Daten informiert teilen: Die Möglichkeiten von Differential Privacy für die Gesellschaft nutzbar machen[1]

Daniel Franzen, Claudia Müller-Birn

Zusammenfassung

Die Nutzung personenbezogener Daten, beispielsweise Mobilitätsdaten, ist für die Bewältigung aktueller gesellschaftlicher Herausforderungen von großer Bedeutung. Allerdings können die benötigten Daten auch einen Eingriff in die Privatsphäre der Datengebenden bedeuten. Die Einschätzung, ob ein Privatsphärenrisiko verhältnismäßig ist, hängt unter anderem vom verwendeten Anonymisierungsverfahren und dem individuellen Privatsphärebedürfnis ab und sollte, im Rahmen einer sogenannten informierten Entscheidung, von den Datengebenden getroffen werden. Wir schlagen daher „Privacy Decision User Interfaces" vor, in denen Datengebenden verständlich kommuniziert wird, wie das verwendete Anonymisierungsverfahren das Privatsphärenrisiko beeinflusst.

Ein solches Anonymisierungsverfahren ist Differential Privacy (DP), das besonders geeignet ist, informierte Entscheidungen zu unterstützen: Im Vergleich zu anderen Verfahren erlaubt DP eine feinere Kontrolle des Kompromisses zwischen der Genauigkeit der weitergebenen Daten (die verrauscht werden) und dem damit verbundenen Privatsphärenrisiko. Allerdings ist die Vermittlung dieses Kompromisses an bisher wenig erforscht. Dadurch wird das Potenzial von DP, informierte Entscheidungen für den Einzelnen aber auch für die Gesellschaft unter Wahrung der Privatsphäre zu unterstützen, bisher zu wenig genutzt.

In unserem Beitrag geben wir einen Überblick über die Herausforderungen und bisherigen Erkenntnisse zur Kommunikation von DP, berichten über unsere Ergebnisse aus zwei empirischen Studien zur Kommunikation des Privatsphäreschutzes durch den Einsatz von *Privacy Decision User*

1 Der vorliegende Beitrag entstand im Rahmen des Verbundprojekts „freemove - Transdisziplinäre Erforschung der Datenschutz-bewussten Verfügbarmachung von Bewegungsdaten für nachhaltige urbane Mobilität", das seit 2021 vom Bundesministerium für Bildung und Forschung gefördert wird (Förderkennzeichen: 01UV2090B).

Interfaces und diskutieren, was diese Ergebnisse für informierte Entscheidungen über die Weitergabe von personenbezogenen Daten bedeuten.

1. Der Wertekonflikt zwischen Genauigkeit und Privatsphäre in Datensätzen

Um die gegenwärtigen Herausforderungen unserer Gesellschaft zu bewältigen, werden Daten benötigt, die die Bedürfnisse der Gesellschaft genau widerspiegeln. Beispielsweise sind für nachhaltige Mobilitätskonzepte Bewegungsdaten erforderlich, die Aufschluss darüber geben, wie Bürger:innen die bestehenden Angebote nutzen und an welchen Stellen Engpässe bestehen. Die Erhebung und Nutzung solcher Daten unterliegt allerdings häufig einem *Wertekonflikt*. Ein solcher Wertekonflikt bezeichnet eine Situation, in der es einen Widerspruch zwischen konkurrierenden oder unvereinbaren Interessen oder Zielen gibt, die von Individuen oder Gruppen als wichtig für ihr Leben empfunden werden (Friedman u. a. 2019). In der Datenerhebung und -nutzung steht der Bedarf an möglichst genauen Daten, um einen Mehrwert für das Gemeinwohl zu erzeugen, dem Bedürfnis des Einzelnen nach Schutz der Privatsphäre gegenüber, da eine solche Datensammlung häufig auch sensible Informationen enthält. Bewegungsdaten können beispielsweise Aufschluss über den Wohn- und Arbeitsort von Individuen geben. Der Vergleich von Bewegungsdaten Einzelner mit denen anderer Personen erlaubt potenziell die Identifikation von sozialen Beziehungen und der Abgleich mit markanten Orten erlaubt Rückschlüsse auf Hobbys, religiöse oder politische Einstellungen, sexuelle Orientierung, sowie die medizinische Verfassung.

Zum Schutz der Datengebenden, aber auch um das Vertrauen von Datengebenden in öffentliche Datensammlungen zu fördern, sollte deshalb dieses Privatsphärerisiko einer Verletzung der Privatsphäre mit effektiven Verfahren reduziert werden. Eine „naive" Anonymisierung, wie das Entfernen von Namen und ähnlichen eindeutigen Identifikatoren, reicht im Allgemeinen nicht aus, da häufig aus vermeintlich nicht personenbezogenen Daten in einem Datensatz auf die Identität oder sensible Informationen der Datengebenden geschlossen werden kann (de Montoje u. a. 2013). Aus diesem Grund modifizieren fortgeschrittene Anonymisierungsverfahren[2] die Daten zusätzlich so, dass das Risiko eines solchen Privatsphäreverlusts verringert wird.

2 Als Anonymisierung bezeichnen wir hier nicht nur das Entfernen von Identifikatoren (des Personenbezugs), sondern auch die Verringerung des Risikos, dass selbst ohne

Die rechtliche Situation in Bezug auf personenbezogene oder anonymisierte Daten ist in der Datenschutz-Grundverordnung (DSGVO) geregelt: Personenbezogene Daten unterliegen strengen Anforderungen und müssen angemessen geschützt werden, während die Verwendung „anonymisierter Daten" durch die DSGVO nicht grundsätzlich eingeschränkt wird. Diese binäre Einteilung spiegelt jedoch die Bandbreite der technischen Anonymisierungsmethoden nur unzureichend wider. Auch fortgeschrittene Anonymisierungsmethoden können eine Verletzung der Privatsphäre nicht gänzlich ausschließen, sondern lediglich das Risiko einer solchen Verletzung reduzieren. Das Schutzniveau, also wie stark dieses Risiko reduziert wird, bewegt sich auf einem kontinuierlichen Spektrum und hängt von der gewählten Methode und von den gewählten Parametern der Methode ab. Ein höheres Schutzniveau („bessere" Privatsphäre) geht dabei auch mit einem höheren Verlust an Datengenauigkeit einher.

Wir erweitern daher die binäre Sichtweise auf Anonymität im Sinne der DSGVO um dieses Kontinuum und widmen uns aus der menschzentrierten Perspektive (Human-Centered Design, Kling u. a. 1998 und Moggridge 2007) dem Wertekonflikt zwischen Datengenauigkeit und Schutz der Privatsphäre. Uns interessiert, wie das Schutzniveau von Anonymisierungsmethoden mit dem individuellen Bedürfnis der Datengebenden nach Privatsphäre in Einklang gebracht werden kann, um individuelle Mobilitätsdaten für die Gesellschaft wertebasiert nutzbar zu machen.

1.1 Informierte Entscheidung zum Teilen von persönlichen Daten

Moderne Anonymisierungsmethoden stellen, analog zu dem anfangs angesprochenen Wertekonflikt, einen Kompromiss zwischen Datengenauigkeit und Privatsphäreschutz dar: Um die Privatsphäre stärker zu schützen, müssen Daten stärker modifiziert werden, was sich jedoch negativ auf die Genauigkeit und damit auch auf den Nutzen der Daten für die Analyse auswirkt. Verfahren wie beispielsweise k-Anonymität erreichen dies durch die Entfernung einzelner Datensätze (Ausreißer) oder durch eine Verallgemeinerung der Daten (Alter: „20-25" statt „23"). DP hingegen modifiziert die Daten durch einen Zufallsprozess (vgl. Abschnitt 2.1). Der Parameter ε von DP erlaubt es den Kompromiss zwischen Schutzniveau und Datenge-

Identifikatoren sensible Informationen aus den gesammelten Daten abgeleitet werden können.

nauigkeit präzise einzustellen. Dabei gilt: Je höher der Wert für den Parameter ε gewählt wird, desto weniger weichen die modifizierten Daten von den tatsächlichen Daten ab. Das resultiert in höherer Datengenauigkeit, allerdings gleichzeitig in einem höheren Risiko für die Privatsphäre. Das angemessene Schutzniveau (d. h. der geeignete Wert für den Parameter ε) ist vom jeweiligen Anwendungsfall abhängig, unter anderem davon, welche Daten von welchen Datengebenden erhoben werden. Wird der Parameter ε (Schutzniveau) zu niedrig gewählt vermittelt DP als fortgeschrittene Anonymisierungsmethode ein hohes wahrgenommenes Schutzniveau, jedoch besteht eine hohe Wahrscheinlichkeit, dass Angreifende auf die sensiblen Daten der Datengebenden schließen können. Mobilitätsdaten sind für eine solche Verletzung der Privatsphäre in besonderem Maße gefährdet, da hier typischerweise die einzelnen Messpunkte mit Zeitstempeln versehen und in Trajektorien verbunden sind. Das bietet zahlreiche Gelegenheiten die Identitäten von Personen aus den vermeintlich anonymisierten Daten wiederherzustellen.

Da es bisher an einer rechtlichen Regelung oder allgemein akzeptierten Standards zum erforderlichen Schutzniveau in unterschiedlichen Kontexten fehlt (Dwork u. a. 2019), ist eine gängige Vorgehensweise, ein angemessenes Schutzniveau zu finden, die sogenannte „informierte Entscheidung“: Datengebende sollen alle nötigen Informationen bekommen und auf dieser Grundlage selbst entscheiden, ob das gewählte Schutzniveau dem Zweck der Erhebung angemessen ist oder ob ein höheres Schutzniveau gegeben sein müsste, um dem Privatsphärebedürfnis zu entsprechen. Unter einer informierten Entscheidung verstehen wir gemäß der Definition von Bekker u. a. eine Wahl, die (1) unter Berücksichtigung aller relevanten Informationen und (2) in Übereinstimmung mit den individuellen Überzeugungen getroffen wird (Bekker u. a. 1999). Von entscheidender Bedeutung ist hierbei, dass die wichtigen Informationen in einer verständlichen Art und Weise zur Verfügung gestellt werden, sodass diese Informationen von den Datengebenden in die Entscheidung einbezogen werden können. Die technischen Details von DP sind allerdings zu kompliziert, um sie für Laien verständlich auszudrücken und selbst die Bedeutung des Parameters ε ist schwer zu kommunizieren. Um den Privatsphäreschutz verständlicher zu machen, kann ε allerdings als ein Privatsphärenrisiko formuliert werden: „Wie wahrscheinlich ist es, dass aus den Daten korrekte Informationen über mich abgeleitet werden können?“ Das Konzept des „Privatsphärerisikos“ ist in der allgemeinen Bevölkerung noch nicht geläufig, aber Risiken im Allgemeinen sind aus anderen Kontexten wie Wettervorhersagen, Glücksspiel

oder der Medizin bekannt. Das Forschungsgebiet der Privacy Decision User Interfaces überträgt die Erkenntnisse zur Risikokommunikation aus diesen Kontexten auf die Privatsphäre. Ziel ist es, eine informierte Entscheidung für oder gegen das Teilen von Daten zu unterstützen.

1.2 Unser Beitrag

Im Rahmen unserer Forschungsarbeit befassen wir uns mit der folgenden übergreifenden Forschungsfrage: „Wie kann die informierte Entscheidung von Laien bei der Nutzung von Differential Privacy mittels Privacy Decision User Interfaces (PD-UIs) effektiv unterstützt werden?“ Nach einer kurzen Einführung zu den Eigenschaften von DP (Kap. 2), beschreiben wir das Design unserer Interfaces und unserer Studien (Kap. 3). Anschließend präsentieren wir die Ergebnisse der Untersuchungen dar(Kap. 4) und diskutieren auf Basis dieser Ergebnisse verschiedene Konsequenzen und Vorgehensweisen für den Einsatz von DP zum Nutzen der Gesellschaft (Kap. 5).

2. Das Potenzial und die Herausforderungen von DP

Der Privatsphäreschutz, der durch DP erreicht werden kann, birgt ein großes Potenzial für informierte Entscheidungen. Allerdings sind noch einige Herausforderungen zu bewältigen, bevor DP dieses Potenzial vollständig entfalten kann. Das folgende Kapitel beleuchtet diese Dualität aus Potenzial und Herausforderungen.

2.1 Differential Privacy und die Vorteile gegenüber anderen Anonymisierungsverfahren

Datensätze, die von urbanen Mobilitäts-Dienstleistenden oder öffentlichen Nahverkehrsanbietenden, aber auch von Citizen Science-Projekten gesammelt werden, können der Gesellschaft helfen, bedarfsgesteuerte Lösungen zu finden. Um bei der Datennutzung die Privatsphäre der Datengebenden zu schützen, werden Daten mit unterschiedlichen Verfahren anonymisiert.

Naive Maßnahmen, wie das Entfernen eindeutiger Identifikatoren (z.B. Namen), sind nicht ausreichend, um die Privatsphäre der Datengebenden

effektiv zu schützen. Der Bezug zu Individuen kann oft leicht wiederhergestellt werden, indem die Daten mit öffentlich verfügbaren Datenquellen, wie beispielsweise Zensusdaten, verknüpft werden (Douriez u. a. 2016, Narayanan u. a. 2008). Gerade bei Bewegungsdaten hat eine Studie gezeigt, dass schon die Kenntnis von zwei Punkten mit Aufenthaltsort und -zeit einer Person ausreicht, um 50% aller Individuen in einem typischen Datensatz eindeutig zu identifizieren (de Montoje u. a. 2013). Selbst ohne eine solche Identifikation könnten sensible Information ermittelt werden. Wenn beispielsweise die Menge aller möglichen Taxifahrten, die eine Zielperson in einem Zeitraum durchgeführt haben könnte, alle an einem sensiblen Ort enden, kann geschlossen werden, dass die Zielperson diesen Ort aufgesucht hat ohne ihre exakte Taxifahrt zu kennen. Daher sind gerade bei Bewegungsdaten effektivere Schutzverfahren nötig.

Zusätzlich zur Entfernung von Identifikatoren modifizieren fortgeschrittene Anonymisierungsverfahren, wie beispielsweise k-Anonymität (Sweeney 2002), die Daten auf gezielte Art und Weise um eine Re-identifikation oder das Lernen einer sensiblen Information zu erschweren. Je mehr die Daten verändert werden, desto stärker ist der Privatsphäreschutz, aber desto ungenauer werden die Daten. Allerdings erlauben auch diese fortgeschrittenen Verfahren keine differenzierten Aussagen zum Schutz der Privatsphäre, beispielsweise hinsichtlich der Wahrscheinlichkeit, dass sensible Informationen aus den Daten erschlossen werden können. Stattdessen werden die Daten nach Anwendung des Anonymisierungsverfahren typischerweise als anonym angenommen. Falls jedoch ein neuer Datensatz gefunden wird, der durch einen Abgleich die Re-Identifikation einer Person ermöglicht, ist der Schutz plötzlich sehr gering. Folglich können Datengebenden lediglich sehr ungenaue Angaben zur Höhe oder Qualität des Schutzes der Privatsphäre kommuniziert werden.

Eine mögliche Lösung könnte DP darstellen. DP wurde als eine mathematische Anonymisierungs-Eigenschaft definiert (Dwork 2006) und kann durch verschiedene Algorithmen erreicht werden (Dwork 2006, Kairouz u. a. 2015, Wang u. a. 2016)[3]. Anonymisierungsverfahren, die die DP-Eigenschaft erfüllen, garantieren exakte Obergrenzen für das Privatsphärenrisiko

3 Die mathematische Definition und die technische Funktionsweise von Differential Privacy wird an dieser Stelle aus Platzgründen nicht im Detail vorgestellt. Im Rest des Beitrags reicht es zu verstehen, dass mit dem Parameter ε der Kompromiss zwischen Genauigkeit der Daten und dem Privatsphäreschutz eingestellt werden kann. Für eine einfache Beschreibung der Arbeitsweise von DP, verweisen wir auf unsere Veröffentlichung (Franzen u. a. 2022).

der Datengebenden. Die DP-Garantie lässt sich vereinfacht wie folgt beschrieben: „Wenn die DP-geschützten Daten weitergegeben werden, dann steigt die Wahrscheinlichkeit, dass jemand Informationen erraten kann, höchstens um diesen Faktor: X". Die Höhe des Faktors kann von den Datensammelnden über den Parameter ε exakt justiert werden, um den Kompromiss zwischen der Genauigkeit der Daten und dem Schutz der Privatsphäre für den jeweiligen Anwendungsfall zu optimieren.

Anonymisierungsverfahren, wie auch DP, nutzen ein Angriffsmodell um zu beschreiben, welcher Privatsphäreschutz erreicht wird. Das Angriffsmodell beschreibt, welches zusätzliche Wissen und welche Fähigkeiten hypothetische Angreifende haben müssen, um sensible Informationen über eine Zielperson aus den Daten zu lernen. Im Unterschied zu allen anderen Anonymisierungsverfahren nimmt das Angriffsmodell von DP an, dass Angreifende bereits alle Informationen außer der sensiblen Information über die Zielperson kennen. Da die Schutzgarantie von DP auf dieser Grundlage gegeben wird, behält sie auch mit der Veröffentlichung von weiteren zukünftigen Datensätzen ihre Gültigkeit. Des Weiteren nimmt DP an, dass Angreifenden stets eine fundierte Vermutung über die sensible Information der Zielperson möglich ist, welche mit einer gewissen Wahrscheinlichkeit korrekt ist. Diese Wahrscheinlichkeit beträgt 100 %, wenn die Information zweifelsfrei aus anderen Quellen verfügbar ist. Aber selbst ohne nützliche Hintergrundinformationen, können Angreifende beispielsweise Ja/Nein-Attribute (wie eine medizinische Diagnose) über einen einfachen Münzwurf mit einer Wahrscheinlichkeit von 50 % korrekt raten. Basierend auf dem Konzept der Wahrscheinlichkeit der Vermutung, modifiziert DP die Daten so, dass sich die Wahrscheinlichkeit der Korrektheit der Vermutung durch die neue Datenweitergabe höchstens um einen bestimmten Faktor (abhängig von dem Parameter ε) vergrößern kann. Der Parameter ε stellt damit den Kompromiss von DP zwischen Privatsphäreschutz und Genauigkeit der Daten dar. Je kleiner der Parameter ε gewählt wird, desto kleiner wird dieser Faktor und desto weniger können Angreifende über die Zielperson herausfinden, aber gleichzeitig verringert sich die Genauigkeit der Daten für die Auswertung.[4]

4 Die Definition und die Funktionsweise von Differential Privacy wird an dieser Stelle aus Platzgründen nicht im Detail vorgestellt. Im Rest des Beitrags reicht es zu verstehen, dass mit dem Parameter ε der Kompromiss zwischen Genauigkeit der Daten und dem Privatsphäreschutz eingestellt werden kann. Für eine einfache Beschreibung der Arbeitsweise von DP, verweisen wir auf unsere Veröffentlichung (Franzen u. a. 2022).

Dieses besondere Angriffsmodell von DP erlaubt es, eine numerische Grenze für das Privatsphärenrisiko zu garantieren, statt lediglich eine ungenaue Versicherung anzugeben, dass „fast kein Risiko" besteht. Da bei DP laut Annahme Angreifende bereits über das maximale Wissen verfügen, ist der Privatsphäreschutz auch nicht davon abhängig, welche Datensätze in der Zukunft verfügbar werden (im Gegensatz zu Verfahren wie k-Anonymität). DP ermöglicht somit eine Kommunikation des genauen Risikos für die Privatsphäre an Datengebende und kann damit eine Grundlage für eine informierte Entscheidung bereitstellen.

2.2 Die Herausforderung von Differential Privacy

DP wird bereits in unterschiedlichen Datenerhebungen eingesetzt, beispielsweise von Microsoft, Apple und Google (Domingo-Ferrer u. a. 2021) oder von der U.S. Zensusbehörde (Kenny u. a. 2021). Allerdings ist die Angabe, dass DP für eine Datensammlung genutzt wird, alleine nicht aussagekräftig. Der Schutz für die Privatsphäre ist *maßgeblich abhängig von dem Parameter ε*. Mit sinnvoll kleinen ε-Werten stellt DP einen guten Privatsphäreschutz dar, aber größere Werte können unter Umständen keinen aussagekräftigen Schutz der sensiblen Daten gewährleisten. Ohne Angabe des Parameters ist es den Datengebenden somit nicht möglich, den Schutz ihrer Daten einzuschätzen (Dwork u. a. 2019).

Die Kommunikation des Privatsphärenrisikos von DP ist mit zwei Herausforderungen konfrontiert: einerseits die Komplexität von DP (Wie erreicht DP den Schutz?) und andererseits die Komplexität von Risikokommunikation (Was bedeutet ein Risiko von 34% und wie kann es verständlich erklärt werden?). In Anbetracht dieser Komplexität könnte seitens der Datensammelnden die Befürchtung bestehen, dass eine leichtfertige Erwähnung des „Risikos" Datengebende von der Weitergabe ihrer Daten abschrecken könnte. Erschwerend kommt hinzu, dass Risikokommunikation kontextabhängig ist, d. h. die Effekte der Kommunikation auf das Risikoverständnis der Datengebenden von dem Kontext des Risikos abhängen. Aus diesem Grund ist die Übertragung der Ergebnisse aus der Forschung zu Risikokommunikation in anderen Fachbereichen, wie beispielsweise aus der Medizin oder dem Katastrophenschutz auf die Privatsphärekommunikation möglicherweise nicht ohne Weiteres möglich. Das führt dazu, dass in der Praxis der gewählte ε-Wert oder die dadurch abgeleiteten Privatsphäregarantien den Datengebenden üblicherweise nicht kommuniziert werden

(Cummings u. a. 2021) und das Potenzial von DP somit nicht genutzt werden kann.

Die bisherigen Forschungsarbeiten zum Thema „Kommunikation von DP" beschränkten sich auf *qualitative* Beschreibungen von DP, wie sie in der Praxis verwendet werden, im Gegensatz zu einer möglichen quantitativen Kommunikation der Höhe des Privatsphäreschutzes: Cummings u. a. identifizierten aus 76 DP-Beschreibungen, die in der Praxis genutzt werden, sechs verschiedene Themen (z. B. „Methode", „Vertrauen" oder „Risiko"). In ihrer Vergleichsstudie (Cummings u. a. 2021) zur Wahrnehmung dieser Themen haben die Autorinnen herausgestellt, dass verschiedene Themen verschiedene Privatsphäreerwartungen der Datengebenden wecken. Xiong u. a. untersuchten in zwei aufeinander aufbauenden Studien den Effekt von Beschreibungen von DP auf die Bereitschaft von Datengebenden, ihre Daten weiterzuzugeben. In der ersten Studie (Xiong u. a. 2020) wurden verschiedene Beschreibungen von DP verglichen. Dabei konnte festgestellt werden, dass einige Faktoren (z. B. die Bekanntheit und das Vertrauen in die datensammelnde Organisation) einen größeren Einfluss auf die Weitergabebereitschaft der Datengebenden haben, als die Unterschiede der DP-Beschreibungen. Mit mehrfach verbesserten Beschreibungen von DP ist es Xiong u. a. gelungen das Verständnis der Studienteilnehmenden bezüglich DP unter bestimmten Voraussetzungen zu verbessern. In ihrer zweiten Studie (Xiong u. a. 2022) untersuchten die Autor:innen zusätzlich den Einfluss von Symbolen und Animationen in PD-UIs. Die Ergebnisse zeigen, dass statische Symbole keinen Nachteil gegenüber Animationen aufweisen, und dass die Teilnehmenden zwar einen stärkeren Privatsphäreschutz bevorzugen, jedoch auch gewillt sind, Privatsphärerisiken für sinnvolle Zwecke zu akzeptieren. Die Ergebnisse dieser bisher durchgeführten Studien sind vielversprechend, was die Kommunikation von Privatsphärerisiken angeht, beziehen sich aber alle auf qualitative Beschreibungen von DP bei denen der Wert des Parameters ε und der daraus resultierender Privatsphäreschutz nicht einbezogen wurde.

Abschließend sei eine weitere Herausforderung für die Kommunikation von Privatsphärerisiken genannt: die individuellen statistischen Kenntnisse, die sogenannte „Numeracy" (Cokely u. a. 2012). Personen mit geringen statistischen Kenntnissen überschätzen, im Gegensatz zu Personen mit besseren statistischen Kenntnissen, oft ihre Fähigkeiten Risiken einzuschätzen (Kruger u. a. 2000). Eine nicht abgestimmte Risikokommunikation könnte diesen Personen ein unbegründetes Sicherheitsgefühl vermitteln und sie damit verleiten, häufiger zu teilen, ohne die wirklichen Konsequenzen ver-

standen zu haben. Dadurch könnten sensible Daten unbeabsichtigt preisgegeben werden.

Zusammenfassend lässt sich sagen, dass DP als erstes Anonymisierungsverfahren das Potenzial birgt das quantifizierte Privatsphärenrisiko einer Datenweitergabe verständlich zu kommunizieren und damit zu einer informierten Entscheidung beizutragen. Um dieses Potenzial allerdings voll zu entfalten, müssen neue Kommunikationsansätze für DP entwickelt werden.

3. Privacy Decision User Interfaces für DP

Im Folgenden beschreiben wir die Überlegungen, die letztlich zur Gestaltung der von uns vorgeschlagenen und evaluierten Kommunikationsansätzen geführt haben.

3.1 Das Ziel von Privacy Decision User Interfaces

Das Ziel unserer User Interfaces ist die Unterstützung einer informierten Entscheidung. Für eine informierte Entscheidung (Bekker u. a. 1999) müssen die Datengebenden entscheiden können, ob sie das Risiko der Datenweitergabe als für den Zweck angemessen empfinden. Dieses Empfinden hängt von individuellen Faktoren ab. Daher ist nicht zu erwarten, dass alle Teilnehmenden sich in der jeweiligen Situation gleich entscheiden, wodurch die Weitergabebereitschaft kein angemessenes Messinstrument für eine informierte Entscheidung darstellt. Stattdessen nehmen wir an, dass eine informierte Entscheidung vorliegt, wenn die Entscheidung der Teilnehmenden mit ihren Privatsphärebedenken korreliert: Wir erwarten, dass Teilnehmende mit niedrigem Privatsphärebedürfnis bei gleichem Grund und erhofften Nutzen der Erhebung auch in unserer Studie öfter ihre Daten teilen als Teilnehmende mit höherem Privatsphärebedürfnis. Um diese informierte Entscheidung zu unterstützen, ist es essenziell, dass Datengebende die Konsequenzen ihrer Entscheidung verstehen. Die technischen Details von DP sind selbst für Expert:innen schwer nachzuvollziehen (Lee u. a. 2011). Daher ist eine Kommunikation der vollständigen Funktionsweise von DP nicht zielführend, um die Konsequenzen einer Datenweitergabe verständlich zu machen. Die Gestaltung der hier vorgeschlagenen PD-UIs fokussiert sich stattdessen auf die Kommunikation der Auswirkungen von DP unter Berücksichtigung des gewählten Privatsphäre-Parameters ε. Die

User Interfaces sollen Datengebenden helfen, die Frage zu beantworten „Was bedeutet die Weitergabe meiner Daten für mein Privatsphärenrisiko?“ DP ist für diese Art der Kommunikation aus zwei Gründen besonders geeignet:

1. Der Schutz durch DP ist unabhängiger von äußeren Faktoren, da DP auf der Annahme basiert, dass Angreifende bereits alles potenziell verfügbare Wissen, außer der sensiblen Information, besitzen.
2. Die Definition von DP selbst beschreibt die Eigenschaft der Privatsphäre-Garantie, nicht aber den Algorithmus, wie diese Garantie erreicht wird. Die Garantie kann durch verschiedene Algorithmen umgesetzt werden und ist daher auch unabhängig vom genutzten Algorithmus formuliert.

Statt also die Funktionsweise eines DP-Algorithmus zu erklären, zielen die hier vorgeschlagenen PD-UIs darauf ab, den Datengebenden das Privatsphärenrisiko zu kommunizieren. Wir nutzen dazu ein Risiko-Modell (Mehner u. a. 2022) für DP. Dieses Modell berechnet aus dem Privatsphäre-Parameter ε ein Privatsphärenrisiko, welches angibt, wie wahrscheinlich es ist, dass Angreifende die sensible Information über die Zielperson richtig vermuten können[5].

Um das Privatsphärenrisiko verständlich zu vermitteln, beziehen wir Berücksichtigung bestehender Forschung zur generellen numerischen Risikokommunikation, zwei Aspekte ein: die *textuelle Vermittlung von Risiken* und der *Einsatz von interaktiven UI-Elementen*. Um den Effekt dieser Aspekte auf die informierte Entscheidung zu untersuchen, wurden zwei aufeinander aufbauende empirische Studien durchgeführt. Im Folgenden werden die betrachteten Optionen für beide Aspekte vorgestellt.

3.2 Studie 1: Textuelle Risikoformate

In der medizinischen Forschung wurden bereits vielfältige Erkenntnisse zur effektiven Risikokommunikation erzielt. Eine Richtung der Forschung in der Medizin fokussiert sich auf die Frage, welche textuellen Formate Patient:innen ein realistisches Risikoempfinden ermöglichen. Aus den empfohlenen Risikoformaten in der Medizin haben wir zwei besonders geeignete

5 Weitere Informationen zu diesem Modell und wie es in den PD-UIs genutzt wird findet sich in unserer Veröffentlichung (Franzen u. a. 2022).

Grundformate, Prozente (z. B. „52 %“) und Häufigkeiten (z. B. „26 aus 50“), ausgewählt, die auf Privatsphärerisiken übertragbar sind. Zusätzlich werden in der Medizin verschiedene Variationen der Risikokommunikation unabhängig vom gewählten Grundformat empfohlen. Im Rahmen der Risikokommunikation von DP-Privatsphärerisiken haben wir zwei vielversprechende Variationen ausgewählt: Eine negative Formulierung „Das Risiko tritt in 52 % der Fälle ein“ kann einen anderen Effekt auf die Entscheidung haben als die äquivalente positive Formulierung „Das Risiko tritt in 48 % der Fälle *nicht* ein“ (sog. „Framing Effect“). Unsere Variation „Outcome Framing“ beschreibt daher explizit beide Wahrscheinlichkeiten. In der Medizin wird ferner empfohlen Risiken mit anderen bekannten Risiken zu vergleichen, um einen intuitiveren Zugang zu ermöglichen. Da DP per Definition immer einen Vergleich zwischen dem Risiko vor und nach der Datenweitergabe darstellt, geben wir in der Variation „Comparison to status quo“ explizit beide diese Wahrscheinlichkeiten an.

Insgesamt ergaben sich aus den Grundformaten und Variationen sechs Risikobeschreibungen: jedes Grundformat jeweils ohne Variation, mit „Outcome Framing“ oder mit „Comparison to status quo“. Als siebte Risikobeschreibung nutzen wir eine gebräuchliche Beschreibung von DP, die kein numerisches Privatsphärenrisiko explizit nennt. Diese sieben Beschreibungen wurden für die erste Studie in eine typische Benutzeroberfläche eingebettet und Studienteilnehmenden im Kontext einer Ride-Sharing App präsentiert (Beispiele in Abb. 1).[6]

3.3 Studie 2: Grafische User Interface-Elemente

Die Repräsentation des Risikos in den verschiedenen textuellen Formaten, kann durch grafische Elemente sinnvoll unterstützt werden. Daher haben wir in einer Vorstudie zunächst aus Antworten zu qualitativen Fragen herausgearbeitet, dass vor allem drei Aspekte für das Verständnis des DP-Risikos wichtig sind:

Erstens ist numerisches Risiko an sich schwer zu verstehen und besonders Datengebende mit geringen statistischen Kenntnissen benötigen Unterstützung, um mit den angezeigten Zahlen umzugehen. Eine vielversprechende Methode ist die grafische Darstellung des Risikos. Wir visualisieren

6 Weitere Informationen zum Design der genutzten UIs und zum Studiendesign können nachgelesen werden in unserer Veröffentlichung zu dieser Studie (Franzen u. a 2022).

das Risiko als Icon Array, das 100 Kreise in einer zweidimensionalen Anordnung zeigt. Einige Kreise sind ausgefüllt und verdeutlichen, wie viele Personen von 100 von dem beschriebenen Risiko betroffen wären. Bei einem Risiko von 22 % wären beispielsweise 22 der 100 Kreise ausgefüllt. Wir vermuten, dass Icon Arrays aufgrund ihrer Anschaulichkeit eine intuitive Darstellung von Risiken bieten und damit insbesondere Personen mit geringen statistischen Kenntnissen helfen können, das Privatsphärenrisiko zu verstehen.

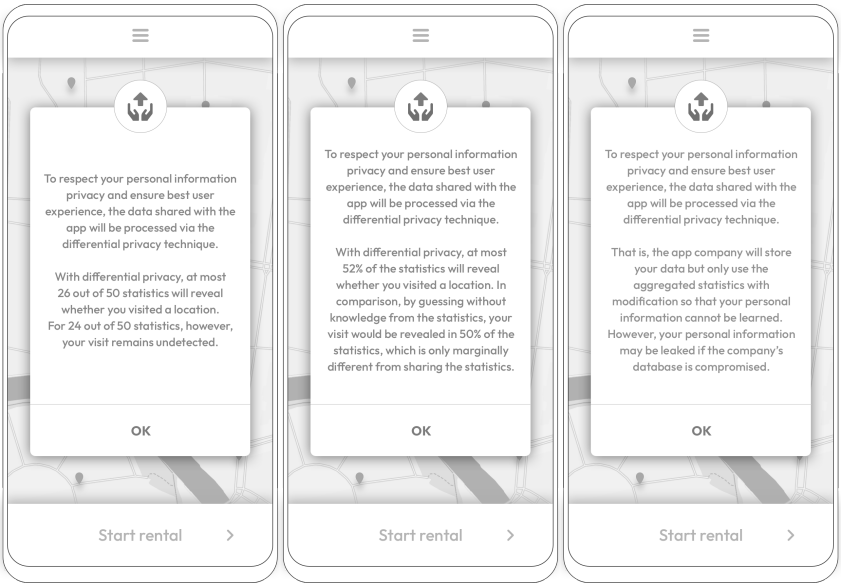

Abbildung 1: UIs mit textuellen Risikoformaten

Quelle: Franzen u.a. 2022

Abbildungslegende: Beispiele der benutzen UIs mit Risikoformaten. Gezeigt sind von links nach rechts: Häufigkeiten mit Outcome Framing, Prozente mit Vergleich zum Status Quo und Beschreibung ohne explizite Nennung des numerischen Risikos

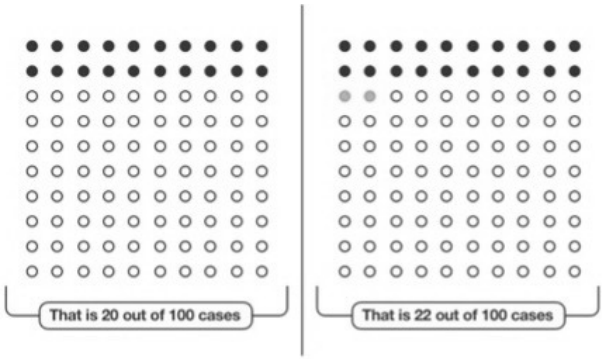

Abbildung 2: Icon-Arrays

Quelle: Franzen u.a. 2024

Abbildungslegende: Beispiele für die Icon Array-Visualisierung, links 20%, rechts 22%

Der zweite Aspekt beim Verständnis von DP ist der Umstand, dass DP zwei Risiken vergleicht: DP nimmt an, dass bereits vor der Datenweitergabe ein gewisses Vorrisiko existiert. Das bedeutet, dass Angreifende schon vor der betroffenen Datenerhebung mit einer gewissen Wahrscheinlichkeit eine korrekte Vermutung zur sensiblen Information anstellen können. DP vergleicht, wie sehr die neue Datenweitergabe dieses Vorrisiko im schlimmsten Falle anheben könnte. Dieser Vergleichscharakter von DP muss vermittelt werden. Eine Möglichkeit ist eine Gegenüberstellung der beiden Risiken. Wir haben daher unsere Benutzeroberfläche vertikal in zwei Hälften zum Risiko vor bzw. nach der Datenweitergabe unterteilt (vgl. Abb. 3).

Außerdem kann die Icon Array-Visualisierung auch den Unterschied zwischen den beiden Risiken in einer anderen Farbe darstellen (vgl. Abb. 2, rechts in grau), um die Intuition über den relativen Anstieg des Risikos weiter zu unterstützen.

Drittens hängt das Vorrisiko, mit dem DP vergleicht, von zahlreichen individuellen Faktoren ab, beispielsweise davon, wie oft eine Person bereits Daten geteilt hat, um welche Daten es sich handelt oder wie die Verteilung der sensiblen Information in der Allgemeinbevölkerung ist. Darüber hinaus können selbst für die gleiche Person unterschiedliche Informationen (wie z. B. verschiedene Orte) unterschiedliche Vorrisiken haben. Ein PD-UI kann daher nicht ein einziges Risikopaar präsentieren. Datengebende müssen vielmehr in der Lage sein, diese Risikopaare für verschiedene Situationen und Vorrisiken zu erkunden. Eine solche Exploration ist in unserem

Abbildung 3: Gegenüberstellung der Risiken in der Benutzeroberfläche

Quelle: Franzen u.a. 2024

Abbildungslegende: Benutzeroberfläche, die den Vergleich der beiden Risiken erleichtert. Links: Informationen zum Vorrisiko mit Bedienfeld „Nicht teilen", rechts: Informationen zum Risiko nach der Datenweitergabe mit Bedienfeld „Teilen"

Privacy Decision UI durch verbundene Slider realisiert (vgl. Abb. 4). Je ein Slider visualisiert das Risiko vor bzw. nach der Datenweitergabe. Datengebende können die Slider auf verschiedene Werte anpassen, wodurch der jeweils andere Slider automatisch anhand des durch DP garantierten Zusammenhangs auf die entsprechende Position gesetzt wird. Auf diese Weise können Datengebende entweder auf der linken Seite das Vorrisiko ihrer individuellen Situation anpassen und so das Risiko nach der Datenweitergabe auf dem rechten Slider sehen oder sie können rechts das maximal tolerierte Risiko nach der Datenweitergabe einstellen und auf dem linken Slider ablesen, bis zu welchem Vorrisiko ihre Informationen durch DP geschützt sind. Dadurch ist es Datengebenden möglich, den Privatsphäreschutz von DP auch für mehrere unterschiedliche Situationen zu explorieren und ein mentales Modell aufzubauen.

Wir erwarten, dass jedes dieser Elemente einen Einfluss auf die informierte Entscheidung haben könnte. Daher haben wir unterschiedliche Kombinationen dieser Elemente in PD-UIs realisiert und für die zweite Studie in eine fiktive Car-Sharing App eingebettet. Exemplarische Darstellungen dieser Benutzeroberflächen sind in Abb. 5 dargestellt.

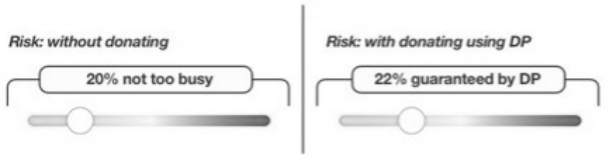

Abbildung 4: Verbundene Slider

Quelle: Franzen u.a. 2024

Abbildungslegende: Slider, mit denen Datengebende den Privatsphäreschutz erforschen können. Links: Slider mit Vorrisiko, rechts: Slider mit Risiko nach Datenweitergabe. Die Bedienung eines Slider führt automatisch zur Anpassung des anderen Sliders, in Übereinstimmung mit der DP-Garantie.

Abbildung 5: UIs mit unterstützenden UI-Elementen

Quelle: Franzen u.a. 2024

Abbildungslegende: Beispiele der erstellten Benutzeroberflächen mit unterschiedlichen Elementen. Gezeigt sind von links nach rechts: „Hybrid“ mit Slider und Icon-Arrays, „Interactive“ nur mit den verbundenen Slidern und “Beschreibung qualitativ” ohne weitere UI-Elemente

3.4 Studiendurchführung

Um den Effekt der textuellen und grafischen Risikokommunikation auf die informierte Entscheidung zu vergleichen, haben wir die Benutzeroberflächen mittels Crowdsourcing auf der Plattform „Mechanical Turk" von Amazon[7] evaluiert. Die Eckdaten der beiden Studien sind in der Tabelle 1 zusammengefasst. Im Rahmen der Studien wurden verschiedene Variablen erhoben, darunter die Entscheidung für oder gegen die Datenweitergabe, bestehende Privatsphärebedenken, das Verständnis der gezeigten Informationen sowie die Zufriedenheit im Umgang mit den UIs. Zusätzlich wurden Kompetenzen und Persönlichkeitsmerkmale der Teilnehmenden, beispielsweise statistische Kenntnisse, erfasst, um zu evaluieren, ob diese Faktoren einen Einfluss auf die Effektivität der UIs haben.

	Studie 1: Textuelle Formate	**Studie 2: Grafische Elemente**
Kontext	Ride-Sharing App	Car-Sharing App
Haupteinfluss	Risikoformate	UI-Elemente
Zielvariable	Verständnis (subjektiv, objektiv)	Informierte Entscheidung (Entscheidungen vgl. mit Privatsphärebedenken)
Rekrutierung	Crowdsourcing (Amazon Mechanical Turk)	
Teilnehmende	343	378
Gruppen	7 (~49 pro Gruppe)	5 (~75 pro Gruppe)
Studiendesign	Zwischenindividueller Vergleich	Zwischenindividueller Vergleich
Zusätzlich betrachtete Variablen	Privatsphärebedenken, statistisches Vorwissen, Geschlecht	Usability, Einprägsamkeit des Risikos / Entscheidung, statistisches Vorwissen, Entscheidungstyp, Kognitionsbedürfnis

Tabelle 1: Eckdaten der Studiendesigns

4. Kommunikation von Privatsphärerisiken für informierte Entscheidungen

Im Folgenden geben wir einen Überblick über die Ergebnisse der beiden Studien.

7 https://www.mturk.com/

4.1 Textuelle Risikokommunikationsformate

Unsere erste Studie untersuchte verschiedene textuelle Risikoformate. Die Ergebnisse zeigen, dass das objektive Verständnis der Teilnehmenden, gemessen mit Kontrollfragen zu Fakten über den Schutz der Privatsphäre, bei allen sieben Risikoformaten etwa gleich ist. Auffallend ist jedoch, dass das Verständnis im Mittel mit durchschnittlich 1,8 von maximal 4 Punkten generell schlecht ist. Dies unterstützt die Vermutung, dass die Vermittlung von Privatsphärerisiken mittels textueller Risikoformate nicht effektiv ist und alternative Ansätze zur Unterstützung notwendig sind.

Die Teilnehmenden wurden auch gefragt, wie gut sie sich auf einer Skala von 1 bis 7 informiert fühlen. Hierbei hat das Risikoformat ohne numerische Risikoangaben zu einer höheren Selbsteinschätzung (5,6 von 7) geführt als die sechs numerischen Risikoformate. Das schlechteste Risikoformat, „Frequenzen mit Vergleich zum Status Quo", ergab eine signifikant schlechtere Einschätzung (4,6 von 7). Die anderen fünf Risikoformate schnitten schlechter (4,9 - 5,1) als das nicht-numerische Format ab, allerdings nicht statistisch signifikant schlechter. Die Tatsache, dass die Teilnehmenden ähnlich viel verstanden haben, sich aber schlechter informiert fühlten, legt nahe, dass Menschen bei der numerischen Risikokommunikation mehr Unterstützung benötigen, um die vermittelten Informationen in eine informierte Entscheidung einfließen lassen zu können.

Darüber hinaus haben wir den Einfluss persönlicher Merkmale auf das Risikoverständnis untersucht. Dabei konnte bestätigt werden, dass das objektive Verständnis von DP, das mit Kontrollfragen gemessen wurde, nicht von diesen Faktoren abhängt. Bei der Analyse der Selbsteinschätzungen zeigte sich jedoch ein Zusammenhang zwischen statistischen Kenntnissen und der Selbsteinschätzung: In einigen Varianten unserer UIs schätzen Teilnehmende mit geringeren statistischen Kenntnissen ihr Verständnis von DP signifikant höher ein als Teilnehmende mit höheren statistischen Kenntnissen. Dies ist, ähnlich dem Dunning Kruger-Effekt, dadurch erklärbar, dass Personen mit geringeren statistischen Kenntnissen sich ihrer Schwächen nicht bewusst sind. Diese Selbstüberschätzung verhindert eine informierte Entscheidung, da sich Personen mit niedrigen statistischen Kenntnissen sicherer fühlen, als es ihrem Verständnis des Privatsphäreschutzes entspricht. Dadurch besteht die Möglichkeit, dass sie ihre Daten mit einem höheren Privatsphärenrisiko weitergeben als beabsichtigt. Ohne

geeignete Gegenmaßnahmen könnte dieser Effekt zu einer Benachteiligung dieser Bevölkerungsgruppen führen[8].

4.2 Grafische Elemente der Risikokommunikation

In unserer zweiten Studie wurde untersucht, welche Elemente einer Benutzeroberfläche die Datengebenden unterstützen können, eine informierte Entscheidung zu treffen. Diese Elemente werden zusätzlich zu den textuellen Risikoinformationen eingesetzt. Um eine informierte Entscheidung zu messen, wurde der Zusammenhang zwischen Entscheidung und Privatsphärebedenken untersucht. In der Benutzeroberfläche, die sowohl Slider als auch Icon-Arrays enthält („Hybrid", siehe Abb. 5), konnte dieser Zusammenhang bestätigt werden. Datengebende, die sich bei dieser Benutzeroberfläche für eine Datenweitergabe entschieden haben, haben im Durchschnitt geringere Privatsphärebedenken (⌀ 5,6 von 7 Punkten) als Datengebende, die sich gegen eine Datenweitergabe entschieden haben (⌀ 6,25). Im Vergleich zu den anderen Benutzeroberflächen ist dieser Effekt drei- bis sechsmal größer (vgl. Abb. 6) und deutet darauf hin, dass die Datengebenden bei dieser Benutzeroberfläche die Risikoinformationen besser in ihre Entscheidung einbeziehen können.
Wir empfehlen daher die Verwendung von PD-UIs, die sowohl eine interaktive Risikoexploration als auch eine grafische Risikovisualisierung beinhalten.

Darüber hinaus haben wir untersucht, wie sich die Benutzeroberflächen auf die Bereitschaft zur Datenweitergabe auswirken: Der Anteil der Personen, die sich für die Datenweitergabe entschieden haben, ist unabhängig von der verwendeten Benutzeroberfläche in etwa gleich (63 %-72 %). Wir konnten in unserer Studie also keinen negativen Einfluss der Risikokommunikation auf die Bereitschaft zur Datenweitergabe feststellen. Stattdessen haben sich bei der Benutzeroberfläche mit Slider und Icon Array andere Teilnehmende, nämlich vor allem diejenigen mit weniger Privatsphärebedenken, für die Datenweitergabe entschieden.

Auch in dieser Studie konnte ein Einfluss der statistischen Kenntnisse nachgewiesen werden: Bei einigen Benutzeroberflächen führte ein geringeres statistisches Vorwissen dazu, dass eher geteilt wurde, während bei

8 Mehr Details zu diesen Ergebnissen sind in unserer Veröffentlichung zu dieser Studie (Franzen u. a. 2022) verfügbar.

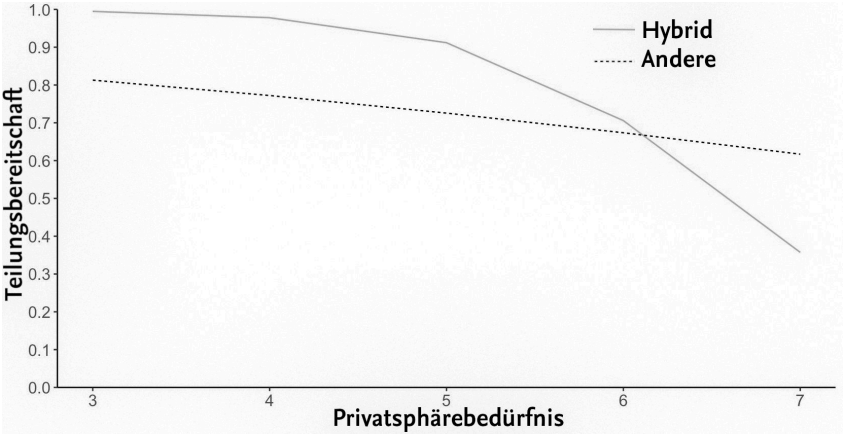

Abbildung 6: Zusammenhang zwischen Privatsphärebedenken und Weitergabebereitschaft

Quelle: Franzen u.a. 2024

Abbildungslegende: Das Diagramm zeigt den Zusammenhang zwischen Privatsphärebedenken (x-Achse) und der Weitergabebereitschaft (y-Achse). Die Benutzeroberfläche mit Slider und Icon-Arrays (Hybrid, durchgezogene Linie) zeigt einen deutlichen Zusammenhang im Vergleich zu den Daten aller anderen Benutzeroberflächen (gestrichelte Linie)

anderen Benutzeroberflächen eher Teilnehmende mit besseren statistischen Kenntnissen teilten. Darüber hinaus fanden wir weitere kleinere Effekte von persönlichen Merkmalen, die die Einprägsamkeit von Risikoinformationen und Zufriedenheit mit den angezeigten Informationen beeinflussen. Die Möglichkeit solcher Effekte sollte bei der Gestaltung von PD-UIs berücksichtigt werden[9].

5. Das Potenzial von DP für die Gesellschaft nutzbar machen.

Unsere Studien geben erste Einblicke wie Risikokommunikation die informierte Entscheidung von Datengebenden unterstützen kann. Diese Unterstützung hat das Potenzial große Datensätze zu generieren, die aus vielen einzelnen informiert gegebenen Datenpunkten bestehen. Diese können

9 Mehr Details zu der Methodik und den Ergebnissen dieser Studie sind in der Veröffentlichung zu dieser Studie verfügbar (Franzen u. a. 2024).

der Gesellschaft helfen, nötige Entscheidungen zu aktuellen Herausforderungen bedarfsgerecht und repräsentativ zu treffen. Um dieses Ziel zu erreichen, leiten wir aus den Ergebnissen unserer Studien nachfolgend Handlungsempfehlungen ab.

5.1 Transparente Kommunikation als Motivator zur Datenweitergabe

In unseren Studien zur Kommunikation von Privatsphärerisiken beim Einsatz von DP haben wir festgestellt, dass quantitative Privatsphärerisiken durchaus zu einer informierten Entscheidung beitragen. Befürchtungen, dass die Erklärung von Risiken das Verständnis von DP negativ beeinflussen könnte, konnten wir in unserer ersten Studie nicht feststellen. Auch die Teilungsbereitschaft wurde durch die transparente Kommunikation von Privatsphärerisiken in der zweiten Studie nicht negativ beeinflusst. Im Gegenteil konnten wir bei der Nutzung von interaktiven und grafisch visualisierten Risikobeschreibungen einen signifikanten Anstieg der Informiertheit der Entscheidung feststellen, d. h. eine Übereinstimmung der Entscheidung mit den Privatsphärebedenken. Diese Ergebnisse sehen wir als klares Zeichen, dass die transparente Kommunikation von Privatsphärerisiken praktikabel und sogar erstrebenswert für die Kommunikation mit Datengebenden ist. Wir sprechen uns daher klar für eine verbesserte transparente Kommunikation von Privatsphärerisiken aus. Transparenz kann perspektivisch das Vertrauen in Datensammlungen unterstützen und damit auch weitere Gruppe von Datengebenden motivieren, Daten zur Verfügung zu stellen.

5.2 Gesellschaftlicher Lernprozess zu Privatsphärerisiken

Das Ziel unserer Forschung ist es, das Potenzial von DP für die Gesellschaft nutzbar zu machen. Nicht alle Datengebenden können über Nacht zu Risiko-Expert:innen werden. Vielmehr verfolgen wir eine mehrstufige Vision: Zunächst muss den Datengebenden während der Entscheidung zur Datenweitergabe die Information zu dem gewählten Kompromiss verständlich kommuniziert werden. Damit können Datengebende unterstützt werden bei der bewussten Entscheidung für oder gegen die Datenweitergabe. Neben individuellen Faktoren, wie momentane Aufmerksamkeit, Umgebungs-

einflüsse oder persönliche Kompetenzen, stellt die Risikokommunikation lediglich einen weiteren Einfluss auf die Privatsphäreentscheidung dar. Selbst bei optimaler Kommunikation kann nicht jede Entscheidung perfekt mit den Privatsphärebedenken der Datengebenden übereinstimmen. Die vorgeschlagene Gestaltung von Benutzeroberflächen für informierte Entscheidungen wird jedoch mit der Zeit mittels vieler solcher Entscheidungen in der Gesellschaft zur Entwicklung von Normen beitragen, die sinnvolle Werte für den Privatsphäreschutz für unterschiedliche Datenkategorien offenlegen. Beispielsweise könnte herausgestellt werden, ob das allgemeine Privatsphärebedürfnis in der Bevölkerung bei Mobilitätsdaten, die aus einzelnen anonymisierten Punkten bestehen, geringer ist als bei verbundenen Punkten, die mittels eines Pseudonyms zu einem umfassenderen Bewegungsprofil verknüpft werden können. In einem zweiten Schritt können diese etablierten Normen die Politik informieren, verpflichtende Mindestwerte für Anonymisierung in verschiedenen Datenkategorien zu formulieren (vgl. Dwork u. a. 2019). Die Einführung von Richtwerten für angemessene Anonymisierungsniveaus könnte auch rechtlich zu mehr Klarheit beitragen, beispielsweise hinsichtlich der Frage, welcher Grad der Anonymisierung erforderlich ist, um eine Beziehung zu einer identifizierbaren natürlichen Person auszuschließen (vgl. DSGVO Erwägungsgrund 26[10]).

In einem dritten Schritt könnten diese Richtwerte schließlich wieder in das Bewusstsein und die Intuition von Bürger:innen eingehen und so ein gemeinsames Verständnis von akzeptablen Risikoniveaus schaffen. Ein solches Verständnis würde im Endeffekt die Risikokompetenzen in der Gesellschaft stärken. Die neue Risikokompetenz könnte erfahrenen Datengebenden mittels einer Variante von DP, der lokalen DP (Kasiviswanathan u. a. 2008), sogar ermöglichen selbst das gewünschte Privatsphäreniveau auszuwählen, bevor Daten weitergegeben werden, und damit den Kompromiss für die individuellen Bedürfnisse zu optimieren: so privat wie nötig, aber so präzise wie damit möglich.

5.3 Individuelle Kompetenzen und Haltungen einbeziehen

Die PD-UIs, die in unseren Studien einen positiven Effekt auf die informierte Entscheidung bewiesen haben, enthalten viel Information und

10 https://dsgvo-gesetz.de/erwaegungsgruende/nr-26/ (zuletzt aufgerufen 4. Juni 2024)

Komplexität und sind daher nicht für alle Nutzer:innen gleichermaßen geeignet. Mit weiteren Erkenntnissen aus der Risikokommunikation in verwandten Forschungsbereichen könnte diese Komplexität möglicherweise noch reduziert werden. Aber selbst mit einfachen UI-Elementen haben unsere Studien an mehreren Stellen aufgezeigt, dass persönliche Eigenschaften einen Einfluss auf die Effektivität der Risikokommunikation haben können. Das könnte beispielsweise dazu führen, dass Datengebende mit geringen statistischen Kenntnissen benachteiligt werden, wie wir oben diskutiert haben. Um dem entgegenzuwirken, schlagen wir PD-UIs vor, die adaptiv auf persönliche Eigenschaften eingehen können. Im Bereich der Privacy Usability wurden Benutzeroberflächen mit unterschiedlichen Detailebenen umgesetzt (Schaub u. a. 2015). Hier werden standardmäßig einfach verständliche Privatsphäre-Icons angezeigt, die aber bei Interesse in einer weiteren Ansicht genauer erklärt werden. Für Nutzer:innen mit höherem Informationsbedürfnis werden auf der dritten Ebene detaillierte Dokumente verfügbar gemacht. Eine ähnliche Umsetzung könnte auch bei der Nutzung von DP die Informationsbedürfnisse von verschiedenen Datengebenden erfüllen, ohne zu überfordern.

Für besonders wichtige Entscheidungen könnten allerdings auch personalisierte UIs sinnvoll sein. Dazu ist zunächst eine Analyse der Kompetenzen der Datengebenden erforderlich. Auf Basis dieser Analyse könnte dann eine Benutzeroberflächenvariation ausgewählt werden, die spezifisch entworfen wurde, um Datengebende in diesem Kompetenzbereich optimal zu unterstützen. In einer typischen Entscheidungssituation ist sicherlich nicht genug Zeit, um zunächst ein persönliches Profil zu erstellen. In Fällen, in denen es um eine langfristige oder wiederholte detaillierte Aufzeichnung von Bewegungsdaten geht, könnte dieser Schritt jedoch angemessen sein. Beispielsweise könnte eine Erhebungsplattform, die einen Pool mit wiederkehrenden Teilnehmenden verwaltet, bei der Registrierung sinnvolle Kompetenzen mittels kurzer Befragungen ermitteln und daraufhin die PD-UIs individuell anpassen.

6. Fazit und Zusammenfassung

Differential Privacy ermöglicht, im Unterschied zu anderen Anonymisierungsverfahren, die präzise Kommunikation des Privatsphärenrisikos unabhängig vom Wissen der Angreifenden. Dadurch eröffnet sich ein enormes Potenzial, Datengebende in die Lage zu versetzen, eine (wirklich)

informierte Entscheidung zu treffen. Um dieses Potenzial jedoch nutzen zu können, muss der Privatsphäreschutz den Datengebenden verständlich kommuniziert werden. Unsere Studien legen nahe, dass eine Kombination aus interaktiver Exploration der Risiken mit grafischen Risikovisualisierungen dazu beitragen kann, Datengebende bei einer informierten Entscheidung zu unterstützen. Allerdings müssen bei der Umsetzung persönliche Kompetenzen berücksichtigt werden, um eine Benachteiligung bestimmter Gruppen zu vermeiden. Die Kombination dieser Ergebnisse verspricht eine verantwortungsvollere Datensammlung und somit eine nachhaltige Lösung für den seit jeher bestehenden Konflikt zwischen dem Schutz der Privatsphäre der Datengebenden und dem gesellschaftlichen Mehrwert, der durch die Daten generiert werden kann.

Literatur

Acquisti, Alessandro; Adjerid, Idris; Balebako, Rebecca; Brandimarte, Laura; Cranor, Lorrie Faith; Komanduri, Saranga; Leon, Pedro Giovanni; Sadeh, Norman; Schaub, Florian; Sleeper, Manya; Wang, Yang und Wilson, Shomir (2017): Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys*, *50*(3), 44:1-44:41. https://doi.org/10.1145/3054926

Bekker, Hilary; Thornton, Jim G.; Airey, Mark C.; Connelly, James B.; Hewison, Jenny; Robinson, M. B.; Lilleyman, J.; MacIntosh, M.; Maule, Alexander John und Michie, Susan. (1999): Informed decision making: an annotated bibliography and systematic review. *Health Technology Assessment*, *3*(1), 1–156.

Cokely, Edward; Galesic, Mirta; Schulz, Eric; Ghazal, Saima und Garcia-Retamero, Rocio. (2012): Measuring Risk Literacy: The Berlin Numeracy Test. *Judgment and Decision Making*, *7*. https://doi.org/10.1037/t45862-000

Cummings, Rachel; Kaptchuk, Gabriel und Redmiles, Elissa M. (2021): "I need a better description":An Investigation Into User Expectations For Differential Privacy. *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, S. 3037–3052. https://doi.org/10.1145/3460120.3485252

de Montjoye, Yves-Alexandre; Hidalgo, César A.; Verleysen, Michel und Blondel, Vincent D. (2013): Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports*, *3*(1), 1376. https://doi.org/10.1038/srep01376

Domingo-Ferrer, Josep; Sánchez, David und Blanco-Justicia, Alberto (2021): The limits of differential privacy (and its misuse in data release and machine learning). *Communications of the ACM*, *64*(7), 33–35. https://doi.org/10.1145/3433638

Douriez, Marie; Doraiswamy, Harish; Freire, Juliana und Silva, Cláudio T. (2016): Anonymizing NYC Taxi Data: Does It Matter? *2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA)*, S. 140–148. https://doi.org/10.1109/DSAA.2016.21

Dwork, Cynthia (2006): Differential Privacy. In M. Bugliesi, B. Preneel, V. Sassone, & I. Wegener (Hrsg.), *Automata, Languages and Programming*. Berlin u.a.: Springer. S. 1–12. https://doi.org/10.1007/11787006_1

Dwork, Cynthia; Kohli, Nitin und Mulligan, Deirdre (2019): Differential Privacy in Practice: Expose your Epsilons! *Journal of Privacy and Confidentiality*, *9*(2), Article 2. https://doi.org/10.29012/jpc.689

Franzen, Daniel; Müller-Birn, Claudia und Wegwarth, Odette (2024): Communicating the Privacy-Utility Trade-off: Supporting Informed Data Donation with Privacy Decision Interfaces for Differential Privacy. *Proceedings of the ACM on Human-Computer Interaction*, *8*(CSCW1), 32, 1-32:56. https://doi.org/10.1145/3637309

Franzen, Daniel; Nuñez von Voigt, Saskia; Sörries, Peter; Tschorsch, Florian und Müller-Birn, Claudia (2022): Am I Private and If So, how Many? Communicating Privacy Guarantees of Differential Privacy with Risk Communication Formats. *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, S. 1125–1139. https://doi.org/10.1145/3548606.3560693

Friedman, Batya und Hendry, David G. (2019): *Value Sensitive Design: Shaping Technology with Moral Imagination*. Cambridge: MIT Press. https://doi.org/10.7551/mitpress/7585.001.0001

Kairouz, Peter; Oh, Sewoong und Viswanath, Pramod (2015): Extremal Mechanisms for Local Differential Privacy. *arXiv:1407.1338*. https://doi.org/10.48550/arXiv.1407.1338

Kasiviswanathan, Shiva Prasad; Lee, Homin K.; Nissim, Kobbi; Raskhodnikova, Sofya und Smith, Adam (2008): What Can We Learn Privately? *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, 531–540. https://doi.org/10.1109/FOCS.2008.27

Kenny, Christopher T.; Kuriwaki, Shiro; McCartan, Cory; Rosenman, Evan T. R.; Simko, Tyler und Imai, Kosuke (o. J.): The use of differential privacy for census data and its impact on redistricting: The case of the 2020 U.S. Census. *Science Advances*, *7*(41), eabk3283. https://doi.org/10.1126/sciadv.abk3283

Kling, Rob und Star, Susan Leigh (1998): Human centered systems in the perspective of organizational and social informatics. *ACM SIGCAS Computers and Society*, *28*(1), S. 22–29. https://doi.org/10.1145/277351.277356

Kruger, Justin und Dunning, David (2000): Unskilled and Unaware of It: How Difficulties in Recognizing One's Own Incompetence Lead to Inflated Self-Assessments. *Journal of Personality and Social Psychology*, *77*: 1121–1134. https://doi.org/10.1037//0022-3514.77.6.1121

Lee, Jaewoo und Clifton, Chris (2011): How Much Is Enough? Choosing ε for Differential Privacy. In X. Lai, J. Zhou, & H. Li (Hrsg.), *Information Security*. Berlin u.a.: Springer. S. 325–340. https://doi.org/10.1007/978-3-642-24861-0_22

Leimstädtner, David; Sörries, Peter und Müller-Birn, Claudia (2023): Investigating Responsible Nudge Design for Informed Decision-Making Enabling Transparent and Reflective Decision-Making. *Proceedings of Mensch und Computer 2023*, S. 220–236. https://doi.org/10.1145/3603555.3603567

Mehner, Luise; Tschorsch, Florian und Nunez von Voigt, Saskia (2021): Towards Explaining Epsilon: A Worst-Case Study of Differential Privacy Risks. *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, S. 328–331. https://doi.org/10.1109/EuroSPW54576.2021.00041

Moggridge, Bill (2007): *Designing Interactions*. Cambridge: MIT Press.

Narayanan, Arvind und Shmatikov, Vitaly (2008): Robust De-anonymization of Large Sparse Datasets. *2008 IEEE Symposium on Security and Privacy (SP 2008)*, S. 111–125. https://doi.org/10.1109/SP.2008.33

Schaub, Florian; Balebako, Rebecca; Durity, Adam L. und Cranor, Lorrie Faith (2015): A Design Space for Effective Privacy Notices. *SOUPS 2015 Proceedings*, S. 1–17. https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub

Sweeney, Latanya (2002): k-anonymity: a model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(5): 557–570. https://doi.org/10.1142/S0218488502001648

Wang, Yue; Wu, Xintao und Hu, Donghui (2016): Using Randomized Response for Differential Privacy Preserving Data Collection. *Workshop Proceedings of the EDBT/ICDT 2016 Joint Conference*.

Xiong, Aiping; Wang, Tianhao; Li, Ninghui und Jha, Somesh (2020): Towards Effective Differential Privacy Communication for Users' Data Sharing Decision and Comprehension. *2020 IEEE Symposium on Security and Privacy (SP)*, S. 392–410. https://doi.org/10.1109/SP40000.2020.00088

Xiong, Aiping; Wu, Chuhao; Wang, Tianhao; Proctor, Robert W.; Blocki, Jeremiah; Li, Ninghui und Jha, Somesh (2022): Using Illustrations to Communicate Differential Privacy Trust Models: An Investigation of Users' Comprehension, Perception, and Data Sharing Decision. *arXiv:2202.10014*. http://arxiv.org/abs/2202.10014