m3.material.io/styles`, zuletzt besucht am 02.03.2023

[5] `https://reactrouter.com/en/main`, zuletzt besucht am 02.03.2023

[6] `https://github.com/CleverProgrammers/twitter-clone`, zuletzt besucht am 02.03.2023

lokalen Speichers des Browsers, ist es möglich den Zustand einzelner Privatsphäreerklärungen zu speichern. Somit wird gemerkt auf welcher Seite der Privatsphäreerklärung der Nutzer sich befindet und ob diese akzeptiert oder abgelehnt wurde. Weiterhin ermöglicht der lokale Speicher des Browsers auch das Zurücksetzen der Privatsphäreerklärungen, sofern der Nutzer sich dazu entscheiden sollte eine Funktionalität nicht mehr verwenden zu möchten. Der Button zur Zurücksetzung der entsprechenden Privatsphäreerklärung ist dabei im Popover Element immer unter der eigentlichen Funktionalität. Beispielsweise ist dieser bei der Kameraanwendung unter dem Button zur Aufnahme eines Bildes.
Die Buttons zur Zurücksetzung der Privatsphäreerklärungen für Posts, Interaktionen und Lesezeichen, stellen hierbei Ausnahmefälle dar, da diese Funktionalitäten nicht in einem Popover stattfinden.
Im Fall der Privatsphäreerklärung zum Posten ist dieser wie in Abschnitt 4.2 beschrieben in der Box, die zum Posten dient, jedoch ist der Button hier in einer anderen Farbe hinterlegt und räumlich näher an den Buttons, die zur Modifikation des Posts dienen.
Bei den Privatsphäreerklärungen für Interaktionen und Lesezeichen, sind die jeweiligen Buttons in einem drei Punkte Menü hinterlegt.

4.6 Vergleich zwischen dem Papierprototypen und dem finalen Prototypen

In Abbildung 4.2 ist der fertige Prototyp abgebildet. Im Vergleich zum Papierprototypen, der in Abbildung 4.1 abgebildet ist, wurden die Icons mit den dazugehörig passenden Icons aus der MUI-Bibliothek ersetzt. Weiterhin ist die Oberfläche an einem hellen Design orientiert, da dies bei vielen Anwendungen der Standard ist. In der Postbox ist der Button zum Posten vorerst ausgegraut bis der Nutzer die Bedingungen zum Posten akzeptiert hat. Zusätzlich ist die Interaktion mit einem Post einer anderen Person auch nicht möglich bis die Privatsphäreerklärung zur Interaktion akzeptiert wurde. Die Buttons zum Akzeptieren und Ablehnen haben die gleiche Farbe, damit dies auf die Entscheidung des Nutzers keinen Einfluss hat und beide Positionen neutral betrachtet werden können.
Innerhalb der Privatsphäreerklärung zur Kamera wurde eine weitere Funktionalität mithilfe eines Tab-Panels eingefügt, die es Nutzern erlaubt Bilder aus dem lokalen Speicher hochzuladen. Eine weitere Änderung ist die Art und Weise wie durch die einzelnen Seiten der Privatsphäreerklärung navigiert wird. Statt dem Label, der zur nächsten Seite führt, gibt es eine Navigation mit Punkten, die an der Navigation an iOS orientiert ist [7]. Dabei ist durch die Punkte sichtbar auf welcher Seite der Nutzer sich befindet und wie viele

[7] `https://developer.apple.com/design/human-interface-guidelines/components/presentation/page-controls/`, zuletzt besucht am 22.03.2023

Seiten es gibt. Im Vergleich zu der Navigation in iOS ist es jedoch nicht selbsterklärend, wenn eine Wischgeste mit einer Maus durchgeführt wird. Deshalb wurden Pfeile zur Navigation eingefügt, die das Umblättern zur nächsten Seite symbolisieren. Weiterhin gibt es nun einen Hinweis darauf, dass Funktionalitäten eingeschränkt sind sofern die Privatsphäreerklärung vom Nutzer abgelehnt wird. Wenn der Cursor darüber gehalten wird, erscheint zudem ein Hinweistext, der dem Nutzer erklärt, was das Ablehnen der Funktionalität bedeutet. Im Falle der Privatsphäreerklärung zur Kamera wird dem Nutzer mitgeteilt, dass das Nutzen der Kamera nicht möglich ist und die Kamera auch nicht von Bark aktiviert wird, jedoch kann der Nutzer noch die Option des lokalen Speichers in Erwägung ziehen, um ein Bild hochzuladen.

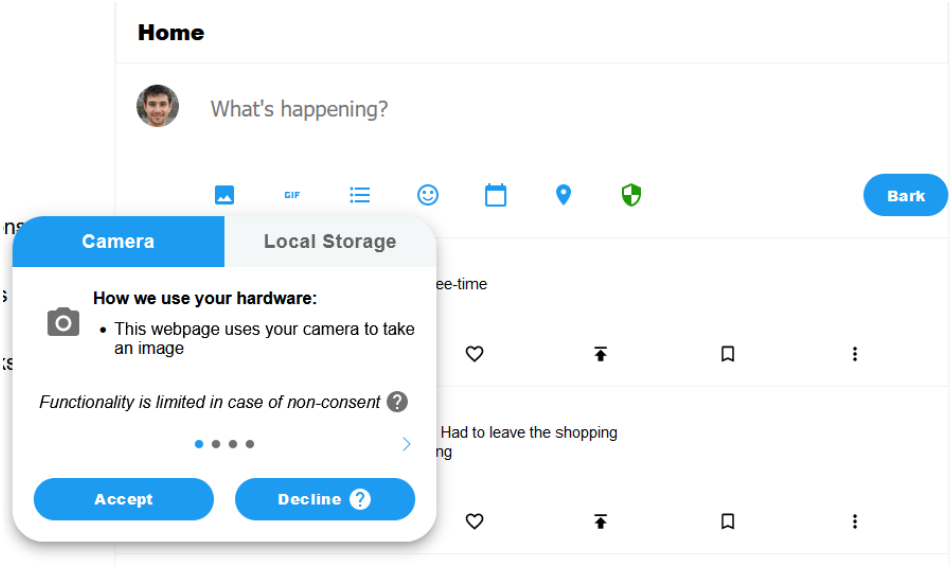

Abbildung 4.2: Finaler Prototyp

4.7 Wahl der Kontexte für die Privatsphäreerklärungen

Zur Durchführung der Nutzerstudie, werden mehrere Kontexte im Anwendungskontext benötigt, damit die Probanden sich mit mehreren Beispielen der Umsetzung beschäftigen können und sich damit auch eine fundiertere Meinung über die kontextuellen Privatsphäreerklärungen machen können. Hierbei ist es von Relevanz auch Kontexte auszuwählen, die für den gewählten Anwendungskontext üblich sind, damit die Probanden im besten Fall sich auch in das Szenario, dass sie gerade ein soziales Medium nutzen, hineinversetzen können.

4.7.1 Posten eines Bildes

Das Posten eines Bildes ist Bestandteil vieler sozialer Medien. Hierbei kann es sich auch um ein Bild handeln, das den Nutzer selbst abbildet. Weiterhin besteht bei der Nutzung dieser Funktionalität auch ein Zugriff auf die Hardware des Nutzers, sei es in Form der Kamera oder in Form des lokalen Datenträgers. Daher handelt es sich um einen Zugriff auf die Privatsphäre des Nutzers, weshalb es hier auch wichtig ist den Nutzer zu berichten, dass dieser Zugriff besteht. Außerdem ist es für den Nutzer auch hilfreich zu wissen, dass andere Nutzer eine lokale Kopie des hochgeladenen Bildes erstellen können, wo das Bild gespeichert wird, wie lange das Bild gespeichert wird und welche Rechte der Nutzer hat.

4.7.2 Posten eines GIFs

GIFs können im Rahmen eines sozialen Mediums als Reaktion auf einen Post in Form eines Kommentares verwendet werden. Üblicherweise handelt es sich hierbei nicht um ein persönliches Bild des Nutzers, jedoch werden dafür häufig Drittanbieterdienste wie z.B. GIPHY[8] oder Tenor[9] verwendet. Der im Prototypen verwendete Dienst GIPHY gibt in den eigenen Datenschutz-Bestimmungen[10] selber an, dass sie auch persönliche Daten durch andere Dienste sammeln. Dabei handelt es sich um die IP-Adresse des Nutzers, die Sprachpräferenz, der Zeitpunkt und weitere identifiziernde Daten, mit denen die Anfrage rückverfolgt werden kann. Deshalb ist es von Relevanz, dass der Nutzer darauf aufmerksam gemacht wird, dass Daten an den Drittanbieterdienst weitergeleitet werden.

4.7.3 Angabe eines Standortes

Optional kann ein Nutzer beim erstellen eines Posts, einen Standort angeben. Hierbei kann ein Zugriff auf die eigene Hardware in Form der GPS-Antenne oder ein Zugriff auf die IP-Adresse des Nutzers bestehen, sofern dieser den Standort nicht manuell angibt. Dazu kommt, dass soziale Medien in der Regel Drittanbieterdienste zur Bereitstellung von Standorten nutzen. Im Beispiel von Twitter ist es der Dienst Foursquare[11]. Die Standortdaten werden von Twitter zum Beispiel auch dazu verwendet, um dem Nutzer „relevante Inhalte“ zu präsentieren[12] Dies stellt einen Eingriff auf die Privatsphäre dar und darüber muss der Nutzer informiert werden.

[8] `https://giphy.com/`, zuletzt besucht am 05.03.2023

[9] `https://tenor.com/de/`, zuletzt besucht am 05.03.2023

[10] `https://support.giphy.com/hc/en-us/articles/360032872931-GIPHY-Privacy-Policy`, zuletzt besucht am 05.03.2023

[11] `https://location.foursquare.com/company/partners/`, zuletzt besucht am 05.03.2023

[12] `https://twitter.com/settings/location_information`, zuletzt besucht am 05.03.2023

4.7.4 Interaktion mit Inhalten

Bei der Interaktion mit Inhalten auf einem sozialen Medium, können seitens der Plattform Nutzerdaten erhoben werden. Twitter gibt an, dass sie hierbei folgende Informationen sammeln und auswerten[13]:

- Das „Retweeten“ eines Posts
- Das Markieren eines Posts mit „Gefällt mir“
- Das Teilen eines Posts
- Das Beantworten eines Posts
- Das Erwähnen anderer Benutzer oder die Erwähnung durch andere Nutzer
- Die eigenen Listen und Lesezeichen
- Die Interaktion mit externen Links

All diese Informationen können dafür verwendet werden, die persönlichen Präferenzen eines Benutzers herauszufinden. Deshalb sollte der Nutzer beim Benutzen dieser Funktionalitäten darauf aufmerksam gemacht werden, dass diese Daten verarbeitet werden.

4.7.5 Suchen von Inhalten

Zum Erkunden von Inhalten, gibt es auf sozialen Medien auch eine Suchfunktion. Twitter selbst warnt den Nutzer jedoch nicht, dass die Suchanfragen gespeichert werden 13. Außerdem bieten sich die Suchanfragen dafür an private Interessen des Nutzers zu identifizieren. Zudem können Suchanfragen und deren Ergebnisse zur Präzisierung der Suche genutzt werden. Deshalb werden diese Informationen den Nutzern in der finalen Umsetzung des Prototypen zur Verfügung gestellt.

4.7.6 Erstellung eines Posts

Das Posten und Teilen von Inhalten ist eine zentrale Funktionalität von sozialen Medien. Hierbei werden laut Twitter Informationen über das eigene Profil geteilt. Zusätzlich kann es beim Posten dazu kommen, dass Informationen mit Drittanbietern geteilt werden, sofern diese Option aktiviert ist 13. Dass Profilinformationen durch das Erstellen eines Posts, für die allgemeine Öffentlichkeit sichtbar ist, ist durch den Kontext zwar erschließbar, aber ein aktiver Hinweis auf diese Tatsache, könnte für Nutzer dennoch hilfreich sein. Zudem sollte die Option zur Teilung der Daten mit Drittanbietern für

[13] `https://twitter.com/en/privacy`, zuletzt besucht am 05.03.2023

Nutzer sichtbarer sein, weshalb diese Option in der finalen Umsetzung des Prototypen in der Privatsphäreerklärung, die bei der Erstellung eines Posts sichtbar ist, vorzufinden ist.

Kapitel 5

Evaluierung der Nutzerstudie

Zur Evaluation des in Kapitel 3 entwickelten Konzepts und des in Kapitel 4 implementierten Prototypen, wurde eine Nutzerstudie durchgeführt, um die in Abschnitt 3.2 definierten Forschungsfragen zu beantworten. Nachfolgend gebe ich Informationen über den Aufbau und Durchführung der Studie. Anschließend werden die Daten bezüglich der Gesamtdauer und dem Verständnis quantitativ und die Daten bezüglich der wahrgenommenen Relevanz qualitativ ausgewertet und die daraus resultierenden Ergebnisse präsentiert. Eine Einordnung und Interpretation der Ergebnisse können dem Kapitel 6 entnommen werden.

5.1 Methodik und technische Umsetzung

Die Nutzerstudie wurde in From eines „synchronous remote usability test“ (snychroner Distanz-Usability-Test) durchgeführt. Bei dieser Art von Usability-Test handelt es sich um eine Form, bei der der Teilnehmer und Experimentator nicht in einem Raum sitzen. Stattdessen wird diese mithilfe von Software über das Internet durchgeführt.

Bei dieser Nutzerstudie wird die Nutzbarkeit (**Usability**) des Prototypen untersucht. Hierfür bietet sich die Methode **Thinking Aloud** an [29], um eventuelle Kritikpunkte an der Umsetzung der Privatsphäreerklärungen seitens der Teilnehmer zu erhalten. Dafür wurden die Teilnehmer dazu eingeladen ihre Gedanken beim Ausfüllen des vorgefertigten Fragebogens frei auszusprechen. Sofern diese es nicht getan haben, habe ich nochmals nachgehakt, um eine mündliche Begründung für Ihre Antwort zu erhalten.

5.1.1 Aufbau der Nutzerstudie

Der Fragebogen zur Studie ist in vier Sektionen gegliedert und ist so gestaltet, dass dieser die Forschungsfragen aus Abschnitt 3.2 abdeckt.

Die erste Sektion enthält allgemeine Fragen über das Nutzerverhalten

des Nutzers. Hierbei geht es um die persönliche Einstellung bezüglich der eigenen Privatsphäre im Internet seitens der Teilnehmer und ob diese soziale Medien nutzen und falls ja wie viele. Diese Sektion dient unter anderem als Eisbrecher, da es nicht unüblich ist, dass Probanden mit einer Nervosität in eine Nutzerstudie einsteigen. Zudem hat diese Sektion auch dabei geholfen, mit den Teilnehmern die Thinking-Aloud-Methode zu üben, da nicht alle Teilnehmer mit dieser vertraut sind und es anfangs für diese befremdlich wirken kann die Gedanken frei auszusprechen.

Daraufhin wurden die Probanden mit dem Prototypen konfrontiert. Hierbei waren die Probanden in zwei Gruppen aufgeteilt. Die eine Gruppe (Gruppe A) hat die kontextuellen Privatsphäreerklärungen gesehen und durfte diese bedienen. Die andere Gruppe (Gruppe B) hat die Privatsphäreerklärungen nicht gesehen, musste jedoch die gleichen Aufgaben bewältigen wie die andere Gruppe. Gruppe A wurde nach der Erledigung der Aufgaben zusätzlich befragt, ob sie sich bei der Erledigung der Aufgaben durch etwas gestört gefühlt haben. Falls sie dies bejahten, wurden sie zusätzlich gefragt, ob es an den kontextuellen Privatsphäreerklärungen gelegen hat und ob sie dennoch einen Vorteil darin gesehen haben.

Hiernach hört die Unterscheidung der Gruppen auf und es wurde geprüft wie gut die Probanden die Privatsphäreerklärungen inhaltlich verstehen. Hierfür dienten die Privatsphäreerklärungen für die Kamera und für GIPHY als Testgegenstand. Die Probanden haben für beide Privatsphäreerklärungen jeweils eine Minute Zeit bekommen, um sich möglichst viel zu merken. Anschließend durften diese erstmal einschätzen wie gut sie die jeweilige Privatsphäreerklärung verstanden haben und zu diesen auch drei kurze inhaltliche Fragen beantworten.

In der letzten Sektion ging es um die Einstufung der Relevanz einzelner Privatsphäreerklärungen seitens der Probanden. Hierfür durften sich die Probanden Zeit lassen und sich die einzelnen Privatsphäreerklärungen nochmal detailliert anschauen. Zu jeder Einstufung wurde, falls seitens der Probanden nicht angegeben, nach einer mündlichen Begründung gefragt.

Jede Durchführung der Nutzerstudie wurde mit Einverständnis der Teilnehmer aufgezeichnet und protokolliert. Somit sind etwas mehr als 35 Stunden Videomaterial zusammengekommen. Die Kodierung der Teilnehmer-ID entspricht der Nummer der Durchführung beginnend bei 1. Somit ist auch einfach herauszufinden, in welcher Gruppe der jeweilige Teilnehmer ist, da lediglich eine Modulo Operation mit 2 benötigt ist. Wenn bei der Operation eine 0 als Ergebnis rauskommt, ist der Teilnehmer in Gruppe A gewesen. Andernfalls ist das Ergebnis der Gruppe B zuzuordnen.

5.1.2 Technische Umsetzung

Die Nutzerstudie wurde online durchgeführt, da es die Organisierung erleichtert und weniger Zeit für die Teilnahme an der Studie in Anspruch

genommen werden muss. Um dies zu bewerkstelligen, müssen die Teilnehmer Zugriff auf das Testsystem durch eine sogenannte Fernzugriff Software erhalten. Zusätzlich müssen die Teilnehmer über einen eigenen Rechner verfügen und an diesem ein Mikrofon haben, damit sie über eine sogenannte Voice-Chat Anwendung mit mir kommunizieren können.

Einrichtung des Testsystems

Aufgrund dessen dass ich nicht möchte, dass die Teilnehmer vollen Zugriff auf mein privates System haben, habe ich mich dazu entschieden ein System nur zur Durchführung der Studie einzurichten. Die Entscheidung fiel hierbei auf die Linux Distribution MX Linux[1], da sie eine hohe Kompatibilität mit meiner Hardware versprach.

Fernzugriff Software

Da der Zugriff auf das Testsystem seitens des Teilnehmers erfolgen muss, ist eine Fernzugriff Software nötig. Hierbei habe ich mich für die Software AnyDesk[2] entschieden, weil diese kostenfrei zur Verfügung steht und nicht auf dem Rechner der Teilnehmer installiert werden muss.

Voice-Chat Anwendungen

Zur Kommunikation mit den Teilnehmern aus der Ferne, ist eine Voice Chat Anwendung nötig. Meistens habe ich dafür die Anwendung Jitsi Meet [3] genutzt, da sie online kostenfrei zur Verfügung steht und seitens der Teilnehmer keine Registrierung und kein installierter Client nötig ist. Bei Teilnehmern, bei denen bereits andere Kontaktdaten bekannt waren, habe ich auch die Plattformen Discord [4] und TeamSpeak [5] genutzt, da es für beide Seiten weniger kompliziert ist.

Software zur Aufzeichnung

Zur Aufzeichnung der Durchläufe mit den Teilnehmern wurde die Software OBS Studio[6] gewählt. Die Software wurde hierbei zur Aufzeichnung meiner Stimme und der Stimme des Teilnehmers verwendet. Zusätzlich wurde durch die Software auch der Bildschirm und somit auch das, was der Teilnehmer macht, aufgezeichnet.

[1] `https://mxlinux.org/`, zuletzt besucht am 13.03.2023
[2] `https://anydesk.com/en`, zuletzt besucht am 13.03.2023
[3] `https://meet.jit.si/`, zuletzt besucht am 13.03.2023
[4] `https://discord.com/`, zuletzt besucht am 13.03.2023
[5] `https://www.teamspeak.com/en/`, zuletzt besucht am 13.03.2023
[6] `https://obsproject.com/`, zuletzt besucht am 13.03.2023

Software zur Terminvergabe

Zur Planung und Vergabe der Termine wurde die Software Doodle[7] verwendet. Hiermit war es für die potentiellen Teilnehmer auch leichter möglich sich einen Termin auszusuchen, da die freien Termine übersichtlich in einem Kalender angezeigt werden. Die vergebenen Termine, an denen die Teilnehmer sich eingetragen haben, wurden zusätzlich in meinem Google-Kalender[8] eingetragen. Zum einen habe ich dadurch eine Erinnerung bekommen, wann der nächste Termin ansteht und zum anderen habe ich damit auch die E-Mail Adresse der Teilnehmer erhalten, um Kontakt zu denen aufzunehmen.

5.2 Beobachtungen

Gedanken um die eigene Privatsphäre

In der ersten Sektion geht es um generelle Fragen, die sich auf die Privatsphäre und das Nutzungsverhalten der Teilnehmer beziehen. Die erste Frage, mit denen die Teilnehmer konfrontiert wurden, ist ob sie sich Gedanken um ihre eigene Privatsphäre im Internet machen. Abbildung 5.1 zeigt das Ergebnis dieser Frage. Hierbei hat kein Teilnehmer angegeben, dass dieser sich gar keine Gedanken um die eigene Privatsphäre macht. Dies zeigt, dass das Konzept der kontextuellen Privatsphäreerklärungen für die Teilnehmer von Interesse sein könnte, da sich jeder Teilnehmer Gedanken um die eigene Privatsphäre im Internet macht. Zusätzlich wurden die Teilnehmer befragt, was der Grund ihrer Sorge ist. Die am häufigsten genannten Gründe und deren Häufigkeit, können der Tabelle 5.1 entnommen werden.

Durchführungszeit der Aufgaben im Anwendungkontext

Es besteht die Grundannahme, dass die nichtfunktionale Anforderung der Erklärbarkeit, die Nutzbarkeit negativ beeinflusst [16]. Um dies zu überprüfen, wurden die Teilnehmer ohne deren Kenntnis in zwei Gruppen aufgeteilt. Beide Gruppen haben die gleichen Aufgaben, auf der in Kapitel 4 entwickelten Oberfläche erledigt. Allerdings mit dem Unterschied, dass Gruppe A die kontextuellen Privatsphäreerklärungen im Prototypen hatte und Gruppe B nicht. Die folgenden Aufgaben, mussten die Teilnehmer erfüllen:

[7] `https://doodle.com/de/`, zuletzt besucht am 13.03.2023
[8] `https://calendar.google.com/calendar/u/0/r`, zuletzt besucht am 13.03.2023

Aussage	**Häufigkeit**
Sammlung der eigenen Daten (durch große Unternehmen)	12
Verlust der Kontrolle über die eigenen Daten	16
Verkauf der eigenen Daten	11
Doxing	2
Profiling	9
Diebstahl von Passwörtern	5
Nutzung bzw Zweckentfremdung von Daten gegen die Person selbst	5
Fehlendes Wissen darüber wofür die Daten verwendet werden	3
Geheimdienste	2
Stalking	2
Öffentliche Verfügbarkeit privater Daten	8
Personalisierte Werbung	8

Tabelle 5.1: Aussagen der Teilnehmer und deren Häufigkeit bezüglich der eigenen Privatsphäre im Internet

1. Posten eines Bildes mitsamt des Standortes
2. Kommentieren eines vorgefertigten Posts mit einem GIF
3. Einen der vorgefertigten Posts mit einem Lesezeichen markieren
4. Suchvorschläge in der Suchleiste öffnen

Die hier gewählten Aufgaben entsprechen Tätigkeiten, die im Anwendungskontext üblich sind. Außerdem sind diese so gewählt, dass möglichst alle Privatsphäreerklärungen von der Gruppe A gesehen werden. Eine Metrik, die sich hierbei gut vergleichen lässt und sich für Usability Tests eignet, ist die Durchführungszeit. Hierbei wird die Zeit gemessen, die der Teilnehmer für die jeweils einzelnen Aufgaben benötigt [22] [42].

Die Abbildung 5.2 und die Abbildung 5.3 zeigen, dass die Aufgaben mit dem Prototypen der Gruppe B schneller gelöst wurden. Der einzige Faktor, der hier abweicht, ist dass die Privatsphäreerklärungen in dem Prototypen für Gruppe B nicht vorhanden sind. Aus den Tabellen 5.2 und 5.3 lassen sich sowohl der Durchschnitt als auch der Median der beiden Gruppen entnehmen. Im Durchschnitt ist die Gruppe B $99,2$ Sekunden und im Median 104 Sekunden schneller gewesen. Daraus lässt sich schließen, dass die Privatsphäreerklärungen einen Einfluss auf die Nutzbarkeit haben.

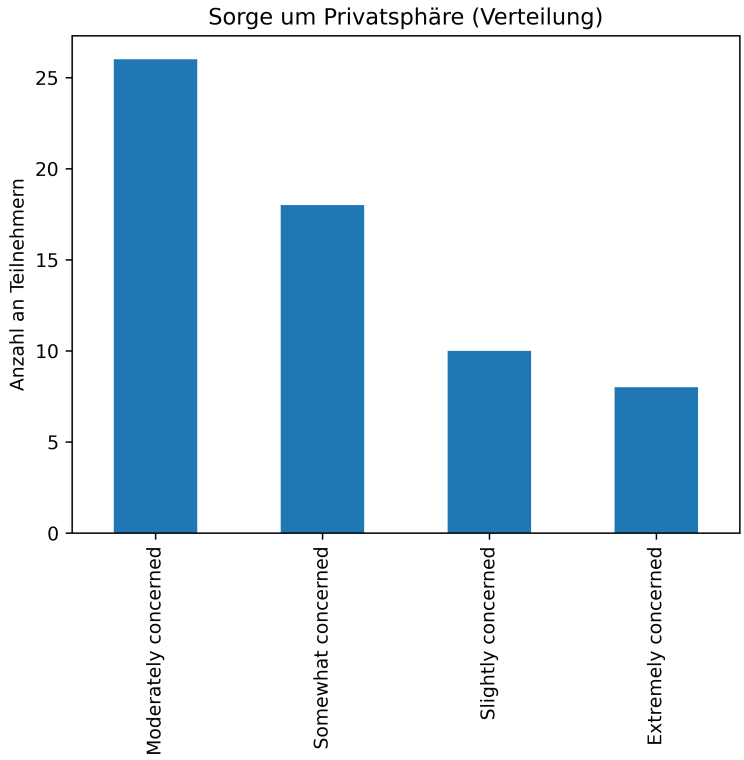

Abbildung 5.1: Sorgen der Teilnehmer bezüglich ihrer Privatsphäre im Internet

Durschschnitt	218,7 Sekunden
Median	201 Sekunden

Tabelle 5.2: Durchschnitt und Median der Gruppe A

Auswertung der Durchführungszeit

Durch statistische Tests, ist es möglich die Validität einer Hypothese durch Prüfung der Nullhypothese zu überprüfen. In diesem Fall werden diese genutzt, um zu überprüfen, ob in der Nutzerstudie eine der beiden Gruppen signifikant schneller war. Hierzu wird die folgende Nullhypothese durch einen zweiseitigen-Hypothesentest geprüft:

> H_0: Es gibt bezüglich der Gesamtdauer keinen Unterschied zwischen Gruppe A und Gruppe B.

Laut Sauro kann der T-Test für 2 unabhängige Mittelwerte verwendet werden. Hierfür sollten folgende Bedingungen gelten [40]:

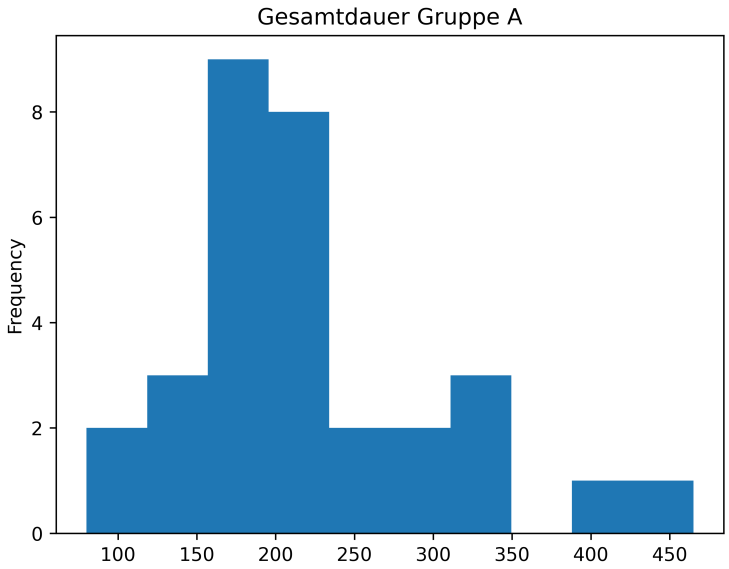

Abbildung 5.2: Gesamtdauer der Aufgaben Gruppe A

Durschschnitt	119,5 Sekunden
Median	97 Sekunden

Tabelle 5.3: Durchschnitt und Median der Gruppe B

1. Beide Stichproben sind repräsentativ für ihre Ausgangspopulationen
2. Beide Stichproben stehen in keinem Zusammenhang zueinander
3. Beide Stichproben sind annähernd normalverteilt
4. Die Varianz beider Gruppen ist annähernd gleich

Bei der Durchführung des T-Tests kann von einer Normalverteilung ausgegangen, da für beide Gruppen $n \geq 30$ und somit der zentrale Grenzwertsatz gilt [30] [40]. Der vierte Punkt, lässt sich laut Sauro mit dem Verhältnis beider Standardabweichungen prüfen. Ist das Verhältnis zwischen beiden Standardabweichung größer als 3, würde dies der Bedingung widersprechen [40]. Die Standardabweichung für Gruppe A beträgt etwa $83,9$ und für Gruppe B etwa $83,2$. Hiermit ist das Verhältnis kleiner als 2 und es kann von einer annähernd gleichen Varianz ausgegangen werden. Somit sind die Bedingungen für den T-Test mit 2 unabhängigen Mittelwerten erfüllt und

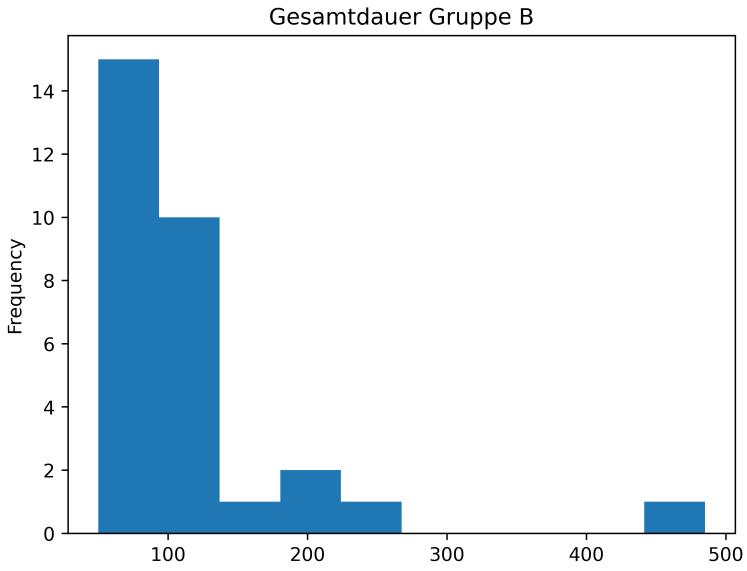

Abbildung 5.3: Gesamtdauer der Aufgaben Gruppe B

kann auf dem Datensatz angewendet werden. Aufgrund dessen dass zeitliche Messungen positiv verzerrt sein können, werden die mithilfe des natürlichen Logarithmus, in eine logarithmische Darstellung umgewandelt [39]. Als Konfidenzintervall werden 95% angestrebt. Wird nun der T-Test auf die logarithmisierten Werte angewendet, ist das Ergebnis für den t-Wert 6.1674 und für den p-Wert 0.00001. Somit gilt, dass $p < 5\%$ ist und damit darf die formulierte Nullhypothese verworfen werden.

Wahrnehmung der Privatsphäreerklärungen

Nach der Durchführung der Aufgaben, wurden die Probanden der Gruppe A zusätzlich befragt, ob sie etwas bei der Bewältigung der Aufgaben gestört hat. Falls die Teilnehmer die Frage mit einem „ja“ beantwortet haben, wurden sie zusätzlich gefragt, ob es sich auf die Privatsphäreerklärungen bezieht oder nicht. Weiterhin wurden die Teilnehmer dazu befragt, ob sie einen Mehrwert bezüglich der Privatsphäreerklärungen entnehmen konnten. 17 von 31 Teilnehmern aus der Gruppe A hatten das Gefühl, dass die Privatsphäreerklärungen bei der Bearbeitung der Aufgaben gestört haben. Dies entspricht etwa $54,8\%$. Von diesen 17 Personen haben 14 Personen dennoch einen Mehrwert darin gesehen. Einige Teilnehmer haben die Privatsphäreerklärungen als beruhigend wahrgenommen und hatten das Gefühl, das nichts verheimlicht wird.

Verständnis der Privatsphäreerklärung

Wie in Abschnitt 3.3 bereits erwähnt, ist die Anforderung der Verständlichkeit wichtig, da es den Weg zur Software-Transparenz ebnen kann. Um diese Eigenschaft zu prüfen, wurde ein Verständnistest angefertigt, bei dem die Teilnehmer die folgenden Aussagen bezüglich der Privatsphäreerklärungen beantworten müssen:

Aussagen bezüglich der Privatsphäreerklärung zu GIPHY

1. Die Erklärung enthält den Inhalt der Nutzungsbedingungen von GIPHY
2. Die Erklärung beinhaltet wie lange das gepostete GIF gespeichert wird
3. Die Erklärung beinhaltet, dass die eigenen Nutzerdaten an GIPHY weitergeleitet werden

Aussagen bezüglich der Privatsphäreerklärung zur Kamera

1. Die Erklärung enthält alternative Wege, um ein Bild zu posten
2. Die Erklärung beinhaltet den Inhalt der DSGVO
3. Die Erklärung enthält Informationen darüber, wann die Kamera angeschaltet wird

Bei der Bewertung der Korrektheit der Antworten, wurde auch die Begründung der Teilnehmer berücksichtigt. Hat ein Teilnehmer z.B. gesagt, dass die DSGVO inhaltlich vertreten ist und dabei auch gesagt, dass diese verlinkt ist, so wurde die Antwort dennoch als richtig bewertet, da der Kern der Frage somit richtig beantwortet wurde. Wenn die Ergebnisse für die Privatsphäreerklärungen einzeln betrachtet werden, stellt sich heraus, dass 26 Teilnehmer die inhaltlichen Fragen für die Privatsphäreerklärung zur Kamera vollständig korrekt beantworten konnten, während es bei der Privatsphäreerklärung zu GIPHY lediglich 5 Teilnehmer sind. Anhand der Abbildung 5.4 ist erkennbar, dass mehr als die Hälfte der Teilnehmer mindestens 4 Fragen korrekt beantwortet haben. Jedoch muss auch berücksichtigt werden, dass keiner der Teilnehmer alle 6 Fragen korrekt beantwortet hat. Aus der Tabelle 5.4 können die einzelnen Aussagen und die Anzahl der korrekten, der falschen und den enthaltenen Antworten entnommen werden.

Aussage	Σ richtig	Σ falsch	Σ unsicher
Die Erklärung enthält den Inhalt der Nutzungsbedingungen für GIPHY.	38	14	10
Die Erklärung beinhaltet wie lange das gepostete GIF gespeichert wird.	54	2	6
Die Erklärung sagt aus, dass die eigenen Nutzerdaten an GIPHY bereitgestellt werden.	13	26	23
Die Erklärung enthält Informationen über alternative Wege, um ein Bild hochzuladen.	53	1	8
Die Erklärung enthält den Inhalt der DSGVO.	44	11	7
Die Erklärung enthält Informationen darüber, wann die Kamera angeschaltet wird.	34	13	15

Tabelle 5.4: Auswertung der Antworten kategorisiert nach Aussagen.

Auswertung des eingeschätzten Verständnisses

Neben der Prüfung des Verständnisses der Privatsphäreerklärungen, wurde auch das wahrgenommene Verständnis seitens der Teilnehmer abgefragt.

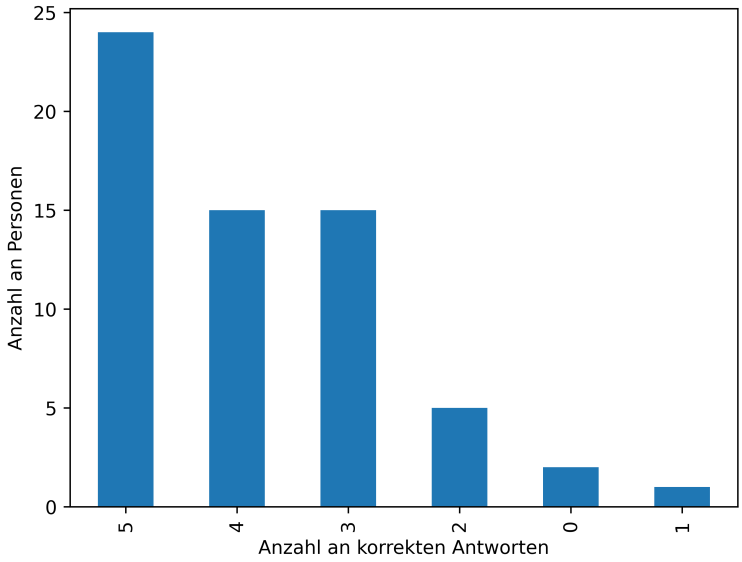

Abbildung 5.4: Anzahl der korrekt angegebenen Antworten

Hierfür sollten die Teilnehmer die folgenden Fragen mit einer 5-stufigen-Likert-Skala (überhaupt nicht einverstanden - vollkommen einverstanden) beantworten:

1. Ich habe die Erklärung für GIPHY vollkommen verstanden
2. Ich habe die Erklärung zur Kamera vollkommen verstanden

Die Einschätzung der Teilnehmer bezüglich des Verständnisses der Privatsphäreerklärungen, kann aus Abbildung 5.5 und Abbildung 5.6 entnommen werden. Um zu überprüfen, ob eine der beiden Privatsphärerklärungen, von den Teilnehmern als verständlicher wahrgenommen wurde, wird die folgende Nullhypothese mithilfe eines zweiseitigen-Hypothesentest überprüft:

H_0: Es gibt bezüglich des wahrgenommen Verständnisses keinen Unterschied zwischen der Privatsphärerklärung für Giphy und der zur Kamera.

Zur Überprüfung wurde der Wilcoxon-Vorzeichen-Rang-Tests verwendet. Zur Durchführung des Tests, wurden die Antworten der Likert-Skala numerisch umgewandelt, sodass die Antwortoption „überhaupt nicht einverstanden“ mit einer 1 und die Antwortoption „vollkommen einverstanden“ mit einer 5 übersetzt wurde. Bei der Durchführung des Tests wurde ein Konfidenzintervall von 95% angestrebt. Als Ergebnis kommt ein Z-Wert in Höhe von -4.5409 und ein p-Wert in Höhe von etwa 0.00001 raus. Somit gilt, dass $p < 5\%$ ist. Hiermit kann die formulierte Nullhypothese verworfen werden und somit kann angenommen werden, dass es bei dem wahrgenommenen Verständnis der beiden Privatsphäreerklärungen einen Unterschied gibt. Dies kann auch durch den Vergleich beider Durchschnittswerte gestützt werden. Wenn die Likert-Skala nummerisch übersetzt wird, ist es möglich einen Durchschnitt der Antworten zu bestimmen. Hierbei ergibt sich für die Privatsphäreerklärung der Kamera ein Durchschnitt von $\overline{x_1} \approx 4,35$ und für die Privatsphäreerklärung zu GIPHY ein Durchschnitt von $\overline{x_2} = 3,5$.

Wahrgenommene Relevanz der Privatsphäreerklärungen

Es besteht durch den in Abschnitt 2.4 angesprochenen Privacy-Calculus die Grundannahme, dass einzelne Privatsphäreerklärungen von den Teilnehmern als relevanter angesehen werden, da die Teilnehmer trotz der Tatsache, dass sie über ihre eigene Privatsphäre aufgeklärt werden abwägen, ob die dargestellten Informationen für sie relevant sind. Aus der Abbildung 5.7

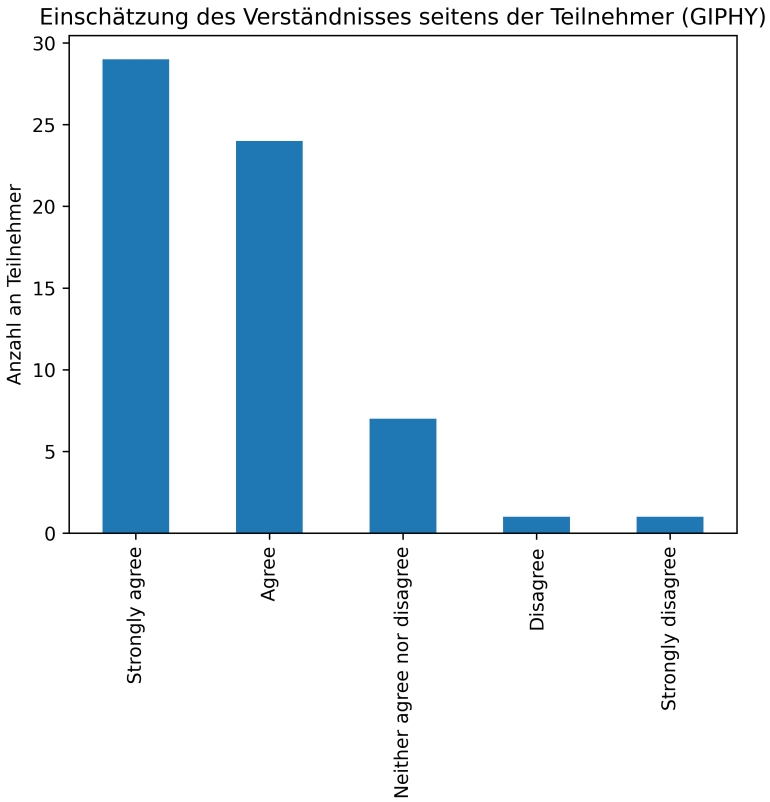

Abbildung 5.5: Einschätzung des Verständnisses bezüglich der Privatsphärerklärung zu GIPHY

lässt sich entnehmen, dass z.B. die Privatsphärerklärung für GIPHY von den Teilnehmern als weniger relevant eingestuft wurde als die Privatsphäreerklärung für GPS. Als Begründung wurde dafür häufig genannt, dass es sich bei GIPHY lediglich um GIFs handelt, die nicht vom Benutzer selbst stammen, was auf den Standort nicht zutrifft, da diese Daten vom Gerät des Benutzers stammen. Lediglich 6 der 62 Teilnehmer haben bei der Einstufung der Relevanz der einzelnen Privatsphäreerklärungen nicht differenziert und alle Privatsphäreerklärungen als relevant eingestuft.

Wenn die Antwortmöglichkeiten auf der Likert-Skala nummerisch übersetzt werden, ist es möglich einen Durchschnittswert für die gegebenen Antworten zu bestimmen. Die Durchschnittswerte der Relevanz einzelner Privatsphäreerklärungen, können der Tabelle 5.5 entnommen werden.

Hieraus lassen sich die Privatsphäreerklärungen, die von den Teilnehmern im Durchschnitt als relevant eingestuft wurden ablesen. Sobald ein Durchschnitt größer als $3,5$ ist, wird die dazugehörige Privatsphäreerklärung als relevant eingestuft, da dieser Wert aufzeigt, dass die Teilnehmer eher dazu tendierten der Aussage bezüglich der Relevanz der Privatsphäreerklärungen

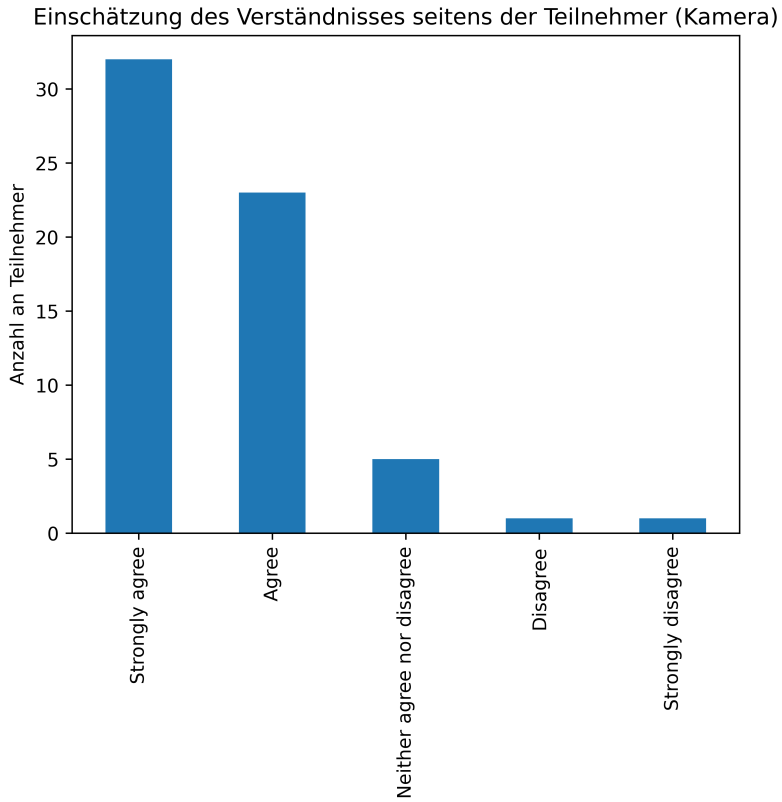

Abbildung 5.6: Einschätzung des Verständnisses bezüglich der Privatsphärerklärung zur Kamera

zuzustimmen. Dementsprechend sind folgende Privatsphäreerklärungen von den Teilnehmern als relevant eingestuft:

- Kamera
- Lokaler Speicher (Bilder)
- GPS
- Manuelle Standorteingabe
- Erstellung eines Posts
- Suche

Bedienbarkeit des Systems

Zur Untersuchung der Bedienbarkeit des Systems, wurden die Teilnehmer zum Schluss darum gebeten, die folgenden drei Fragen aus dem SUS(System-

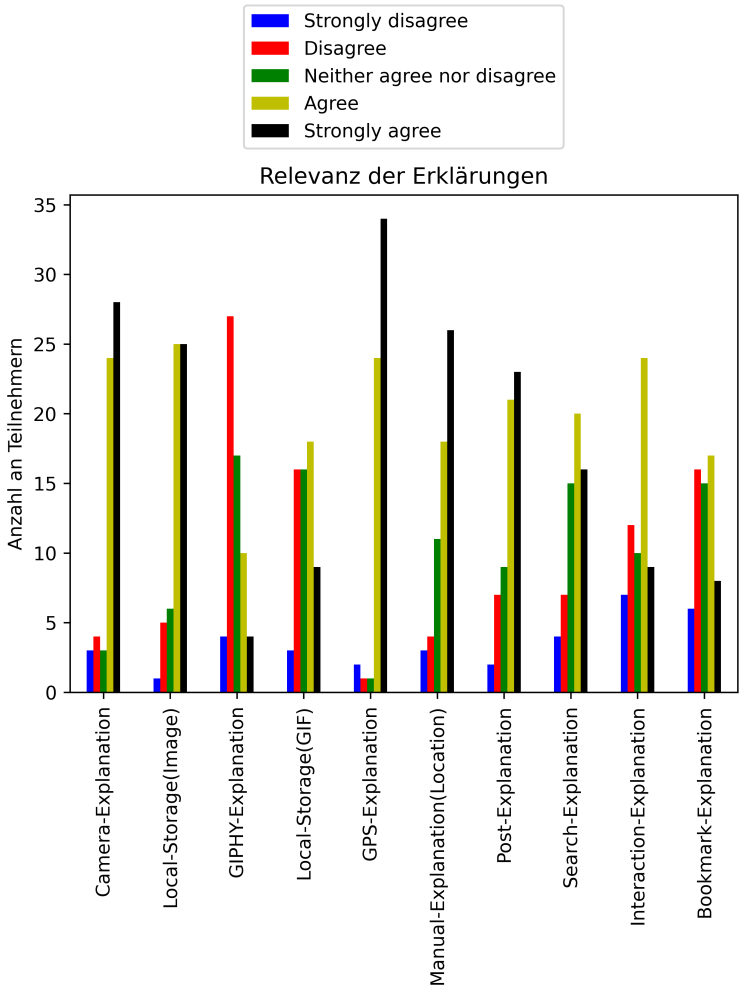

Abbildung 5.7: Einstufung der Relevanz einzelner Privatsphäreerklärungen

Usability-Score)-Fragebogen zu beantworten [8]:

1. Ich kann mir vorstellen Privatsphärerklärungen regulär zu nutzen
2. Ich denke, dass Privatsphärerklärungen einfach zu nutzen sind
3. Ich denke, dass die Mehrheit an Personen Privatsphäreerklärungen nutzen können

Hierbei muss bei der Berechnung des SUS beachtet werden, dass lediglich 30 von 100 Punkten erreicht werden können, da lediglich 3 von 10 Fragen

Privatsphäreerklärung	Durchschnittliche Antwort auf der Likert-Skala (gerundet)
Kamera	4,13
Lokaler Speicher (Bilder)	4,1
GIPHY	2,73
Lokaler Speicher (GIF)	3,23
GPS	4,4
Manuelle Standorteingabe	3,97
Erstellung eines Posts	3,9
Suche	3,6
Interaktion	3,26
Lesezeichen	3,08

Tabelle 5.5: Durchschnittswerte bezüglich der Relevanz der Privatsphäreerklärungen

aus dem Bogen verwendet werden. Der SUS wird nach Brooke bestimmt und die Likert-Skala numerisch mit den Werten von 0 bis 4 übersetzt [8]. Wenn die Rechnung auf die Ergebnisse aus der Nutzerstudie angewendet werden, kommt für die ersten beiden Fragen ein Zwischenergebnis von etwa $3,1$ und für die dritte Frage ein Zwischenergebnis von etwa 3 raus. Werden die Ergebnisse nun aufsummiert und mit $2,5$ multipliziert, so kommt für den durchschnittlichen SUS ein Wert in Höhe von etwa $23,185$ raus. Um den Wert zu vergleichen, muss dieser in die korrekte Relation gesetzt werden. Da Brooke in der Vorlage 10 Fragen verwendet hat [8], wird der SUS mit $\frac{10}{3}$ multipliziert. Dadurch kommt ein skalierter SUS in Höhe von etwa $77,285$ raus. Dieser Wert liegt in einem guten Bereich [9] [6].

Eine Sorge, die bezüglich der dritten Frage häufig genannt wurde, ist dass ältere Personen, denen die Bedienung von Software häufig schwer fällt, die Privatsphäreerklärungen nicht nutzen bzw. auch verstehen können. Außerdem wurde der ersten Frage häufig nur unter der Bedingung zugestimmt, wenn die Privatsphärerklärungen wie in dem Prototypen nur geöffnet werden, sofern diese noch nicht aktiv abgelehnt oder angenommen wurde. Dies könnte darauf hindeuten, dass diese, zumindest in dem Moment an dem sie angezeigt werden, als störend wahrgenommen werden.

5.3 Feedback der Teilnehmer

Die Teilnehmer hatten im Rahmen der Nutzerstudie die Möglichkeit anzugeben, was sie an den Privatsphäreerklärungen ändern würden. An der Stelle haben Teilnehmer Feedback bezüglich der Nutzbarkeit hinterlassen.

Unter anderem wurden die Navigationspfeile von einigen Teilnehmern angesprochen. Diese sollten laut einigen Teilnehmern nicht existieren. Statt-

dessen haben sich die betroffenen Teilnehmer gewünscht, dass es keine Seiten gibt und innerhalb der Privatsphäreerklärungen das Scrollen möglich sein soll. Außerdem wurde das Fragezeichen-Icon und der dort hinterlegte Hinweis bezüglich der Folgen des Ablehnens der Privatsphäreerklärung angesprochen, da die betroffenen Teilnehmer die Interaktionsmöglichkeit nicht für selbsterklärend gehalten haben. Daher haben sich die Teilnehmer gewünscht, dass die hinterlegte Information ohne jegliche Geste zugänglich ist und wie jede andere Information aufgelistet wird und nicht versteckt wird.

Weiterhin wurden die „legally required“ und „Personnel“ kritisiert. Beide Formulierungen beziehen sich auf die Frage „Wer kann meine Daten einsehen?“. Hier ist es für die betroffenen Teilnehmer unklar, wann es rechtlich nötig ist und ob unter „Personnel“ alle Mitarbeiter oder nur einzelne Mitarbeiter gemeint sind. Zudem wurde kritisiert, dass nicht klarifiziert wird, wann genau auf die Kamera zugegriffen wird. Des weiteren haben sich einige Teilnehmer für mehr Informationen ausgesprochen wie z.B. durch eine FAQ Sektion. Der Button zum Zurücksetzen der Privatsphäreerklärungen ist für einige Teilnehmer nicht als solcher erkennbar gewesen. Hier wurde der Vorschlag aufgebracht, dass dieser durch ein „Zurück“-Pfeil ersetzt wird.

5.4 Demographie

Der Folgende Abschnitt beschäftigt sich mit der Auswertung der demographischen Daten bezüglich der Teilnehmer. Hierbei werden Faktoren wie das Alter und der Bildungsgrad berücksichtigt. Außerdem wird die Erfahrung der Teilnehmer mit der Plattform Twitter 2 berücksichtigt, da der in Kapitel 4 entwickelte Prototyp desgintechnisch auf dieser Plattform basiert.

Auswertung der demographischen Daten

Die Personen, die an der Nutzerstudie teilgenommen haben, stammen aus dem privaten Umfeld und aus der Fachgruppe Software Engineering an der Leibniz Universität Hannover. Insgesamt haben 62 Personen an der Studie teilgenommen, wovon etwa $74,2\%$ männlich und etwa $24,2\%$ weiblich sind. Lediglich eine Person hat sich bei der Angabe der Geschlechtsidentität enthalten und keine Person hat ein nicht-binäres Geschlecht angegeben.

Von den 62 Teilnehmern ist ein Teilnehmer minderjährig. Ansonsten gilt, dass die Teilnehmer gesetzlich volljährig sind und das 18. Lebensjahr überschritten haben. Der Median für das Alter der Teilnehmer beträgt 25 und der Durchschnitt etwa 28.

Nach der Definition, die von Chazette und Schneider [17] verwendet wurde gilt, dass Personen mit einem Geburtsjahr von 1980 oder früher als sogenannte „digital immigrants“ zu bezeichnen sind. Personen die nach dem Jahr 1980 geboren sind gelten als „digital natives“ [17]. Auf den jetzigen Zeitpunkt übertragen bedeutet dies, dass Personen mit einem Alter von 43

oder höher als „digital immigrants“ einzustufen sind. Dies trifft auf 4 der 62 Teilnehmer zu, was etwa $6,45\%$ der Teilnehmer entspricht. Im Umkehrschluss bedeutet dies, dass 58 Teilnehmer „digital natives“ sind, was etwa $93,55\%$ der Teilnehmer entspricht.

Neben dem Alter und der Geschlechtsidentität wurden die Teilnehmer bezüglich ihres Berufes befragt. Hierbei hat sich herausgestellt, dass 24 von 62 Teilnehmern Studenten sind und somit etwa $38,7\%$ ausmachen. Weiterhin haben 13 von 62 Teilnehmern (etwa $20,97\%$) angegeben, dass sie IT-Berufe ausüben. Außerdem arbeiten 4 von 62 Teilnehmern im öffentlichen Dienst und der gleiche Anteil an Teilnehmern arbeitet als wissenschaftlicher Mitarbeiter. Diese beiden Gruppen machen jeweils etwa $6,45\%$ der Teilnehmer aus.

Zu Beginn der Studie wurden die Teilnehmer auch gefragt, ob sie mit der Plattform Twitter 2 vertraut sind. 29 von 62 Teilnehmern (etwa $46,77\%$) haben mündlich ausgesagt, dass sie mit der Plattform Twitter vertraut sind. Von diesen 29 Teilnehmern sind 14 in der Gruppe A und 15 in der Gruppe B.

Kapitel 6

Diskussion

In diesem Kapitel werden die gefundenen Ergebnisse aus dem Kapitel 5 intepretiert. Daraufhin werden mögliche Probleme und Limitierungen einzelner Fragen der Studie angesprochen. Zum Schluss wird in Kapitel 8 ein abschließendes Fazit gezogen.

6.1 Interpretation der Ergebnisse

Die Abbildung 5.1 zeigt, dass alle 62 Teilnehmer sich grundsätzlich Gedanken um die eigene Privatsphäre im Internet machen. Von 62 Teilnehmern sind 34 laut eigenen Angaben mindestens mäßig besorgt um ihre eigene Privatsphäre im Internet. Vor diesem Hintergrund lässt sich zeigen, dass kontextuelle Privatsphähreerklärungen von Interesse sind, da diese wie in Kapitel 3 beschrieben, konzeptuell einige Punkte ansprechen, die für die eigene Privatsphäre von Interesse sind.

Die Teilnehmer haben zudem auch genannt was ihre Sorgen sind. Häufig lassen diese Sorgen darauf schließen, dass das Vertrauen und die Aufklärung seitens des Systems fehlt, was daher kommen kann, dass diese Aufklärung häufig lediglich durch die Nutzungsbedingungen stattfindet. Weiterhin sind diese häufig nicht direkt sichtbar, sodass diese schnell in Vergessenheit geraten können. Zusätzlich handelt es sich hierbei um juristische Texte, die zwar die rechtlichen Bedingungen erfüllen, aber sprachlich schwer zu erfassen sind. Im Gegensatz zu den Nutzungsbedingungen erfüllen die Privatsphäreerklärungen zwar nicht die rechtlichen Grundlagen und ersetzen diese auch nicht, aber sie können sich als Ergänzung zu diesen eignen, da sie für den Nutzer sichtbarer sind und da die Nutzer vor der Benutzung einer Funktionalität sich aktiv entscheiden müssen, ob sie die Privatsphäreerklärung akzeptieren.

RQ1: Welchen Einfluss haben kontextuelle Privatsphäreerklärungen auf die Usability?

Durch die Literaturrecherche konnte ich bereits herausfinden, dass die nicht-funktionale Anforderung der Erklärbarkeit einen Einfluss auf die Nutzbarkeit haben kann [16]. Dies ist insofern nachvollziehbar, wenn das hier erstellte Konzept als Beispiel herangezogen wird. Sobald ein Nutzer z.B. ein Bild hochladen möchte, wird dieser mit einer Privatsphäreerklärung konfrontiert, die die Anforderung der Erklärbarkeit erfüllt. Bei der Erreichung des Ziels ist dies ein weiterer Zwischenschritt, der davor nicht in der Form existiert hat. Dies bedeutet, dass grundsätzlich mehr Zeit benötigt wird um das Ziel zu erreichen. Wenn angenommen wird, dass die gleiche Person die Aufgabe umsetzt, wird sie mit der Privatsphäreerklärung wahrscheinlich immer mehr Zeit benötigen, da die Privatsphäreerklärung erstmal als solche erkannt werden muss und zusätzlich wird verlangt, dass der Nutzer aktiv wird.

Diese Annahmen lassen sich durch die Beobachtungen aus Abschnitt 5.2 bestätigen. Den Graphen (Abbildung 5.2 Abbildung 5.3) ist zu entnehmen, dass die Teilnehmer in Gruppe B häufiger schneller durch durch die Aufgaben gekommen sind als die Teilnehmer der Gruppe A. Aus den Tabellen 5.2 und 5.3, können der jeweilige Durchschnitts- und Median-Wert entnommen werden.

Die in Abschnitt 5.2 formulierte Nullhypothese wurde verworfen. Dies stützt die Befunde, da ein Unterschied bezüglich der Gesamtdauer zwischen den beiden Gruppen und somit auch dem Prototypen mit den Privatsphäreerklärungen und ohne den Privatsphäreerklärungen, festgestellt wurde.

Die Ergebnisse aus Abschnitt 5.2 weisen darauf hin, dass ein Einfluss besteht und dass die Privatsphäreerklärungen als störend wahrgenommen werden. Die betroffenen Teilnehmer konnten dennoch häufig einen Nutzen darin sehen.

Der ausgewertete skalierte SUS in Höhe von etwa $77,285$ deutet auf eine gute Nutzbarkeit der Privatssphäreerklärungen. Allerdings muss hier zwischen dem Einfluss auf die Nutzbarkeit des gesamten Systems und der Nutzbarkeit der Privatsphäreerklärungen selbst differenziert werden.

RQ2: Inwiefern ist das Konzept der kontextuellen Privatssphäreerklärungen für die Benutzer nachvollziehbar?

In der Arbeit von Droste wurde beantwortet, wie die Privatsphäreerklärungen strukturiert sein müssen, um für die Teilnehmer verständlich zu sein [21]. Allerdings ist dadurch noch nicht geklärt, inwiefern diese inhaltlich verständlich sind und wie die Teilnehmer ihr eigenes Verständnis einschätzen.

Weiterhin ist durch das Journal von Brunotte ersichtlich, dass die Privatsphäreerklärungen kurze und präzise Erklärungen beinhalten müssen, die in einfacher und nicht technischer Sprache formuliert sein müssen [12]. Diese Kriterien können dafür sorgen, dass möglichst viele Personen die Erklärungen, die denen präsentiert werden, verstehen.

In Abschnitt 5.2 ist sichtbar, dass es einen Unterschied bezüglich der Privatsphäreerklärungen gibt, wenn das Verständnis seitens der Teilnehmer eingeschätzt wird. Die verworfene Nullhypothese und die Abweichungen im Durchschnitt deuten darauf hin, dass die Privatsphäreerklärung für die Kamera von den Teilnehmern eher als verständlich wahrgenommen wurde.

Neben des wahrgenommenen Verständnisses wurde auch das inhaltliche Verständnis der Teilnehmer bezüglich der beiden Privatsphäreerklärungen geprüft. Insgesamt betrachtet haben über die Hälfte der Teilnehmer mindestens 4 inhaltliche Fragen korrekt beantworten können, jedoch hat kein Teilnehmer alle 6 Fragen korrekt beantwortet. Dies könnte bedeuten, dass die Privatsphäreerklärungen inhaltlich eher schwer verständlich sind. Dieses Ergebnis bestätigt die Befunde bezüglich des wahrgenommenen Verständnisses.

RQ3: Unter welchen Umständen ist die Konfrontation der Nutzer mit den kontextuellen Privatsphäreerklärungen im gewählten Anwendungskontext angemessen?

Durch die vorausgegangenen Konzepte der Privatsphäreerklärungen wurde der Inhalt und die Struktur dieser festgelegt, jedoch wurden diese nicht in einem Anwendungskontext eingesetzt [12] [21]. Dies ist mit der Ausarbeitung dieses Konzeptes erfolgt. Allerdings ist nicht klar, inwiefern die einzelnen Privatsphäreerklärungen im gewählten Anwendungskontext angemessen sind.

Wie in Abschnitt 2.4 beschrieben, gibt es eine Schwelle zwischen Risiko und nutzen. Dies lässt sich ebenso im Verhalten der Nutzer beobachten, denn es ist in der Abbildung 5.7 erkennbar, dass z.B. die Kamera-Erklärung von den Teilnehmern eher als relevant eingestuft wurde als die GIPHY-Erklärung. Ein Grund der seitens der Teilnehmer für diese Einstufung genannt wurde ist, dass es sich bei GIPHY nicht um die eigenen Bilder handelt, während es sich bei der Kamera nicht nur um das eigene Bild handelt, sondern auch um die eigene Hardware. Dies könnte darauf hinweisen, dass die Teilnehmer bei der Nutzung von GIPHY kein hohes Risiko sehen und deshalb diese Privatsphäreerklärung als weniger relevant betrachten.

6.2 Limitierung der Ergebnisse

Bezüglich der Frage ob die Teilnehmer sich Gedanken um ihre Privatsphäre im Internet machen, können die Antworten der Teilnehmer nicht validiert werden. Es ist möglich, dass die Teilnehmer diese Frage nicht der Realität entsprechend beantwortet haben, da sie in dieser Situation voreingenommen sind.

Bei der Frage ob die Privatsphäreerklärung bei der Bearbeitung der Aufgaben als störend wahrgenommen wurden ist es möglich, dass die Teilnehmer nicht „gemein“ sein wollten. Auch hier sind die Teilnehmer bezüglich dieser Position voreingenommen und wollten eventuell deshalb nicht die Aussage bestätigen.

So ähnlich betrifft dies auch die Fragen aus dem SUS Fragebogen. Dort ging es darum, ob die Teilnehmer sich vorstellen können die Privatsphäreerklärungen regulär zu nutzen und ob diese leicht nutzbar sind. Da die Person, die das Konzept implementiert hat, in dem Fall mit denen gesprochen hat, ist es möglich, dass eher selten Kritik veräußert wird.

Die Gesamtdauer der einzelnen Gruppen bezüglich der Aufgaben, die auf dem Prototypen erledigt werden mussten, könnte dadurch beeinflusst sein, dass die Gruppen zufällig entstanden sind und vorher nicht eingeschätzt wurde wie gut die Personen im Umgang mit sozialen Medien bzw. mit Technik generell sind. Außerdem muss auch beachtet werden, dass im Vorhinein auch nicht geprüft wurde wie gut das Verständnis der englischen Sprache ist. Es kam des öfteren vor, dass Teilnehmer um eine Übersetzung einzelner Wörter gebeten haben. Allerdings kann nicht gesagt werden ob die Teilnehmer, die Schwierigkeiten in der englischen Sprache haben, sich auch wirklich immer dann geäußert haben, wenn sie etwas nicht verstanden haben. Der in Abschnitt 5.2 durchgeführte statistische Test hat als Bedingung, dass die Stichproben repräsentativ sind für die Ausgangspopulation. Durch die Werte in Abschnitt 5.4 ist jedoch ersichtlich, dass die Teilnehmer die Allgemeinheit nicht repräsentieren, da die Studenten mit einem Anteil an etwa $38,7\%$ überrepräsentiert sind.

Dies betrifft auch die inhaltlichen Fragen zum Verständnis der Privatsphäreerklärungen. Es kam z.B. häufiger vor, dass Teilnehmer die Formulierung „The explanation includes the contents of the terms of service for GIPHY.“ falsch verstanden haben. Die betroffenen Teilnehmer haben diese Aussage häufig so interpretiert, dass es um die Verlinkung zu den besagten Nutzungsbedingungen geht. Nur wenige Teilnehmer haben die Aussage so verstanden wie sie gemeint ist. Nämlich geht es um den Inhalt der Nutzungsbedingungen. Einerseits handelt es sich hierbei um eine sprachliche Barriere seitens der Teilnehmer, da die Formulierung auf Englisch ist. Andererseits kann es sich hierbei auch um eine schlecht gewählte Formulierung handeln, da es auch so ausgelegt werden kann, dass anhand einer Verlinkung der Inhalt auch enthalten ist. Weiterhin

wurden lediglich 2 von 9 Privatsphäreerklärungen inhaltlich überprüft und zusätzlich auch nur in einigen ausgewählten inhaltlichen Aspekten. Um auf ein fundiertes Ergebnis zu kommen, müssten alle inhaltlichen Aspekte in allen Privatsphäreerklärungen abgedeckt werden, was jedoch mehr Zeit seitens der Teilnehmer abverlangen würde.

Außerdem ist es bei dem wahrgenommenen Verständnis der Privatsphäreerklärungen möglich, dass die Teilnehmer sich entweder selber unterschätzt oder überschätzt haben. Zusätzlich könnte sich ein Teilnehmer nicht trauen zuzugeben, dass sie etwas nicht verstanden haben und deswegen angeben, dass sie die Privatsphäreerklärung verstanden haben, obwohl dies nicht der Wahrheit entspricht. Das Verständnis der einzelnen Teilnehmer ließe sich zumindest im Rahmen der abgefragten Inhalte überprüfen, jedoch betrifft dies nicht die Wahrnehmung der Personen. An der Stelle muss differenziert werden, da sich die Wahrnehmung so ohne weiteres sich nicht prüfen lässt. Außerdem haben die Teilnehmer die Privatsphäreerklärung zu GIPHY vor der Erklärung der Kamera gesehen. Dies kann das Ergebnis insofern beeinflussen, dass sie sich inhaltlich in einigen Aspekten ähneln und die Teilnehmer bereits einzelne Seiten kannten, was denen ein sichereres Gefühl bezüglich der Privatsphäreerklärung zur Kamera geben kann.

6.3 Gefundene Nutzbarkeit-Probleme

Trotz eines hohen skalierten SUS, der im guten Bereich liegt, konnten Probleme bezüglich der Nutzbarkeit festgestellt werden. Unter anderem ermöglicht eine implementierte Standorteingabe zwar eine hohe Immersion bei der Nutzung des Prototypen, jedoch trat häufig das Problem auf, dass die Teilnehmer der Studie einen Button zur Bestätigung der Standorteingabe erwartet haben. Dieser Button wurde allerdings nicht implementiert. Stattdessen wird die Eingabe das Standortes automatisch akzeptiert und auf den aktuellen Post angewendet, was im ersten Moment für Verwirrung sorgen kann. Dies könnte die Gesamtdauer hinsichtlich der Erfüllung der Aufgaben innerhalb des Prototypen beeinflusst haben, jedoch wurden beide Gruppen mit diesem Problem konfrontiert, was diesen Effekt wieder ausgleichen könnte. Außerdem ist das genutzte OpenStreetMap-Plugin im Prototypen in einigen Durchläufen abgestürzt. Dies hatte zwar keinen Einfluss auf das Experiment, da die Beseitigung des Fehlers nicht viel Zeit in Anspruch genommen hat und dies aus der Bewertung ausgeschlossen wurde, aber es hat gestört und für Verwirrung gesorgt.

Bezüglich der inhaltlichen Frage, ob die Privatsphäreerklärung zu GIPHY beinhaltet, dass die Nutzerdaten an GIPHY übertragen werden, kann beobachtet werden, dass nur 13 von 62 Teilnehmern diese Aussage korrekt beantworten konnten. Dies ist besonders auffällig, da es die Aussage mit den wenigsten korrekten und mit den meisten falschen Antworten ist. Zusätzlich

dazu hat die Aussage auch die höchste Anzahl an Teilnehmern, die sich bei der Antwort enthalten haben. Bei jeden dieser Rekorde führt diese Aussage mit weitem Abstand. Dies liegt wahrscheinlich daran, dass die Antwort in der Privatsphäreerklärung hinter einem Hinweistext versteckt ist, der nur erscheint sobald über dem „?"-Icon gehovert wird. Häufig haben die Teilnehmer zwar mitbekommen, dass etwas dahinter versteckt ist, da auch der Mauszeiger sich verändert hat, sobald dieser in die Region des Icons gelangt, jedoch musste ich häufig feststellen, dass nach später erfolgter Rückfrage die betroffenen Teilnehmer erwartet haben, dass der Hinweistext mit einem Klick auf das Symbol erscheint. In diesem Fall liegt eine sogenannte „false affordance" vor, da das Icon zwar signalisiert, dass eine Aktion hinterlegt ist, jedoch wird dieses Signal seitens der Teilnehmer falsch interpretiert [13].

Außerdem gab es einige Teilnehmer, die die Navigation mit den verschiedenen Seiten innerhalb der Privatsphäreerklärung falsch interpretiert haben. Diese wurde nämlich so interpretiert, dass die Punkte als Schritt X von N wahrgenommen wurden und die einzelnen Punkte akzeptiert werden müssen, wodurch es bei den Teilnehmern dazu kam, dass sie gedanklich den ersten Punkt akzeptiert haben, in Wirklichkeit aber die gesamte Privatsphäreerklärung akzeptiert haben. Solch ein Design wird unter anderem bei der Installation der Linux Distribution Ubuntu angewendet [1].

Einige dieser Probleme sind durch die Umsetzung der in Abschnitt 5.3 erwähnten Wünsche behebbar.

6.4 Kritik zur durchgeführten Nutzerstudie

Im Nachhinein sind mir Teile der Nutzerstudie aufgefallen, die besser gelöst werden könnten.

Bei der Überprüfung des Einflusses auf die Nutzbarkeit mithilfe der Zeitmessung und der Aufgaben, wäre es praktischer gewesen die Aufgaben in schriftlicher Form z.B. auf dem Prototypen anzuzeigen. Somit wäre es zu weniger Missverständnissen gekommen. Allerdings wurden die Zeitpunkte an denen die Teilnehmer Rückfragen gestellt haben oder die Aufgabe nicht verstanden haben, nicht in die Wertung eingerechnet. Dies hätte daher wahrscheinlich keinen Einfluss auf die Ergebnisse gehabt, aber es hätte für einen angenehmeren Ablauf gesorgt.

Im Verständnisteil hätten die Teilnehmer beim Lesen der Privatsphäreerklärungen nicht zeitlich eingeschränkt sein dürfen. Dies wurde hier gemacht, da ein Durchlauf sonst lange dauern könnte, jedoch ladet das eher nicht dazu ein die Fragen inhaltlich zu hinterfragen und zu verstehen. Außerdem hat die Gruppe B an der Stelle die Privatsphäreerklärungen zum ersten

[1] `https://ubuntu.com/tutorials/install-ubuntu-desktop#5-installation-setup`, zuletzt besucht am 29.03.2023

Mal gesehen. Es wäre fairer gewesen, wenn ich beiden Gruppen an der Stelle eine Einweisung gegeben hätte. Somit hätte es zwischen den beiden Gruppen Fairness gegeben unabhängig davon, ob ein Teilnehmer bereits mit den Privatsphäreerklärungen interagiert hat oder nicht.

Beim SUS hätte ich mehr Fragen aus dem Katalog verwenden sollen, da es eigentlich keinen validen Grund gibt diese nicht zu verwenden. Es hätte lediglich eine Anpassung auf den Kontext gebraucht. Dies ist auch der Grund weshalb ich in dieser Arbeit nur von einem skalierten SUS sprechen kann, da nur 3 von 10 möglichen Fragen beantwortet worden sind.

Außerdem ist durch Abschnitt 5.4 ersichtlich, dass die Teilnehmer nicht die allgemeine Bevölkerung repräsentieren, weshalb die Ergebnisse auch nicht auf die Allgemeinheit anwendbar sind, sondern lediglich auf die Gruppe, die repräsentiert wird und zwar sogenannte „digital natives“. Die Gruppe der sogenannten „digital immigrants“ ist schwach repräsentiert. Dabei wurden seitens der Teilnehmer mündlich häufig Bedenken genannt, ob ältere Personen mit den Privatsphäreerklärungen zurecht kommen.

Kapitel 7

Verwandte Arbeiten

Im folgenden werden Arbeiten, die eine ähnliche Intention haben inhaltlich zusammengefasst und mit dieser Arbeit verglichen. Außerdem werden Vor- und Nachteile der Ansätze aufgezählt und die Unterschiede aufgezählt.

Shulman et al. [43] haben in ihrer Arbeit das Konzept der Datenschutzhinweise in Form von Benachrichtigungen im Anwendungskontext eines sozialen Mediums untersucht. Die Benachrichtigungen enthalten folgende Hinweise:

- Hochgeladene Bilder können Konsequenzen mit sich ziehen.
- Auf welcher Basis Posts empfohlen werden.

Diese Benachrichtigungen können rein Text basierende Erklärungen oder Erklärungen mit Text und Bildern beinhalten. Weiterhin erscheinen diese sobald der Benutzer in der Situation ist eine Entscheidung treffen zu müssen [43].

Im Vergleich zu der hier geschaffenen Lösung, ist aus den Bildern der Benachrichtigungen ersichtlich, dass der Informationsgehalt geringer ist und der Inhalt auf Warnhinweise beschränkt ist. Dies ist auch der Grund weshalb es bei dieser Lösung für die Benutzer keine Möglichkeit gibt aktiv etwas abzulehnen oder zu akzeptieren (vgl. Abbildung 7.1).

Aufgrund des geringeren Informationsgehalts und der bildlichen Darstellung ist es möglich, dass die Lösung von Shulman et al. [43] für die Benutzer verständlicher ist.

Eine Gemeinsamkeit beider Lösungen ist, dass beide Lösungen unter der Berücksichtigung des Anwendungskontextes „Soziales Medium“ entwickelt wurden. Weiterhin werden beide Lösungen kontextuell angewendet, so dass die Benutzer die zum Kontext passenden Benachrichtigungen oder Privatsphäreerklärungen angezeigt bekommen.

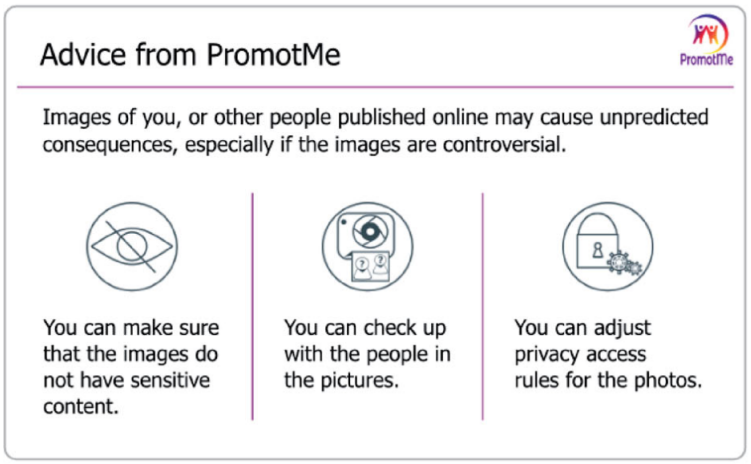

Abbildung 7.1: Beispiel der Datenschutzhinweise von Shulman et al. [43]

Brunotte et al. [10] haben in ihrer Arbeit das Konzept einer Entität, die Datenschutz-Bestimmungen visuell erklärt, untersucht. Dies geschieht in Form einer Browser-Erweiterung namens PriX. PriX untersucht Datenschutz-Bestimmungen von bereits existierenden Webseiten mithilfe eines Algorithmus zur Klassifizierung und Erkennung von Datenschutz-Bestimmungen. Dieser Algorithmus wurde mithilfe des „OPP-115 Corpus“, das ein Satz bestehend aus echten Webseiten mit Datenanmerkungen ist, entwickelt.

Anhand der gefundenen Informationen auf einer Webseite zeigt PriX den Nutzern eine bildliche Repräsentation davon, was mit ihren Daten passiert an [10].

Im Vergleich zu der hier geschaffenen Lösung, werden echte Datenschutz-Bestimmungen auf Webseiten analysiert und inhaltlich heruntergebrochen, so dass diese für den Benutzer schnell nachvollziehbarer sind, jedoch geschieht dies nicht kontextuell und muss vom Benutzer selbst hervorgerufen werden.

Beide Lösungen haben zwar einen Fokus auf die nichtfunktionale Anforderung der Erklärbarkeit gesetzt, aber die Lösungen unterscheiden sich im Inhalt und in der Intention. Während es bei kontextuellen Privatsphäreerklärungen eher darum geht, dass Benutzer selbstständig entscheiden können, ob die eine Funktionalität verwenden möchten und somit mit den Bedingungen einverstanden sind, geht es bei PriX darum den Benutzern die Datenschutz-Bestimmungen näher zu bringen. Hierbei stellen beide Lösungen keinen Ersatz für die Datenschutz-Bestimmungen dar, jedoch können diese als eine Erweiterung oder Ergänzung dieser betrachtet werden.

Bei Anwendungen für das mobile Betriebssystem Android von Google, müssen Anwendungen für das Betriebssystem eine Berechtigung für einen Hardwarezugriff seitens des Benutzers erhalten. Eine Ausnahme, die kein Hardwarezugriff darstellt, ist der Zugriff auf das Telefonbuch des Benutzers.

Hierbei haben Entwickler auch die Möglichkeit dem Nutzer zu erklären, wieso der Zugriff auf eine Hardware benötigt wird (vgl. Abbildung 7.3). Außerdem werden die benötigten Zugriffe vor der Installation (vgl. Abbildung 7.2) einer Anwendung aufgelistet, so dass der Benutzer vor der Verwendung einer Anwendung wissen kann, auf welche Hardware zugegriffen wird [1].

Neben den Anfragen bezüglich des Hardwarezugriffes, wurden ab der Android-Version 12 sogenannte „Datenschutzindikatoren“ hinzugefügt. Das sind kleine Icons, die auf der Benachrichtigungsleiste sichtbar sind sobald eine Hardware verwendet wird. Zum Beispiel wird bei der Verwendung der Kamera durch eine Anwendung ein kleines grünes Kamerasymbol angezeigt, das dem Nutzer signalisiert, dass diese gerade durch eine Anwendung in Benutzung ist. Zusätzlich ist es für den Nutzer möglich herauszufinden, welche Anwendung zuletzt Zugriff auf die jeweilige Hardware hatte (vgl. Abbildung 7.4) [2].

Zwar ähnelt das hier entwickelte Konzept dem Konzept bei Android, jedoch beschränkt sich Android auf den Hardwarezugriff und nicht auf den Zugriff von privaten Daten. Außerdem wird der Nutzer nicht darauf hingewiesen, wofür die erhobenen Daten genutzt werden können und welche Risiken bestehen.

Ähnlich zu dem Berechtigungs-System von Android ist das System in iOS von Apple. Auch hier werden die Benutzer vor der Installation einer Anwendung auf den Zugriff ihrer Daten hingewiesen (vgl. Abbildung 7.5) [3] und zusätzlich erhalten die Benutzer eine Anfrage beim ersten Start der Anwendung (vgl. Abbildung 7.6) [4].

[1] `https://developer.android.com/guide/topics/permissions/overview`, zuletzt besucht am 18.04.2023

[2] `https://source.android.com/docs/core/permissions/privacy-indicators?hl=de`, zuletzt besucht am 18.04.2023

[3] `https://developer.apple.com/app-store/user-privacy-and-data-use/`, zuletzt besucht am 18.04.2023

[4] `https://developer.apple.com/documentation/uikit/protecting_the_user_s_privacy/requesting_access_to_protected_resources`, zuletzt besucht am 18.04.2023

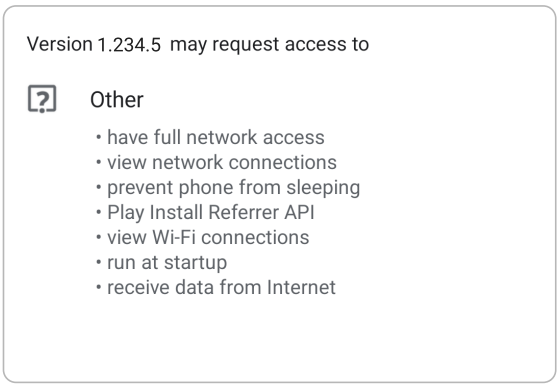

Abbildung 7.2: Auflistung von benötigten Berechtigungen vor der Installation einer Anwendung (Android) [3]

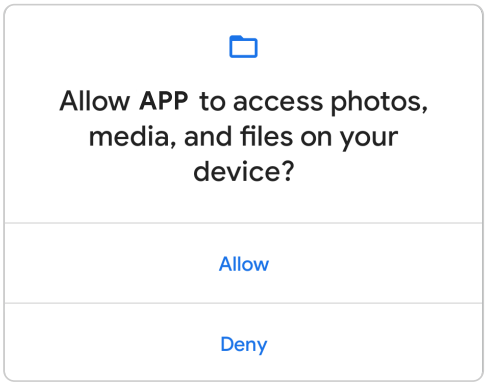

Abbildung 7.3: Anfrage für benötigten Hardwarezugriff während der Nutzung einer Anwendung (Android) [3]

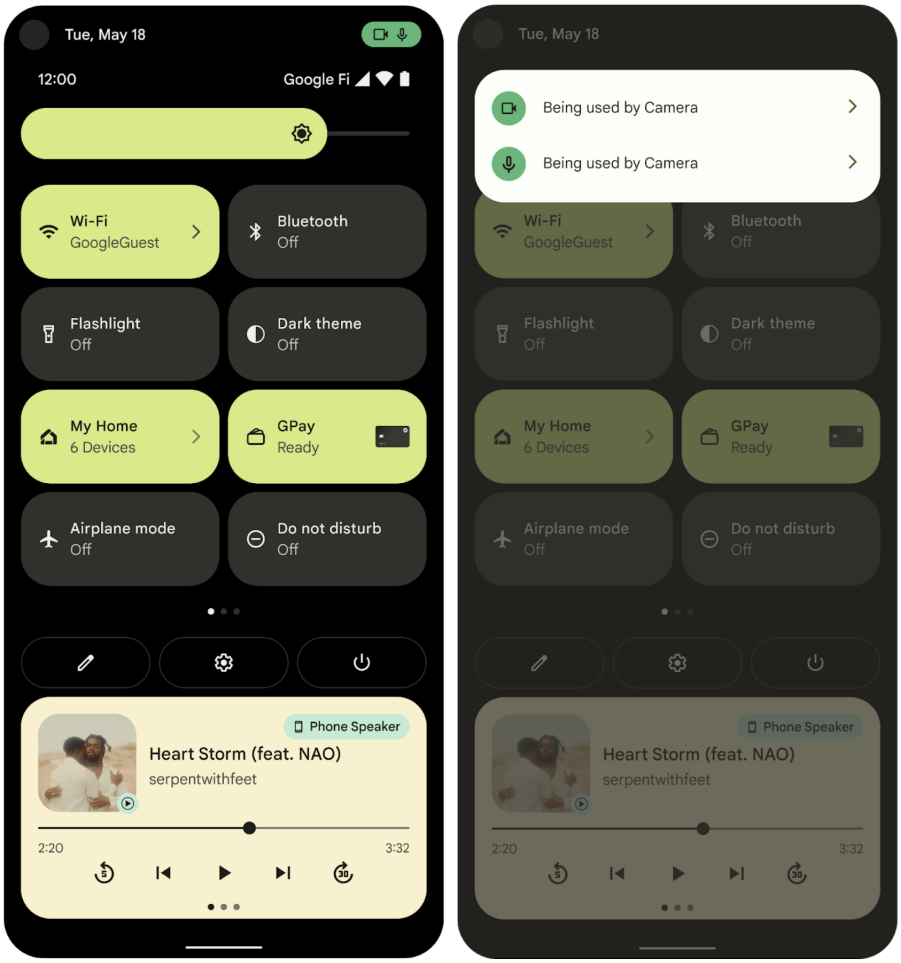

Abbildung 7.4: Datenschutzindikatoren in Android [2]

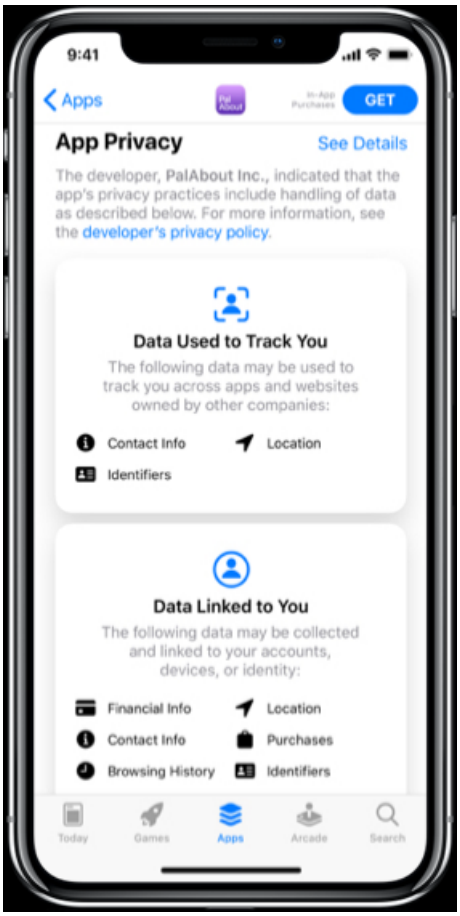

Abbildung 7.5: Auflistung von benötigten Berechtigungen vor der Installation einer Anwendung (iOS) [5]

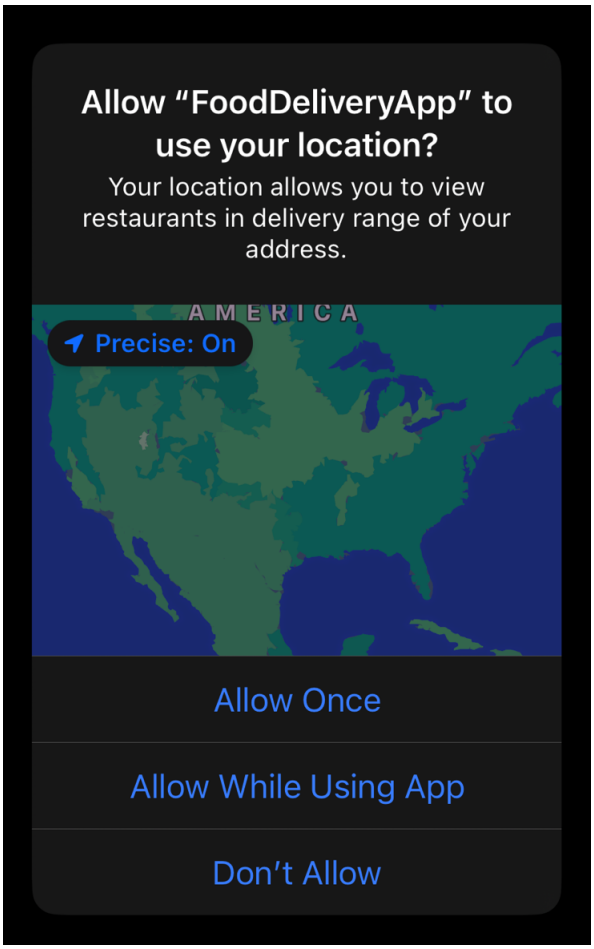

Abbildung 7.6: Anfrage für benötigten Hardwarezugriff während der Nutzung einer Anwednung (iOS) [4]

Droste [21] hat in seiner Arbeit das Konzept der Privatsphäreerklärungen untersucht und anhand eines Prototypen evaluiert. Hierbei wird im Vergleich zu dieser Arbeit das Konzept selbst näher beleuchtet und es werden andere Aspekte betrachtet. Es wird das Verständnis im Zusammenhang zur Struktur, die Zufriedenheit der Benutzer im Zusammenhang des Inhalts, der Einfluss des Bewusstseins bezüglich der Privatsphäre und die Präferenzen der Benutzer analysiert [21]. Dies stellt einen Kontrast zu dieser Arbeit dar, da diese Arbeit einen Fokus auf die Nutzbarkeit, Verständlichkeit und Angemessenheit der Privatsphäreerklärungen setzt.

Die entstandenen Prototypen ähneln sich im Aufbau der Privatsphäreerklärungen. Die feststellbaren Unterschiede sind in der Regel dadurch entstanden, dass zum einen aus den gefundenen Mängeln von Droste gelernt wurde [21] und zum anderen dadurch, dass die Privatsphäreerklärungen kontextuell in einem Anwendungskontext angewendet werden. Ein Mangel,

der z.B. häufig in der Arbeit von Droste angesprochen wird, ist das angewendete „Reverse Dark Pattern“, bei dem unter anderem das Farbschema der Buttons zum Akzeptieren bzw. Ablehnen vertauscht wurde. Dies bedutet, dass der Button zum Ablehnen dementsprechend grün ist. Dies wurde von den Studienteilnehmern kritisiert, da sie es anders herum bereits gewohnt sind, auch wenn es sich hierbei um ein Dark Pattern handelt [21]. Dieser mangel wurde in dieser Arbeit behandelt, indem die Buttons die gleiche Farbe besitzen, da dies neutral ist.

Kapitel 8

Zusammenfassung und Ausblick

Dieses Kapitel fasst die Ergebnisse und die Erkenntnisse aus den vergangenen Kapiteln zusammen. Des Weiteren werden mögliche zukünftige Projekte vorgeschlagen und diskutiert.

8.1 Zusammenfassung

Anhand der Betrachtung der Erklärbarkeit als nichtfunktionale Anforderung ist es möglich, das Bewusstsein der Nutzer bezüglich der eigenen Privatsphäre zu stärken. Dies ist für die Zukunft relevant, da das Sammeln von personenbezogenen Daten ein lukratives Geschäft ist [19] und diese Praxis somit nicht aufhören wird.

Durch die Literaturrecherche hat sich herausgestellt, dass Datenschutzbestimmungen häufig gar nicht oder nicht vollständig gelesen, geschweige denn vollständig verstanden werden. Diese Erkenntnis zeigt, dass der Austausch von personenbezogenen Daten einseitig zu Gunsten der Industrie und zu Ungunsten der Benutzer stattfindet.

Droste [21] und Brunotte [12] haben in ihren Arbeiten herausgefunden, dass Privatsphäreerklärungen zur Aufklärung der Benutzer bezüglich der Privatsphäre helfen können. Dabei wurden die Privatsphäreerklärungen konzeptionell betrachtet und in keiner Anwendung eingebunden. Somit fehlte die nähere Betrachtung der Usability.

Das Ziel dieser Arbeit war die Untersuchung der kontextuellen Privatsphäreerklärungen und deren Auswirkungen auf die Usability sobald diese im Anwendungskontext eines sozialen Mediums eingesetzt werden. Weiterhin wurde das Verständnis seitens der Benutzer bezüglich der Privatsphäreerklärungen und die Angemessenheit dieser im Kontext überprüft.

Zur Implementierung der kontextuellen Privatsphäreerklärungen wurde ein Twitter-Klon 6 verwendet, der um diese erweitert wurde.

Die Inhalte der Privatsphäreerklärungen wurden mithilfe der Nutungsbedingungen von Twitter erarbeitet und mit mithilfe der Arbeiten von Droste [21] und Brunotte [10] konzeptioniert. Weiterhin wurde bei der Konzeptionierung der Privatsphäreerklärungen auf sog. „Dark Patterns“ geachtet, so dass die Benutzer eine möglichst unbeeinflusste Entscheidung treffen können.

Die durchgeführte Nutzerstudie zeigt, dass ein negativer Einfluss auf die Usability bezüglich der Gesamtdauer durch die Privatsphäreerklärungen besteht und die Teilnehmer diese als störend wahrgenommen haben. Allerdings haben die Teilnehmer auch Vorteile in diesem System erkannt. Durch den T-Test für 2 unabhängige Mittelwerte konnte statistische Signifikanz bezüglich der Gesamtdauer der Gruppe A (Prototyp mit Privatsphäreerklärungen) und der Gesamtdauer der Gruppe B (Prototyp ohne Privatsphäreerklärungen) nachgewiesen werden.

Außerdem konnte gezeigt werden, dass die Teilnehmer die Privatsphäreerklärungen inhaltlich als verständlich einstufen. Weiterhin konnten die Teilnehmer inhaltliche Fragen bei gewählten Privatsphäreerklärungen häufig korrekt beantworten. Einzig die Frage, die mit einem Usability-Problem einhergeht, wurde häufig falsch beantwortet. Dies betrifft die Frage bezüglich der Übertragung der Nutzerdaten an GIPHY. An der Stelle haben die meisten Teilnehmer das Fragezeichen-Symbol und die Interaktion damit falsch interpretiert. Durch die anderen Fragen ließ sich dadurch zeigen, dass es nicht am Inhalt oder der verwendeten Sprache lag, sondern an der Usability an der spezifischen Stelle.

Bezüglich der Relevanz und der Angemessenheit der Privatsphäreerklärungen haben Teilnehmer häufig die Rückmeldung gegeben, dass sie Privatsphäreerklärungen, bei denen es sich nicht direkt um persönliche Daten handelt (z.B. GIPHY) als weniger relevant ansehen als solche, bei denen es sich um private Daten handelt (z.B. Kamera).

8.2 Ausblick

Da der einseitige Handel mit persönlichen Daten alltäglich ist und es keine Aussicht auf wesentliche Änderungen gibt, ist eine Lösung für dieses Problem notwendig. Dabei kann die hier geschaffene Lösung Unternehmen dabei helfen an Vertrauenswürdigkeit zu gewinnen und mit den Benutzer transparent zu kommunizieren. Es gibt dennoch Stellen an denen weiter gearbeitet werden muss:

- **Standardisierung**
  Standards können Unternehmen dabei helfen das Konzept leichter einzuführen [28]. Weiterhin würde dies die Hemmschwelle senken, da bereits eine Art Muster vorhanden wäre. Aus der Sicht der Benutzer ist ein Standard auch vorteilhaft, da die Privatsphäreerklärungen überall

ähnlich strukturiert wären und die Benutzer sich dadurch leicht an die Bedienung und den Inhalt gewöhnen können, so dass Inhalte, die für die Benutzer von Relevanz sind, schneller aufgefunden werden können.

- **Verwendung in anderen Anwendungskontexten**
  In dieser Arbeit wurde lediglich der Anwendungskontext eines sozialen Mediums näher betrachtet. Jedoch gibt es weitere Arten von Anwendungen, in denen Benutzer ihre Daten preisgeben wie z.B. bei E-Commerce Seiten. Dort können die Händler unter anderem überprüfen welche Gegenstände der Benutzer gekauft hat und daraus Interessen des Benutzers ableiten. Anhand der gefundenen Interessen, können Benutzer Empfehlungen für Gegenstände erhalten. Bei solch einer Plattform wäre es wichtig mit dem Benutzer zu kommunizieren worauf die Empfehlungen basieren und wodurch diese sich beeinflussen lassen. Außerdem ist es wichtig herauszufinden, ob die Implementierung von Privatsphäreerklärungen bei jeder Art von Software möglich wäre, ohne dass es für den Benutzer zu aufdringlich wirkt.

- **Größere Studie durch Einbindung in berühmte Plattformen**
  Das Konzept wurde im Rahmen einer Nutzerstudie getestet, aber die Daten können dadurch verfälscht sein, da die Teilnehmer in einer Studie eher dazu neigen könnten die mögliche Hypothese zu hinterfragen, wodurch sie in unterschiedliche Rollen wie z.B. die des „good subject“ geraten können [31]. Dementsprechend wäre die Implementation von Privatsphäreerklärungen bei bereits existierenden Plattformen interessant. Die Benutzer der entsprechenden Plattform würden bei einer Befragung bezüglich einer Rückmeldung dann unter keinem Einfluss stehen und daraus resultieren dann auch ehrliche Antworten, sofern die Teilnahme an einer Befragung auf freiwilliger Basis geschieht. Außerdem entstehen dadurch mehr Daten aus verschiedenen Bevölkerungs- und Altersgruppen, was zu besser generalisierbaren Aussagen führen kann.

- **Einarbeitung der Vorschläge seitens der Teilnehmer**

  Seitens der Teilnehmer wurden Vorschläge geäußert, um die Bedienung der Privatsphäreerklärungen unter anderem zu erleichtern. Diese Vorschläge wurden in Abschnitt 5.3 aufgelistet und es wurden seitens der Teilnehmer Probleme bezüglich der Usability angesprochen. Darunter fällt die Navigation innerhalb der Privatsphäreerklärungen, die in dem hier erstellten Prototypen durch eine Navigation durch die Seiten erfolgt und laut einigen Teilnehmer nicht existieren beziehungsweise durch eine Scrollleiste ersetzt werden sollte. Weiterhin haben die Teilnehmer Bedenken bezüglich der versteckten Information hinter dem Fragezeichen-Symbol ausgesprochen und erwartet, dass die hinterlegte Information offen in der Privatsphäreerklärung verfügbar und leicht

sichtbar ist. Zumindest die Einarbeitung dieser beiden Kritikpunkte wäre in Zukunft wichtig, da diese Stellen einen negativen Einfluss auf die Usability haben.

Anhang A

Inhalte auf dem USB-Stick

Der USB-Stick, der mit dieser Arbeit eingereicht wird enthält folgenden Inhalt:

- Das LaTeX-Archiv, das verwendet wurde, um dieses Dokument zu erstellen
- Eine PDF-Version dieses Dokuments
- Die Jupyter-Notebook Datei zur Erstellung der Graphen zur Evaluierung
- Die Ergebnisse der Nutzerstudie in Form einer CSV-Datei
- Die Entwürfe des Papier-Prototypen
- Die finalen Prototypen mitsamt einer Anleitung zum Starten dieser
- Die Videoprotokolle aus der Nutzerstudie
- Die schriftlichen Protokolle aus der Nutzerstudie
- Die in der Arbeit verwendete Literatur

Literaturverzeichnis

[1] M. Alenezi. Software architecture quality measurement stability and understandability. *International Journal of Advanced Computer Science and Applications*, 7(7), 2016.

[2] Android Developers. Datenschutzindikatoren. `https://source.android.com/docs/core/permissions/privacy-indicators?hl=de`, Sep 2022. zuletzt besucht am 18.04.2023.

[3] Android Developers. Permissions on android. `https://developer.android.com/guide/topics/permissions/overview`, Apr 2023. zuletzt besucht am 18.04.2023.

[4] Apple Developers. Requesting access to protected resources. `https://developer.apple.com/documentation/uikit/protecting_the_user_s_privacy/requesting_access_to_protected_resources`, 2023. zuletzt besucht am 18.04.2023.

[5] Apple Developers. User privacy and data use. `https://developer.apple.com/app-store/user-privacy-and-data-use/`, 2023. zuletzt besucht am 18.04.2023.

[6] A. Bangor, P. Kortum, and J. Miller. Determining what individual sus scores mean: Adding an adjective rating scale. *Journal of usability studies*, 4(3):114–123, 2009.

[7] S. B. Barnes. A privacy paradox: Social networking in the united states. *First Monday*, 11(9), Sep. 2006.

[8] J. Brooke. Sus: A 'quick and dirty' usability scale. *Usability Evaluation In Industry*, page 207–212, 1996.

[9] J. Brooke. Sus: a retrospective. *Journal of usability studies*, 8(2):29–40, 2013.

[10] W. Brunotte, L. Chazette, L. Kohler, J. Klunder, and K. Schneider. What About My Privacy? Helping Users Understand Online Privacy

Policies. In *Proceedings of the International Conference on Software and System Processes and International Conference on Global Software Engineering*, ICSSP'22, page 56–65, New York, NY, USA, 2022. Association for Computing Machinery.

[11] W. Brunotte, L. Chazette, and K. Korte. Can Explanations Support Privacy Awareness? A Research Roadmap. In *2021 IEEE 29th International Requirements Engineering Conference Workshops (REW)*, pages 176–180, 2021.

[12] W. Brunotte, A. Specht, L. Chazette, and K. Schneider. Privacy Explanations – A Means to End-User Trust. *Journal of Systems and Software*, 195:111545, 2023.

[13] L. Burlamaqui and A. Dong. The use and misuse of the concept of affordance. In J. S. Gero and S. Hanna, editors, *Design Computing and Cognition '14*, pages 295–311, Cham, 2015. Springer International Publishing.

[14] J. P. Carrascal, C. Riederer, V. Erramilli, M. Cherubini, and R. de Oliveira. Your browsing behavior for a big mac: Economics of personal information online. In *Proceedings of the 22nd International Conference on World Wide Web*, WWW '13, page 189–200, New York, NY, USA, 2013. Association for Computing Machinery.

[15] L. Chazette. *Requirements Engineering for Explainable Systems*. PhD thesis, Leibniz Universität Hannover, 2023.

[16] L. Chazette, W. Brunotte, and T. Speith. Exploring Explainability: A Definition, a Model, and a Knowledge Catalogue. In *2021 IEEE 29th International Requirements Engineering Conference (RE)*, pages 197–208, 2021.

[17] L. Chazette and K. Schneider. Explainability as a non-functional requirement: challenges and recommendations. *Requirements Engineering*, 25(4):493–514, Dec 2020.

[18] M. Chromik, M. Eiband, S. T. Völkel, and D. Buschek. Dark patterns of explainability, transparency, and user control for intelligent systems. In *IUI workshops*, volume 2327, 2019.

[19] M. Crain. The limits of transparency: Data brokers and commodification. *New Media & Society*, 20(1):88–104, 2018.

[20] A. Curley, D. O'Sullivan, D. Gordon, B. Tierney, and I. Stavrakakis. The design of a framework for the detection of web-based dark patterns. 2021.

[21] J. R. C. Droste. Development of a Concept for Privacy Explanations and its Prototypical Evaluation. Master's thesis, Leibniz Universität Hannover, Fachgebiet Software Engineering, Hannover, Germany, April 2022.

[22] J. S. Dumas, J. S. Dumas, and J. Redish. *A practical guide to usability testing*. Intellect books, 1999.

[23] Europäisches Parlament. General data protection regulation (gdpr). `https://gdpr-info.eu/`, Sep 2022. zuletzt besucht am 18.04.2023.

[24] T. Grossman, G. Fitzmaurice, and R. Attar. A survey of software learnability: metrics, methodologies and guidelines. In *Proceedings of the sigchi conference on human factors in computing systems*, pages 649–658, 2009.

[25] S. Kokolakis. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, 64:122–134, 2017.

[26] L. Kästner, M. Langer, V. Lazar, A. Schomäcker, T. Speith, and S. Sterz. On the relation of trust and explainability: Why to engineer for trustworthiness. In *2021 IEEE 29th International Requirements Engineering Conference Workshops (REW)*, pages 169–175, 2021.

[27] J. C. S. d. P. Leite and C. Cappelli. Software transparency. *Business & Information Systems Engineering*, 2(3):127–139, Jun 2010.

[28] J. Y.-C. Liu, V. J. Chen, C.-L. Chan, and T. Lie. The impact of software process standardization on software flexibility and project management performance: Control theory perspective. *Information and Software Technology*, 50(9):889–896, 2008.

[29] S. Möller. *Quality Engineering: Qualität kommunikationstechnischer Systeme*. Springer-Verlag, 2017.

[30] J. T. Mordkoff. The assumption(s) of normality. `http://www2.psychology.uiowa.edu/faculty/mordkoff/GradStats/part%201/I.07%20normal.pdf`, 2016. zuletzt besucht am 18.04.2023.

[31] A. L. Nichols and J. K. Maner. The good-subject effect: Investigating participant demand characteristics. *The Journal of General Psychology*, 135(2):151–166, 2008. PMID: 18507315.

[32] J. Nielsen. *Usability engineering*. Morgan Kaufmann, 1994.

[33] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal. 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*, CHI '20, page 1–13, New York, NY, USA, 2020. Association for Computing Machinery.

[34] I. Nunes and D. Jannach. A systematic review and taxonomy of explanations in decision support and recommender systems. *User Modeling and User-Adapted Interaction*, 27(3):393–444, Dec 2017.

[35] J. A. Obar and A. Oeldorf-Hirsch. The biggest lie on the internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 23(1):128–147, 2020.

[36] K. Olmstead and A. Smith. Americans and cybersecurity. *Pew Research Center*, 26(311–27), 2017.

[37] I. Pentina, L. Zhang, H. Bata, and Y. Chen. Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior*, 65:409–419, 2016.

[38] L. Rainie. Americans' complicated feelings about social media in an era of privacy concerns. `https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/`, Mar 2018. zuletzt besucht am 18.04.2023.

[39] J. Sauro and J. R. Lewis. Average task times in usability tests: What to report? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, page 2347–2350, New York, NY, USA, 2010. Association for Computing Machinery.

[40] J. Sauro and J. R. Lewis. Chapter 5 - is there a statistical difference between designs? In J. Sauro and J. R. Lewis, editors, *Quantifying the User Experience (Second Edition)*, pages 61–102. Morgan Kaufmann, Boston, second edition edition, 2016.

[41] M. Sebastian. *Usability Engineering*, page 64–66. Springer, 2017.

[42] A. Seffah, M. Donyaee, R. B. Kline, and H. K. Padda. Usability measurement and metrics: A consolidated model. *Software quality journal*, 14:159–178, 2006.

[43] Y. Shulman, A. Kitkowska, and J. Meyer. Informing users: Effects of notification properties and user characteristics on sharing attitudes. *International Journal of Human–Computer Interaction*, 0(0):1–29, 2022.

[44] A. E. Waldman. Privacy, notice, and design. *Stan. Tech. L. Rev.*, 21:74, 2018.

[45] C. Wohlin, P. Runeson, M. Host, M. C. Ohlsson, B. Regnell, and A. Wesslen. *Experimentation in software engineering: an introduction.* Springer-Verlag New York, New York, 2012.