AndProtect

AndProtect: Zusammenfassung Online-Befragung „Datenschutz bei mobilen Applikationen“

Chemnitz, Oktober 2016

Susen Döbelt, Josephine Halama, Falk Kuhnert

Allgemeine und Arbeitspsychologie, Technische Universität Chemnitz

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

secuvera

DAI-Labor TU Berlin

ALLGEMEINE UND ARBEITSPSYCHOLOGIE TU CHEMNITZ

Ziel und Durchführung der Befragung

Die Online-Befragung ist eines der ersten Arbeitspakete des Verbundprojektes AndProtect (www.andprotect.de).

Innerhalb der Befragung sollte identifiziert werden, welche **Arten von Daten im mobilen Nutzungskontext** entstehen und wie diese **von Nutzerseite hinsichtlich ihrer Bedenklichkeit für die Wahrung der eigenen Privatsphäre bewertet werden**.

- Durchführung vom 23.02.2016 bis 03.05.2016 (nach 10 Wochen)
- Verteilung über: Studenten/Mitarbeiter-Verteiler, persönliche Kontakte der Projektpartner, Testpersonendatenbank Allgemeine und Arbeitspsychologie der TU Chemnitz, andere Projekte der Förderinitiative, TU Chemnitz-Facebook-Meldung

Aufbau der Befragung

Begrüßung und Einleitung der Befragung

- Nutzung verschiedener App-Gruppen (Karten-App, Messenger-App, Wetter-App und Shopping-App)
- Bewertung der Bedrohlichkeit für die eigene Privatsphäre von 15 Datenarten für jede App-Gruppe bei a) Interaktion mit der App und b) kontinuierlichem Tracking

- Wünsche: Verbesserung Privatsphärenschutz im mobilen Bereich

- Selbsteinschätzung hinsichtlich: Technikaffinität, Wissen über Apps, Privatsphärenbedenken, Privatsphärenverletzung in der Vergangenheit, Gerätenutzung (Smartphone, Tablet), demografische Angaben (Alter, Bildung, etc.)

Abschluss der Befragung: Teilnahme Verlosung, Teilnahme an weiteren Studien

Dauer der Befragung: *MW* = 00:32:19 min

Befragungsteilnehmer

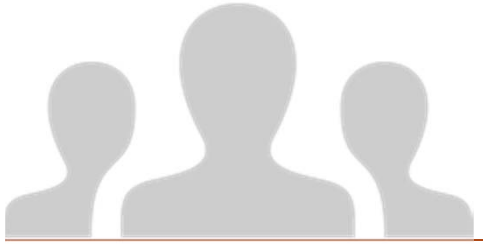
Vollständig ausgefüllte Fragebögen: *N* = 227

Alter: *MW* = 34,87 Jahre (*SD* = 12,22)

Geschlecht der Befragten: *n* = 81 weiblich (36%), *n* = 146 männlich (64%)

Höchster Schulabschluss (*n* = 227): überwiegend Fachhochschul- oder Hochschulreife (78%), Realschulabschluss (oder Gleichwertiges;13%)

Wirtschaftszweig (*n* = 146): Information und Kommunikation (21%), Freiberufliche, wissenschaftliche und technische Dienstleister (16%), Öffentliche Verwaltung, Verteidigung, Sozialversicherung (11%)

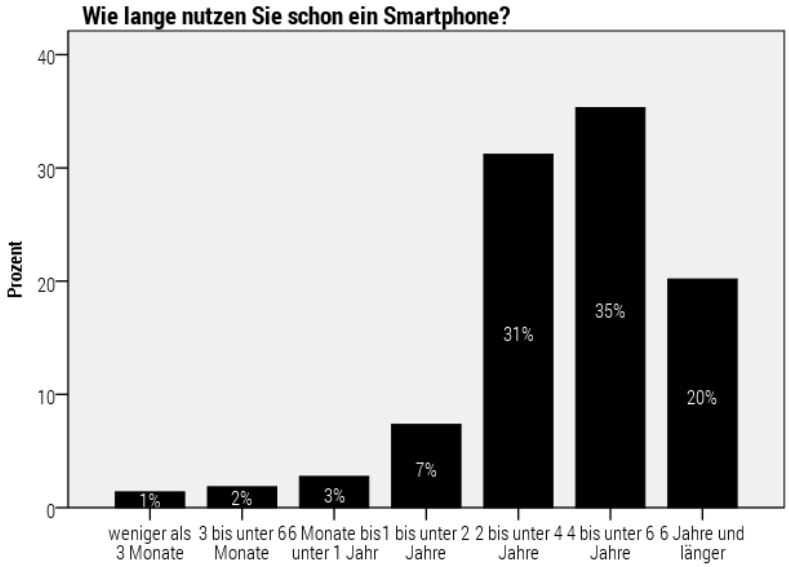


Befragungsteilnehmer
Smartphone-Nutzung (1/3)

Smartphone-Nutzung (*n* = 218):
am häufigsten seit 4-6 Jahren (35%), gefolgt von 2-4 Jahre (31%), und 6 Jahre und länger (20%)

Smartphone-Nutzung pro Tag (*n* = 218):
durchschnittlich ca. 2h pro Tag, schwankt jedoch stark (*MW* = 113,17; *SD* = 116,85)

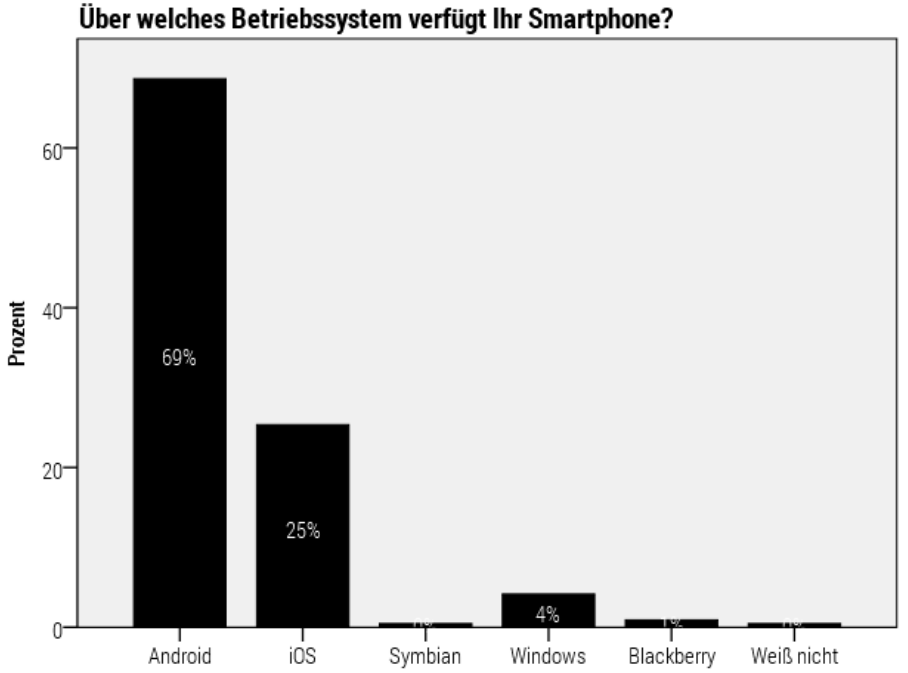
Dies entspricht der durchschnittlichen Nutzungszeit von 1h und 52 (appkind.de).



Befragungsteilnehmer
Smartphone-Nutzung (2/3)

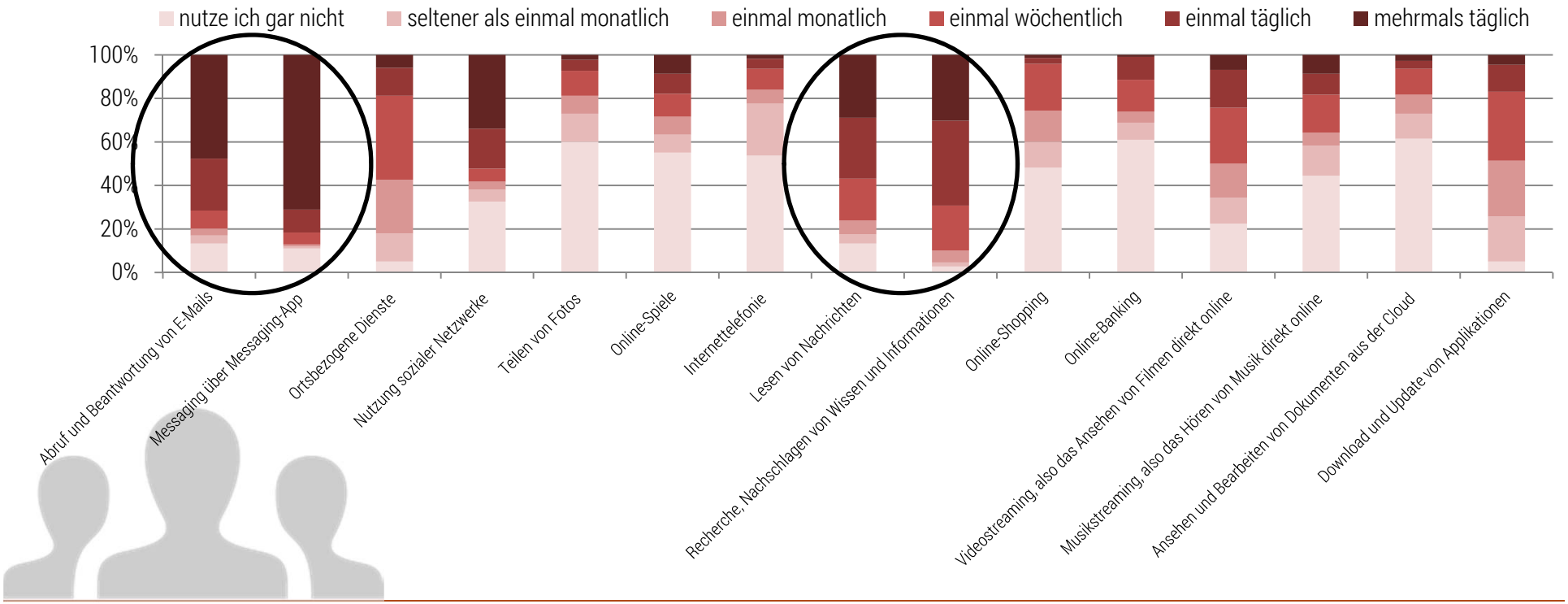
Verwendetes Smartphone Betriebssystem (*n* = 217): am häufigsten Android (69%), gefolgt von iOS (25%), und Windows (4%)

Dies entspricht der Reihenfolge der Marktanteile in Deutschland im Februar 2015 (statistica 2016)



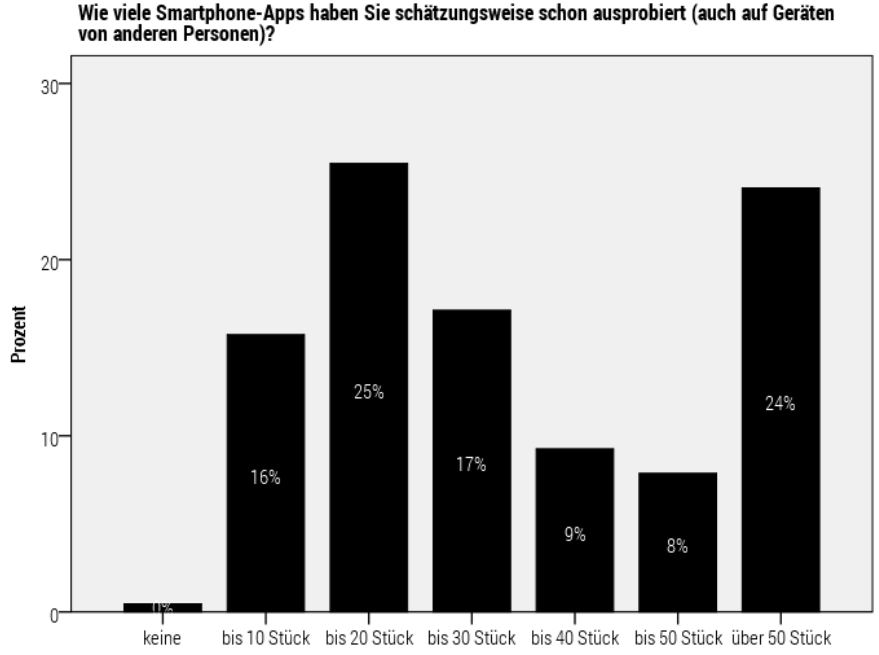
Befragungsteilnehmer
Smartphone-Nutzung (3/3)

Zweck Smartphone-Nutzung (*n* = 218): überwiegend für Kommunikations- und Recherchezwecke



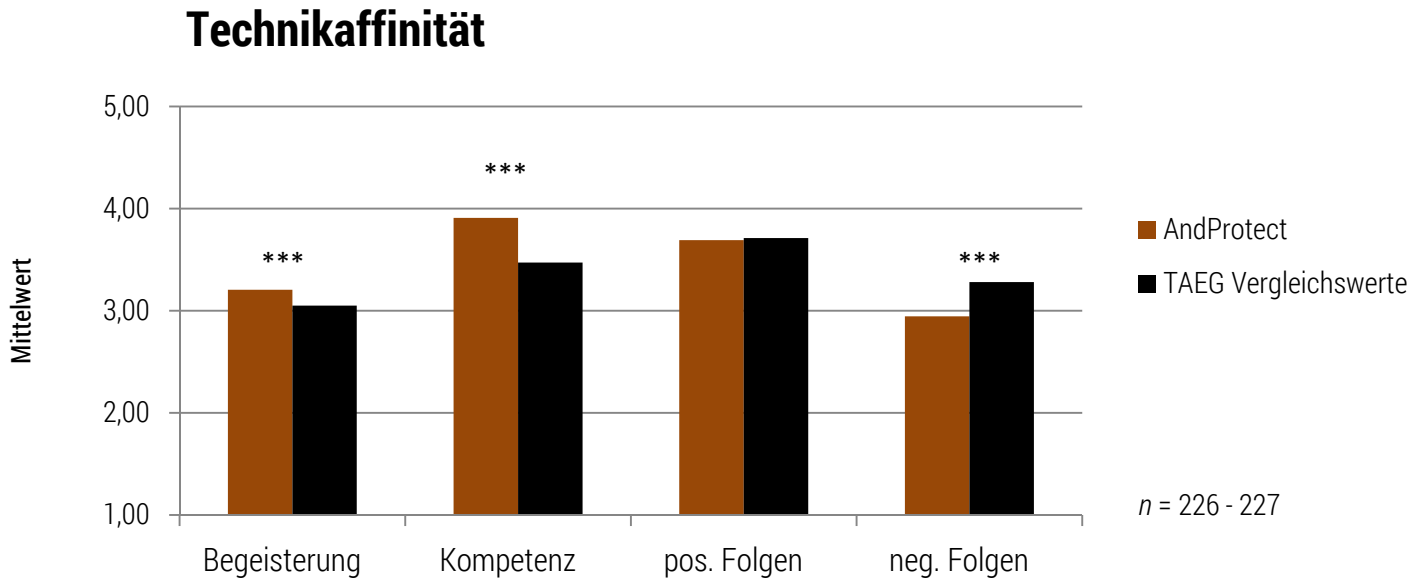
Befragungsteilnehmer
Nutzung von Smartphone-Apps

Smartphone-Apps (*n* = 216): zweigipflige Verteilung der Antworten - bis 20 Stück (25%) am häufigsten genannt, dicht gefolgt von 50 und mehr (24%).



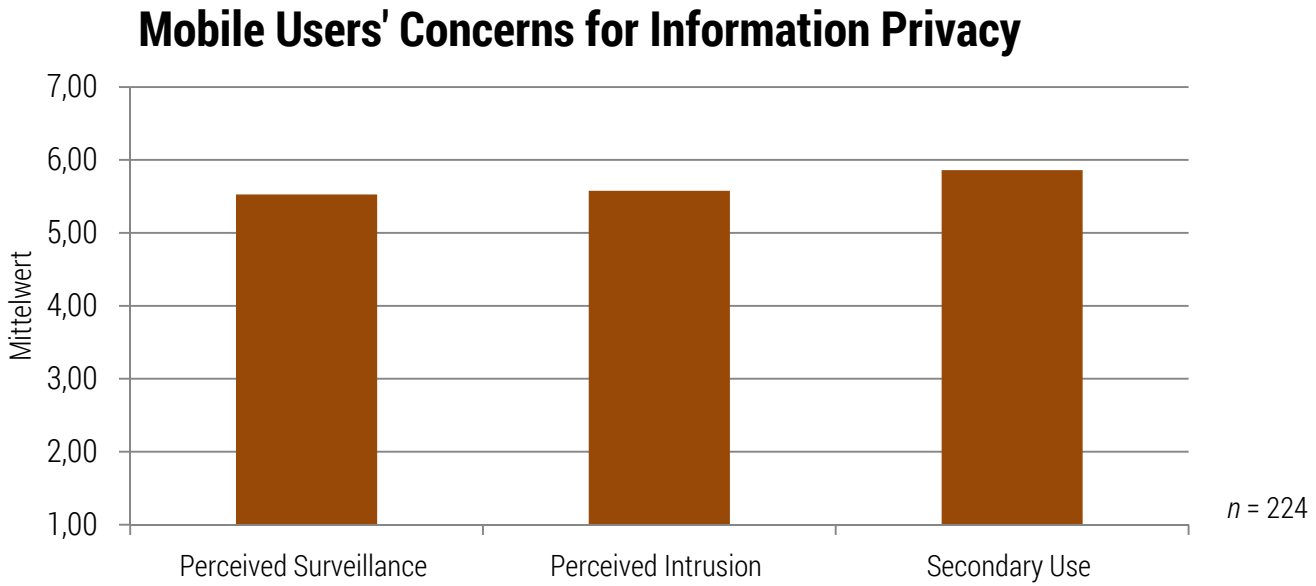
Befragungsteilnehmer
Technikaffinität

Die Befragten schätzen sich als technikaffin ein. Sie gaben an, signifikant begeisterter, kompetenter, und hinsichtlich der negativen Folgen weniger skeptisch zu sein als die Vergleichsstichprobe des Fragebogens (TAEG).



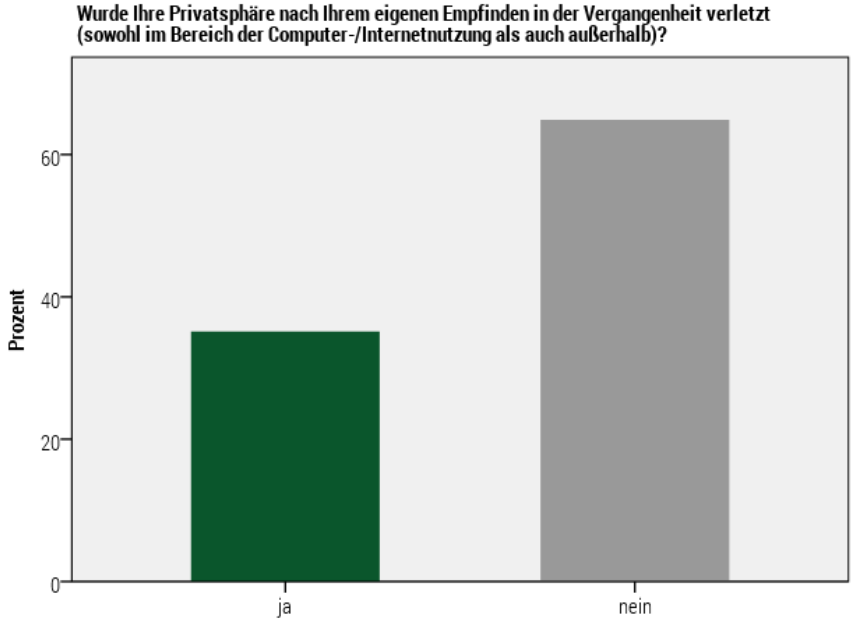
Befragungsteilnehmer
Privatsphärenbedenken im mobilen Bereich

Die Befragten schätzen sich als eher besorgt hinsichtlich der Wahrung ihrer Privatsphäre durch die Nutzung mobiler Apps ein. Besonders hinsichtlich der Weiterverwendung persönlicher Daten von Dritten geben die Befragten an besorgt zu sein.



Befragungsteilnehmer
Negative Erlebnisse (1/3)

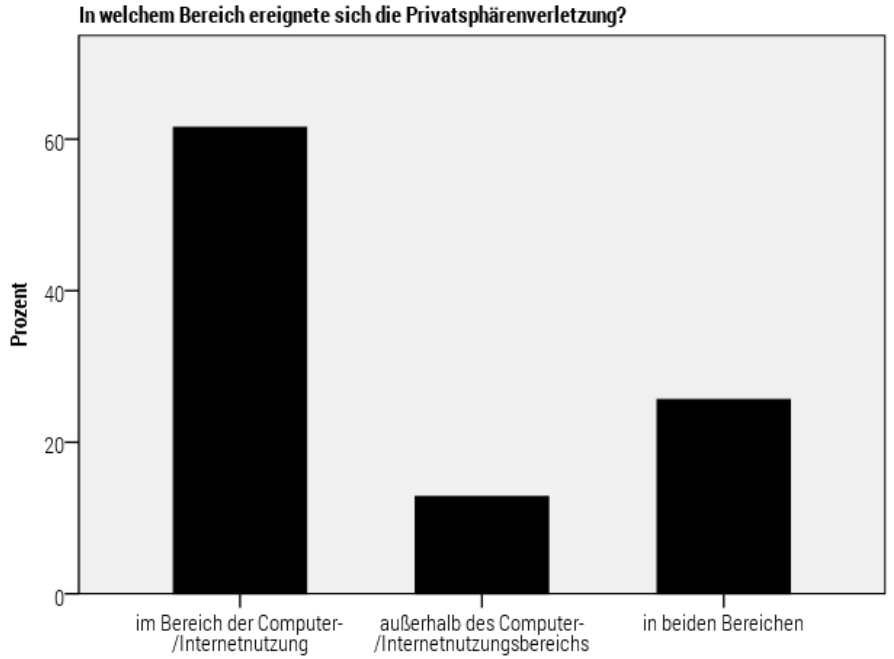
Verletzung der Privatsphäre (*n* = 222): der überwiegende Teil der Befragten (63%) gab an, keine negativen Erlebnisse in Bezug auf einen Privatsphärenverletzung in der Vergangenheit erlebt zu haben.



Befragungsteilnehmer
Negative Erlebnisse (2/3)

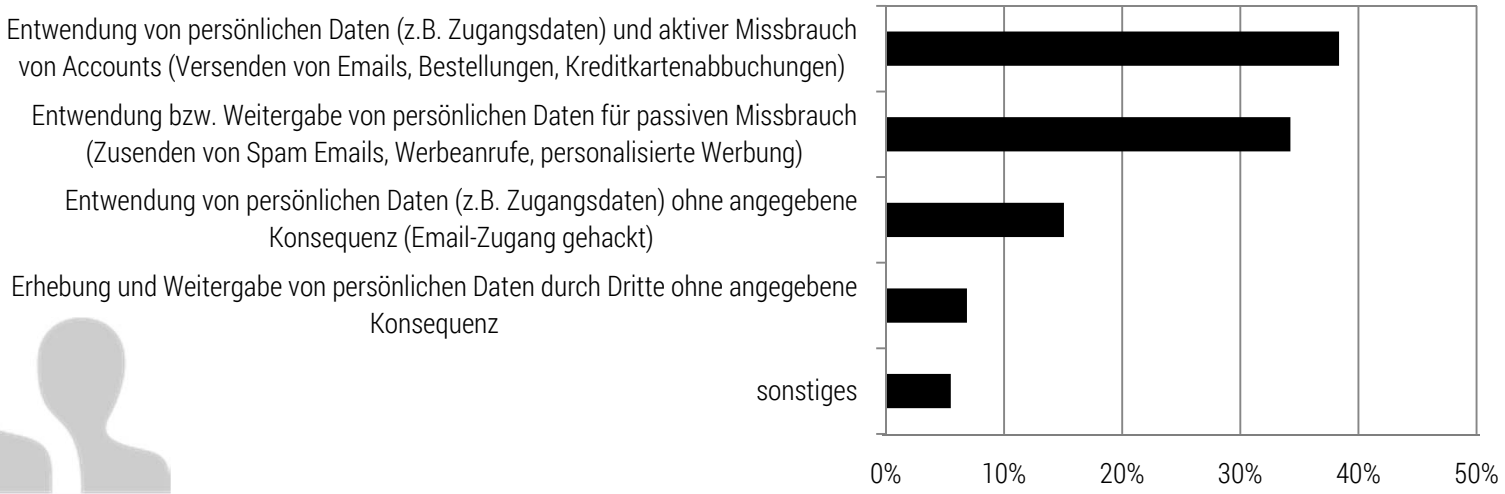
Verletzung der Privatsphäre (*n* = 78): sofern die Frage nach negativen Erlebnissen in Bezug auf die Privatsphäre bejaht wurde, konnten die Befragten den Bereich näher spezifizieren…

Der überwiegende Teil der Befragten (62%) gab an, dass die Privatsphäre im Bereich Computer/-Internetnutzung stattgefunden hätte.



Befragungsteilnehmer
Negative Erlebnisse (3/3)

Die Befragten hatten die Möglichkeit konkrete negative Erlebnisse zu schildern, in denen ihre Privatsphäre bzw. persönlich Daten missbraucht wurden. *n* = 62 Teilnehmer machten hier Angaben und erwähnten insgesamt 73 negative Ereignisse.
Am häufigsten (38%) wurden dabei Ereignisse beschrieben in denen persönliche Daten entwendet wurden und damit aktiver Missbrauch betrieben wurde, z.B. Email-Accounts gehackt wurden und anschließend darüber Spam-Mails verschickt wurden.



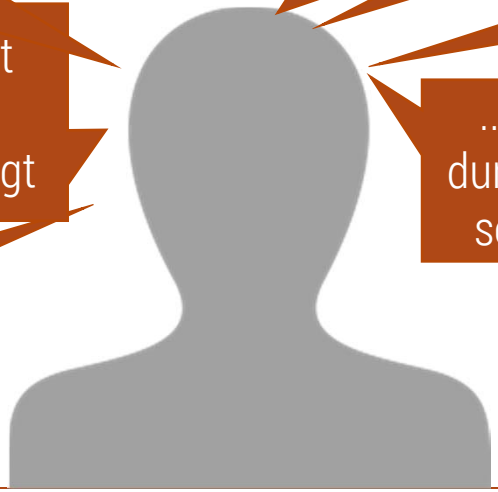
Wer hat die AndProtect-Befragung ausgefüllt?

Nutzt sein Android-Smartphone im Wesentlichen um von unterwegs aus Emails zu beantworten und mit Freunden zu chatten.

Hat seit 5 Jahren ein Smartphone und weit mehr als 50 Apps ausprobiert.

Hochschulstudium absolviert, jetzt Vollzeit in der Informations- und Kommunikationsbranche beschäftigt

Männlich, 35 Jahre



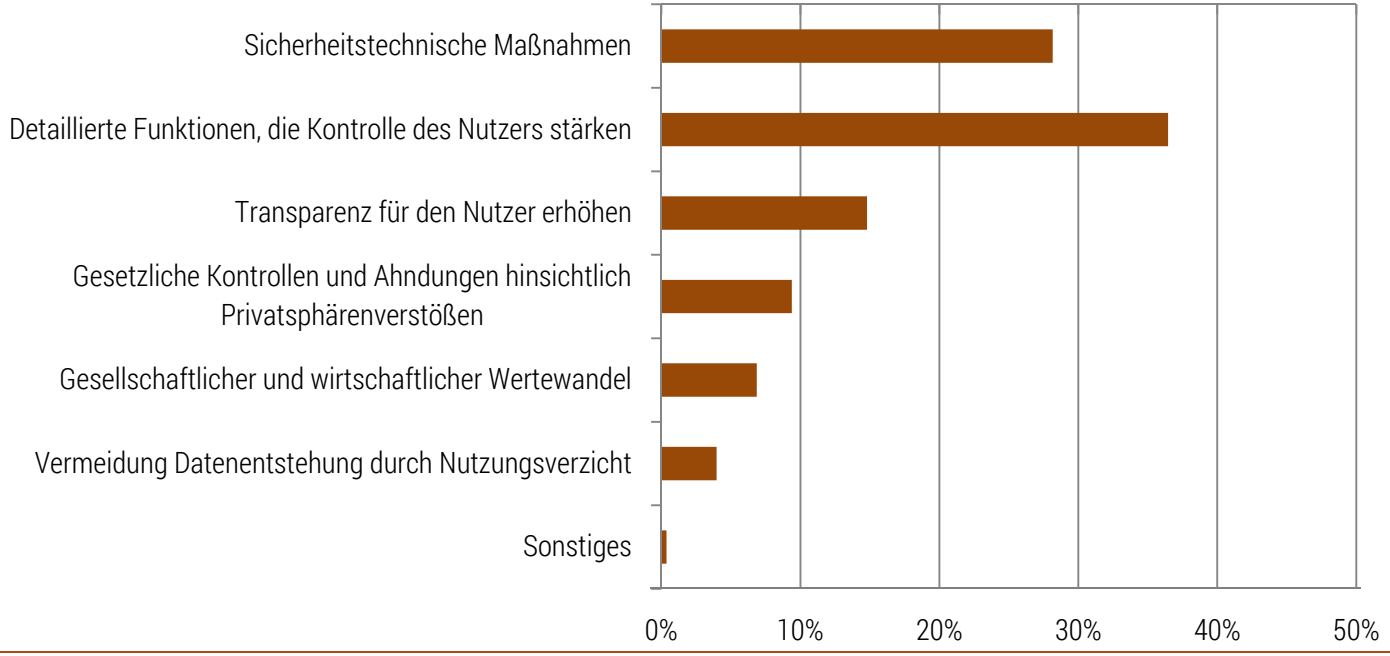
Ist technikaffin.

Ist sehr besorgt hinsichtlich seiner Privatsphäre…

…und hat v.a. Bedenken, dass Dritte durch die Nutzung von Apps Zugriff auf seine persönliche Daten bekommen.

Wünsche zur Verbesserung des Privatsphärenschutzes im mobilen Bereich

Am häufigsten (37% der Vorschläge) wünschten sich die Befragten mehr Funktionen um ihre Kontrolle über ihre Daten zu stärken, gefolgt von installierten sicherheitstechnischen Maßnahmen auf dem Smartphone (28% der Vorschläge) und Maßnahmen, die die Transparenz erhöhen (15% der Vorschläge).



Wünsche zur Verbesserung des Privatsphärenschutzes im mobilen Bereich

Sicherheitstechnische Maßnahmen
„[…] die app mit "pseudo-daten zu füttern"

Detaillierte Funktionen, die Kontrolle des Nutzers stärken
„Der Benutzer kann/muss selber bestimmen, welche Daten an wen weitergegeben werden (ausdrückliche Zustimmung; eigene Daten gehören dem Nutzer).“

Transparenz für den Nutzer erhöhen
„Anzeige von verständlichen Informationen über die Daten, auf die die App zugreift.[…] “

Gesetzliche Kontrollen und Ahndungen hinsichtlich Privatsphärenverstößen
„- mehr Firmen vor Gericht stellen, wenn sie Daten missbrauchen- strengere Gesetze- mehr Kontrollen- […] “

Gesellschaftlicher und wirtschaftlicher Wertewandel
„Andere Informationsgesellschaft. Momentan sind Großkonzerne und staatliche Institutionen im Sammelfieber. “

Vermeidung Datenentstehung durch Nutzungsverzicht
„ Verzicht auf App - Nutzung “

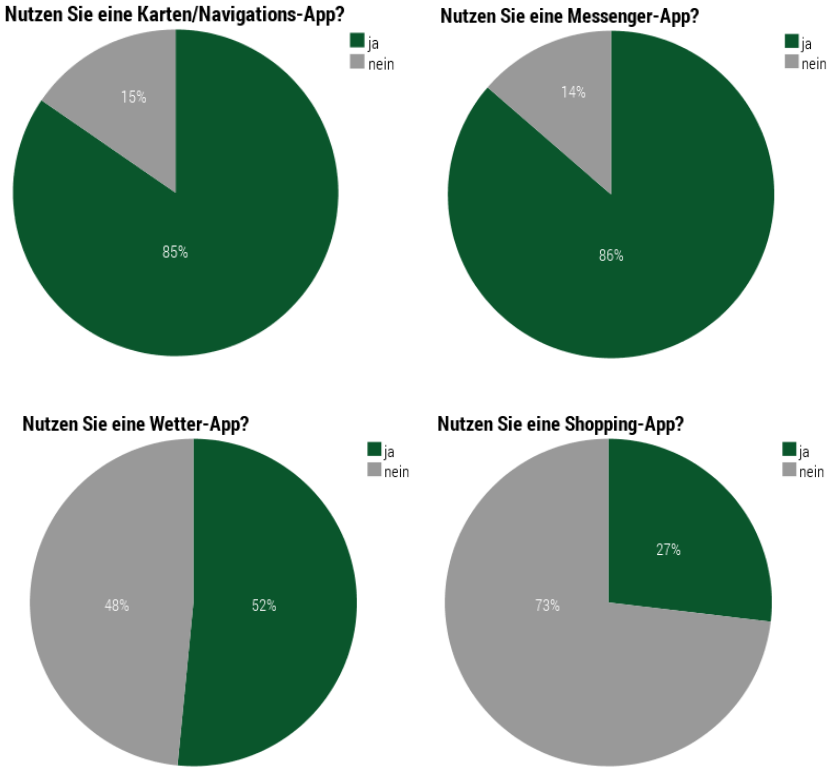
Sonstiges

Fazit Wünsche für Verbesserungen

Die qualitativen und kategorisierten Antworten zeigen, dass sich die Befragten am häufigsten wünschen aktive Mittel zur Verfügung zu haben (z.B. **Funktionen um ihre Kontrolle über ihre Daten zu stärken bzw. installierten sicherheitstechnischen Maßnahmen auf dem Smartphone**) um ihre Privatsphäre zu schützen .

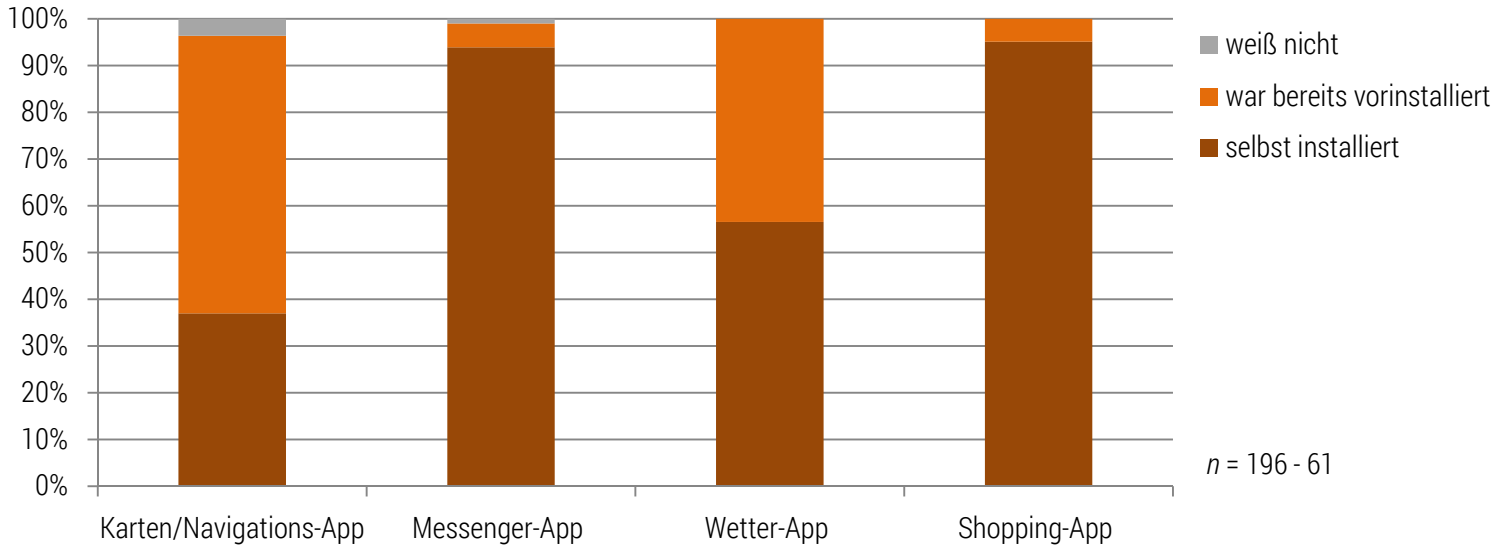
Nutzung verschiedener App-Gruppen

Die Befragten (*n* = 217) nutzten überwiegend die vorgegebenen App-Gruppen-Nutzung: Messenger-App (86%), Navigations-/Karten-App (85%), Wetter-App (52%). Lediglich die Shopping-App wurde nur von einem Drittel der Befragten genutzt: Shopping-App (27%).



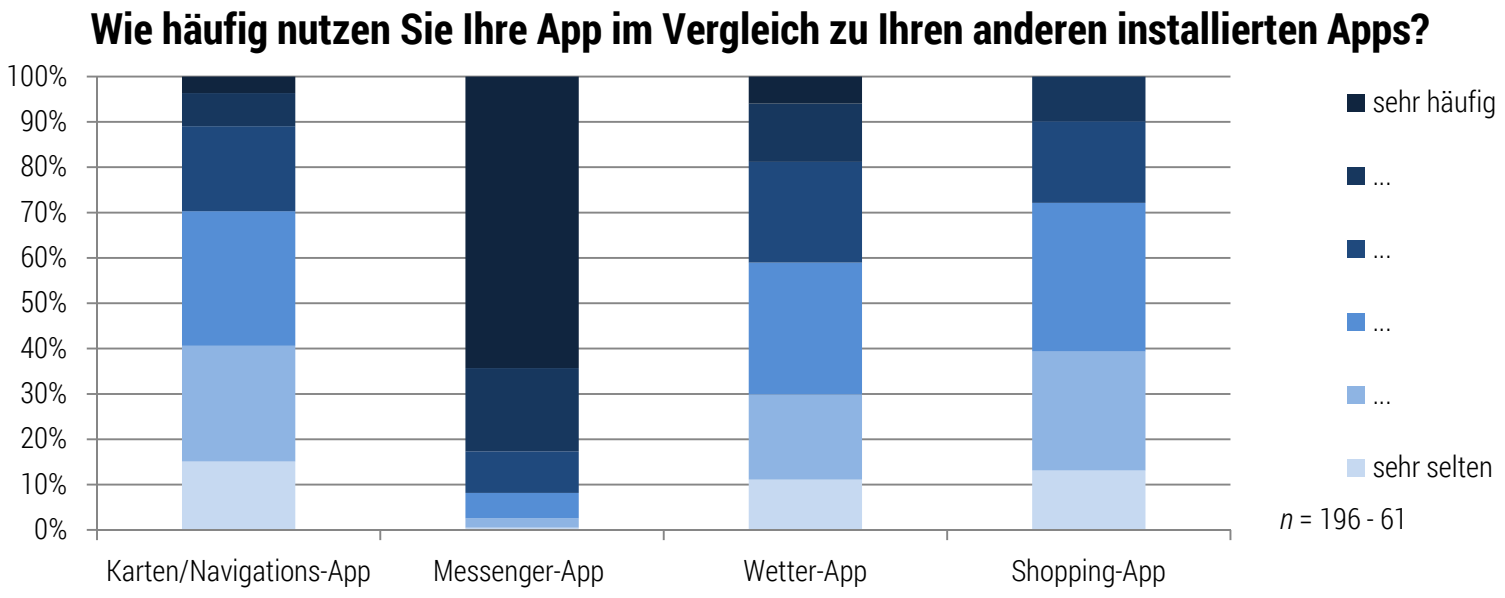
Installation verschiedener App-Gruppen

App-Gruppen-Installation: die Messenger-App (93%) und die Shopping-App (95%) wurden von den Befragten überwiegend selbst installiert.

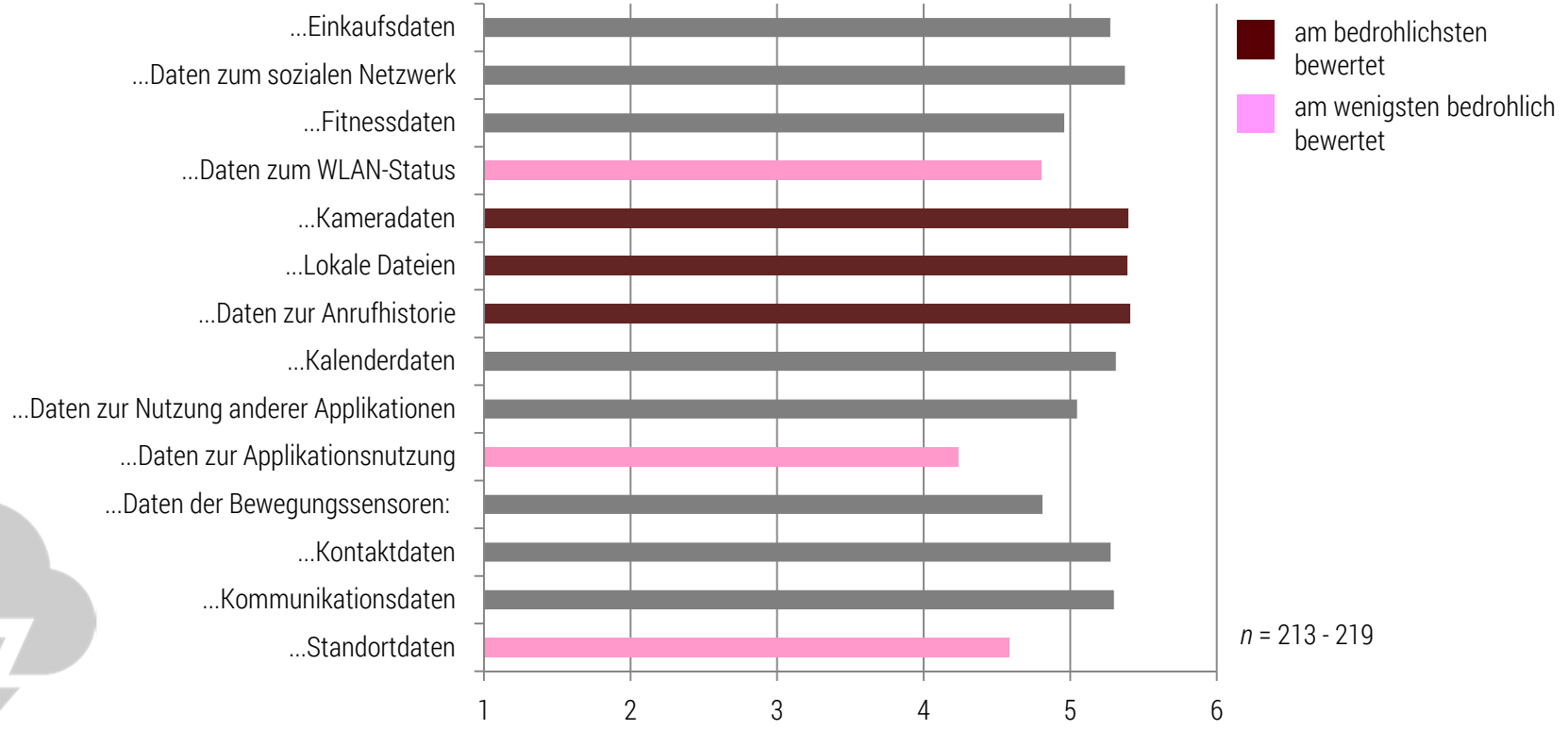


Nutzungshäufigkeit verschiedener App-Gruppen

App-Gruppen-Nutzungshäufigkeit: im Vergleich zu anderen Apps wird die Messenger-App (*MW* = 5,36; *SD* = 1,05) im Mittel „häufig“, die Wetter-App (*MW* = 3,25; *SD* = 1,36) sowie die Karten/Navigations-App (*MW* = 2,89; *SD* = 1,29) und die Shopping-App (*MW* = 2,85; *SD* = 1,17) „eher selten“ von den Befragten genutzt.

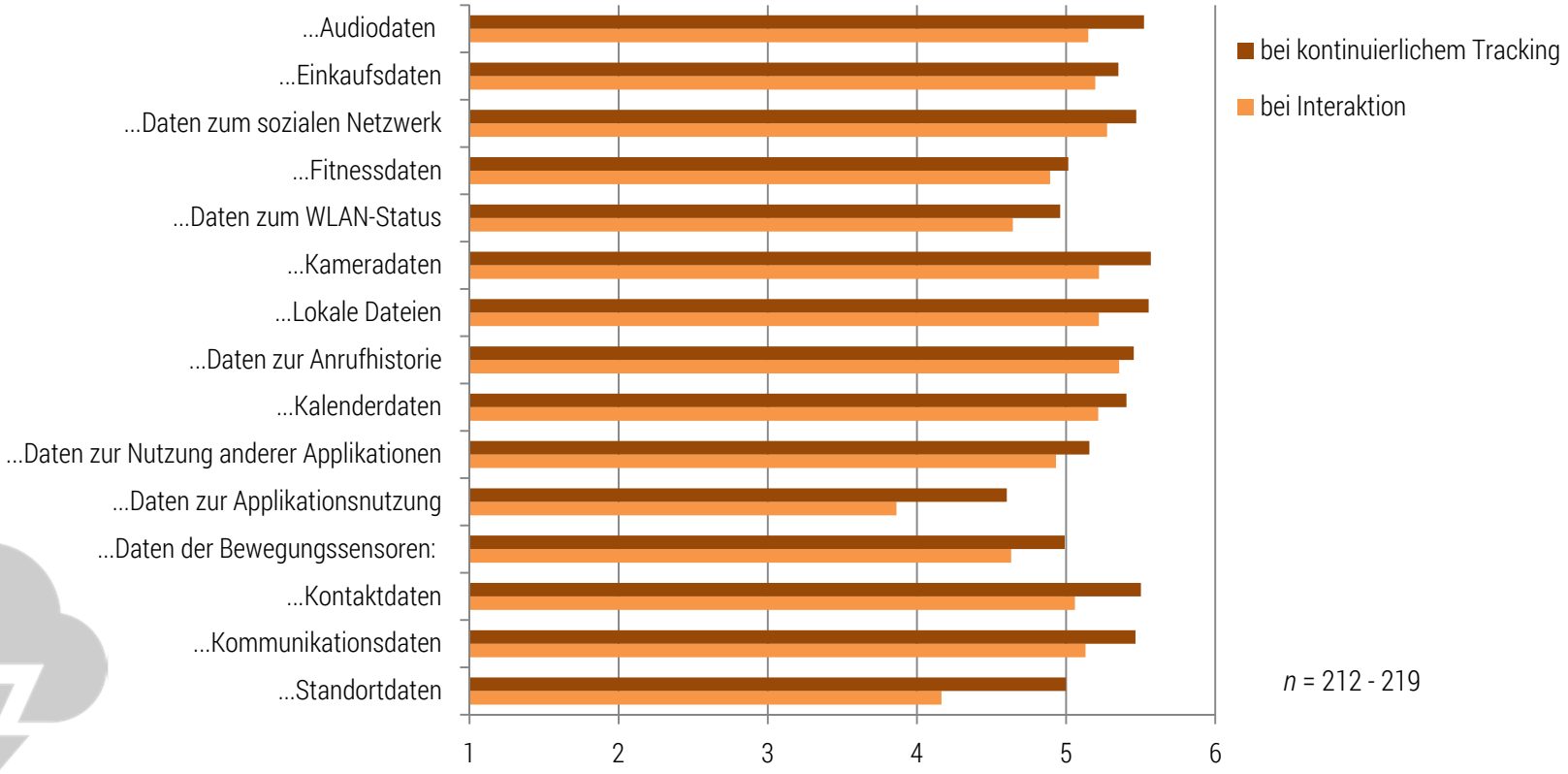


Wie bedrohlich ist die Erfassung unterschiedlicher Datenarten?



(1 = *stimmt gar nicht*, 2 = *stimmt weitgehend*, 3 = *stimmt eher nicht*, 4 = *stimmt eher*, 5 = *stimmt weitgehend*, 6 = *stimmt völlig*)

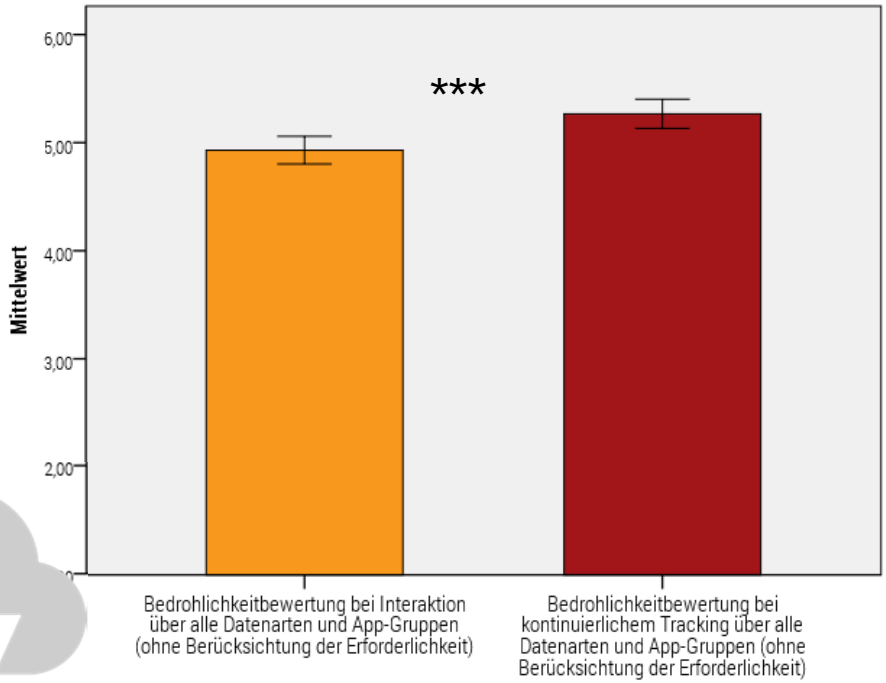
Wie bedrohlich ist die Erfassung unterschiedlicher Datenarten?



n = 212 - 219

(1 = *stimmt gar nicht*, 2 = *stimmt weitgehend*, 3 = *stimmt eher nicht*, 4 = *stimmt eher*, 5 = *stimmt weitgehend*, 6 = *stimmt völlig*)

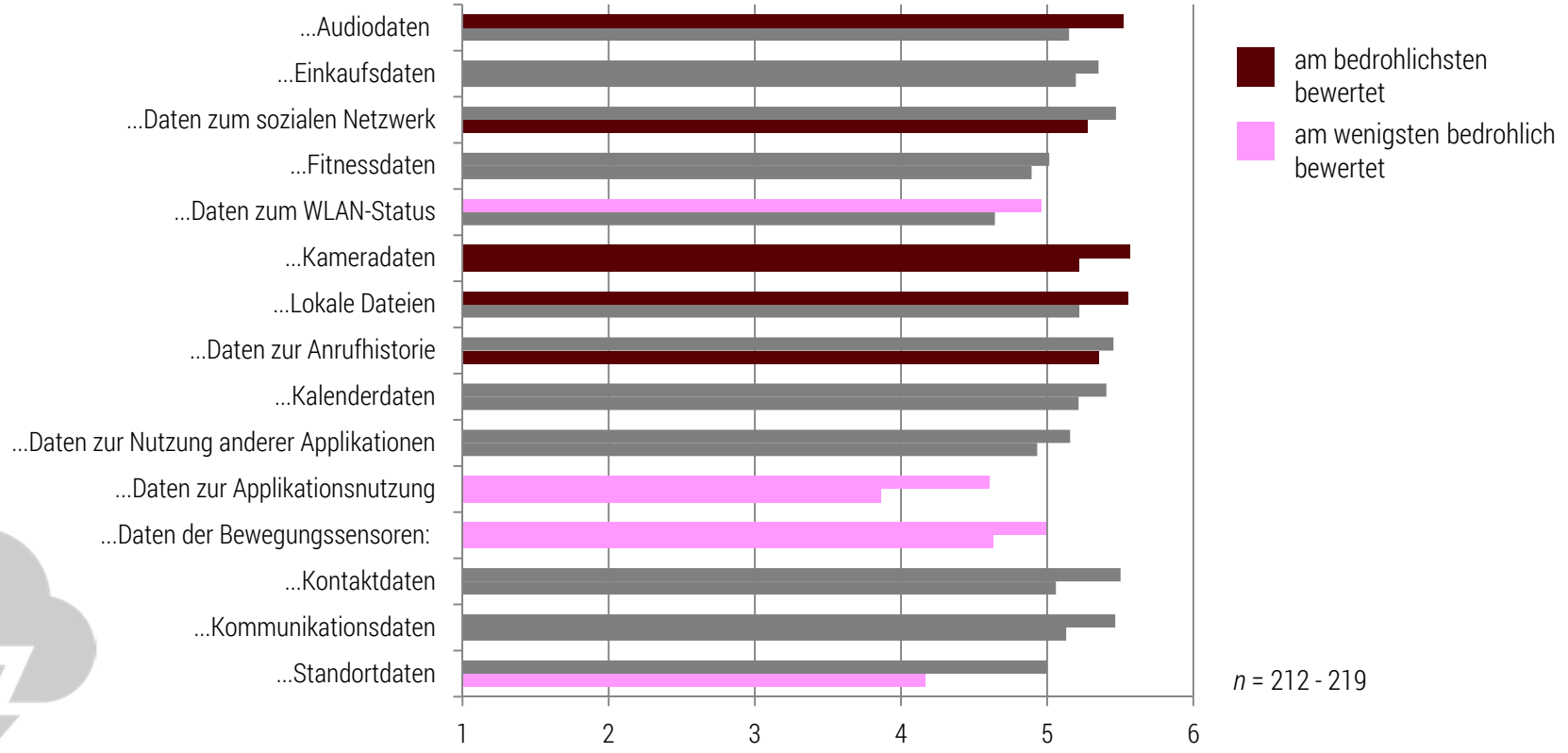
Wie bedrohlich ist die Erfassung unterschiedlicher Datenarten?



Der Unterschied der Bedrohlichkeitsbewertungen der Befragten zwischen der Datenverwendung bei Interaktion vs. kontinuierlichem Verwenden im Hintergrund ist statistisch hoch signifikant (z = 10,687; p = 0,000; r =0,72).

n = 219

Wie bedrohlich ist die Erfassung unterschiedlicher Datenarten?



(1 = *stimmt gar nicht*, 2 = *stimmt weitgehend*, 3 = *stimmt eher nicht*, 4 = *stimmt eher*, 5 = *stimmt weitgehend*, 6 = *stimmt völlig*)

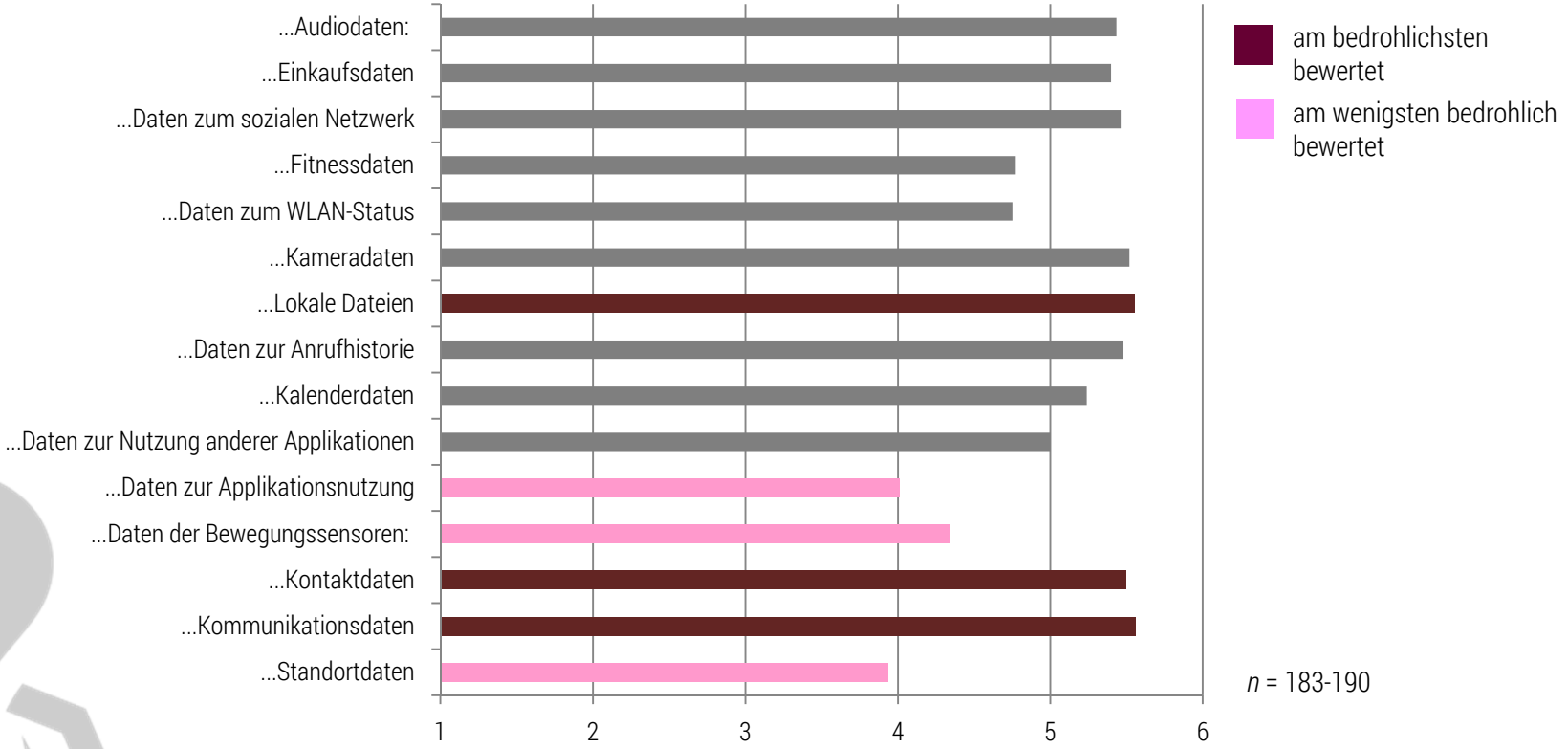
Fazit: Bedenken Datenarten

Bei dem überwiegenden Teil der präsentierten Datenarten stimmen die Befragten zu, ihre Privatsphäre als bedroht zu empfinden, wenn eine App diese Daten verwendet. Generell wird die **Verwendung von Audiodaten**, **Kommunikationsdaten**, und **Lokalen Dateien am kritischsten** bewertet. **Am wenigsten bedro**hlich bewerten die Befragten **Daten zur Applikationsnutzung**, **Daten von Bewegungssensoren** und **Standortdaten**.

Die Befragten bewerten **das kontinuierliche Verwenden** der präsentierten Datenarten als **deutlich bedrohlicher** als das Verwendung dieser Daten bei Interaktion mit einer App. Verwendet bei Interaktion eine Karten- bzw. Messenger-App die präsentierten Datenarten, geben die Befragten an ihre Privatsphäre deutlich weniger bedroht zu empfinden, als das bei Wetter- oder Shopping-Apps der Fall ist.

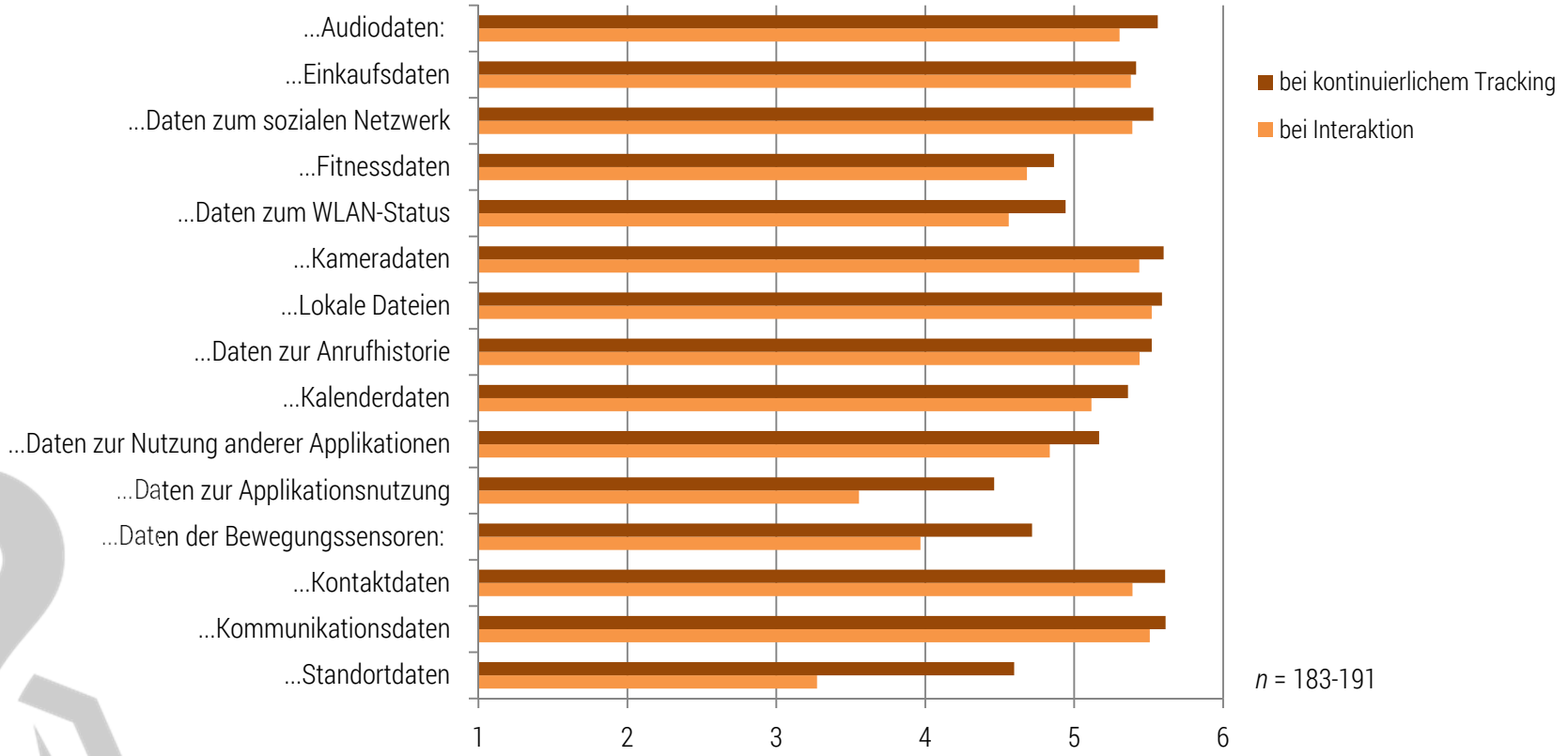
Bei kontinuierlicher Verwendung der präsentierten Daten lassen sich nur schwache Unterschiede zwischen der Karten-App und allen anderen App-Gruppen feststellen. Hier gaben die Befragten an, dass die kontinuierliche Verwendung der präsentierten Datenarten bei Karten-Apps für die Befragten geringfügig weniger bedrohlicher ist als bei Messenger, Wetter- , und Shopping-Apps.

Karten/Navigations-App



(1 = *stimmt gar nicht*, 2 = *stimmt weitgehend*, 3 = *stimmt eher nicht*, 4 = *stimmt eher*, 5 = *stimmt weitgehend*, 6 = *stimmt völlig*)

Karten/Navigations-App

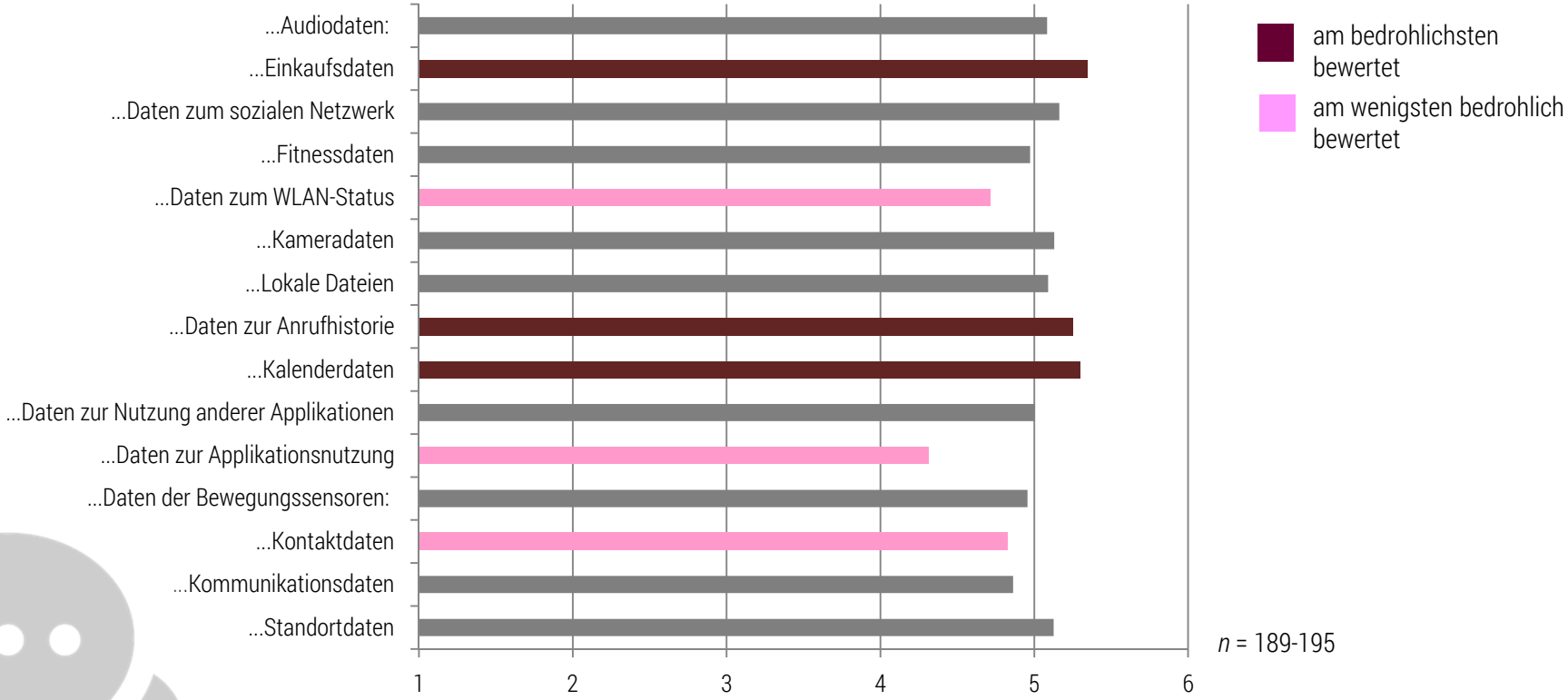


(1 = *stimmt gar nicht*, 2 = *stimmt weitgehend*, 3 = *stimmt eher nicht*, 4 = *stimmt eher*, 5 = *stimmt weitgehend*, 6 = *stimmt völlig*)

Zwischenfazit: Karten/Navigations-App

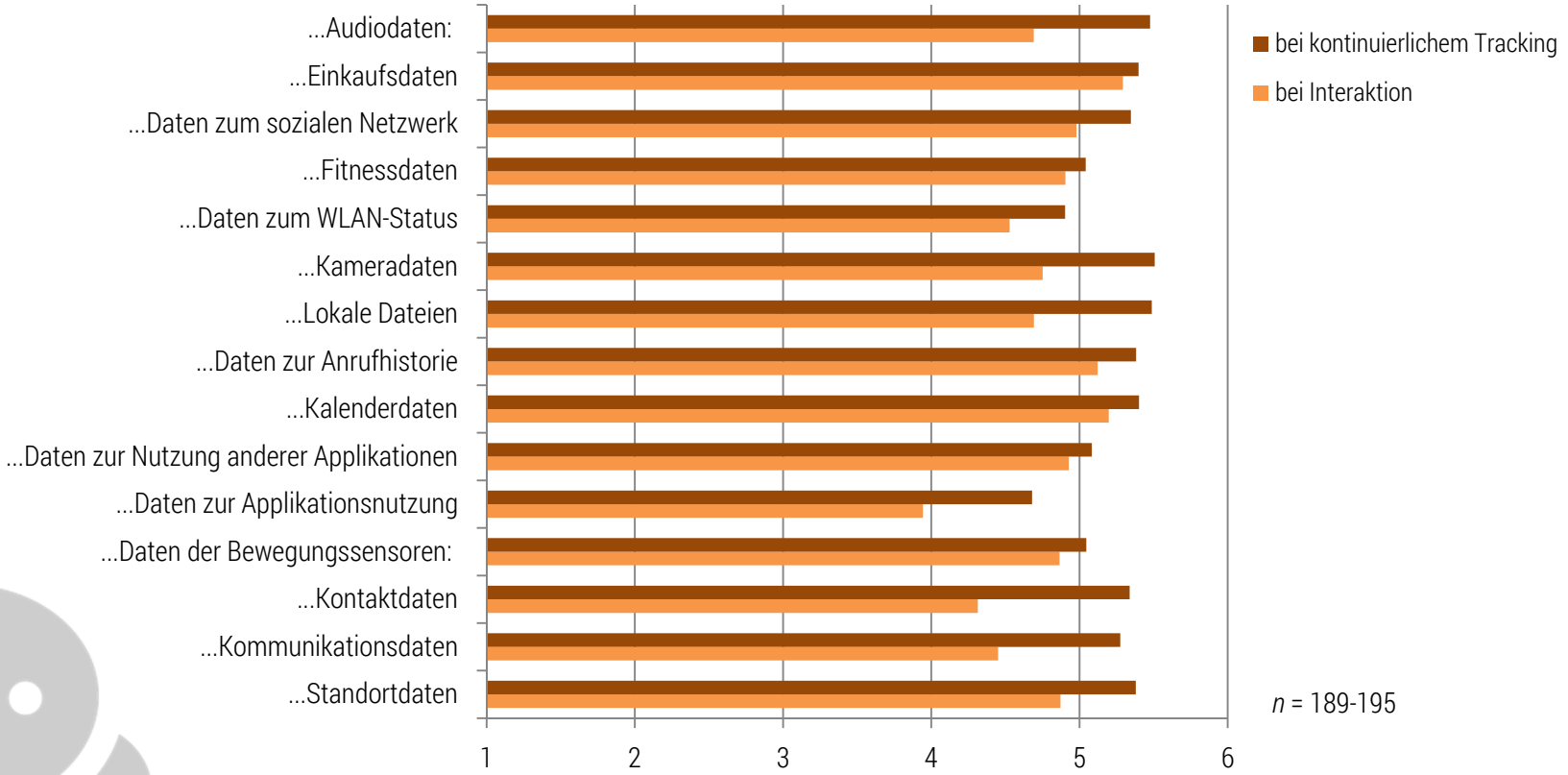
Die Befragten bewerten die Verwendung von **Kommunikationsdaten sowie lokalen Dateien am bedrohlichsten** für die eigene Privatsphäre. **Standortdaten** werden dagegen als **am wenigsten bedrohlich** eingeschätzt. An dieser Einschätzung verändert sich nur wenig im Falle der Verwendung bei Interaktion bzw. kontinuierlicher Verwendung im Hintergrund.
Allerdings zeigt sich auch für die Karten/Navigations-App ein deutlicher Unterschied hinsichtlich der Bedrohlichkeitsbewertungen für alle Datenarten bei Interaktion vs. kontinuierlichem Tracking. Auch hier bewerten die Befragten das kontinuierliche Verwenden von Daten im Hintergrund durch eine Karten/Navigations-App als bedrohlicher.
Die Nutzungshäufigkeit bzw. Wichtigkeit der Karten/Navigations-App hängt dabei nicht mit den Bedrohlichkeitsbewertungen zusammen.

Messenger-App



(1 = *stimmt gar nicht*, 2 = *stimmt weitgehend*, 3 = *stimmt eher nicht*, 4 = *stimmt eher*, 5 = *stimmt weitgehend*, 6 = *stimmt völlig*)

Messenger-App



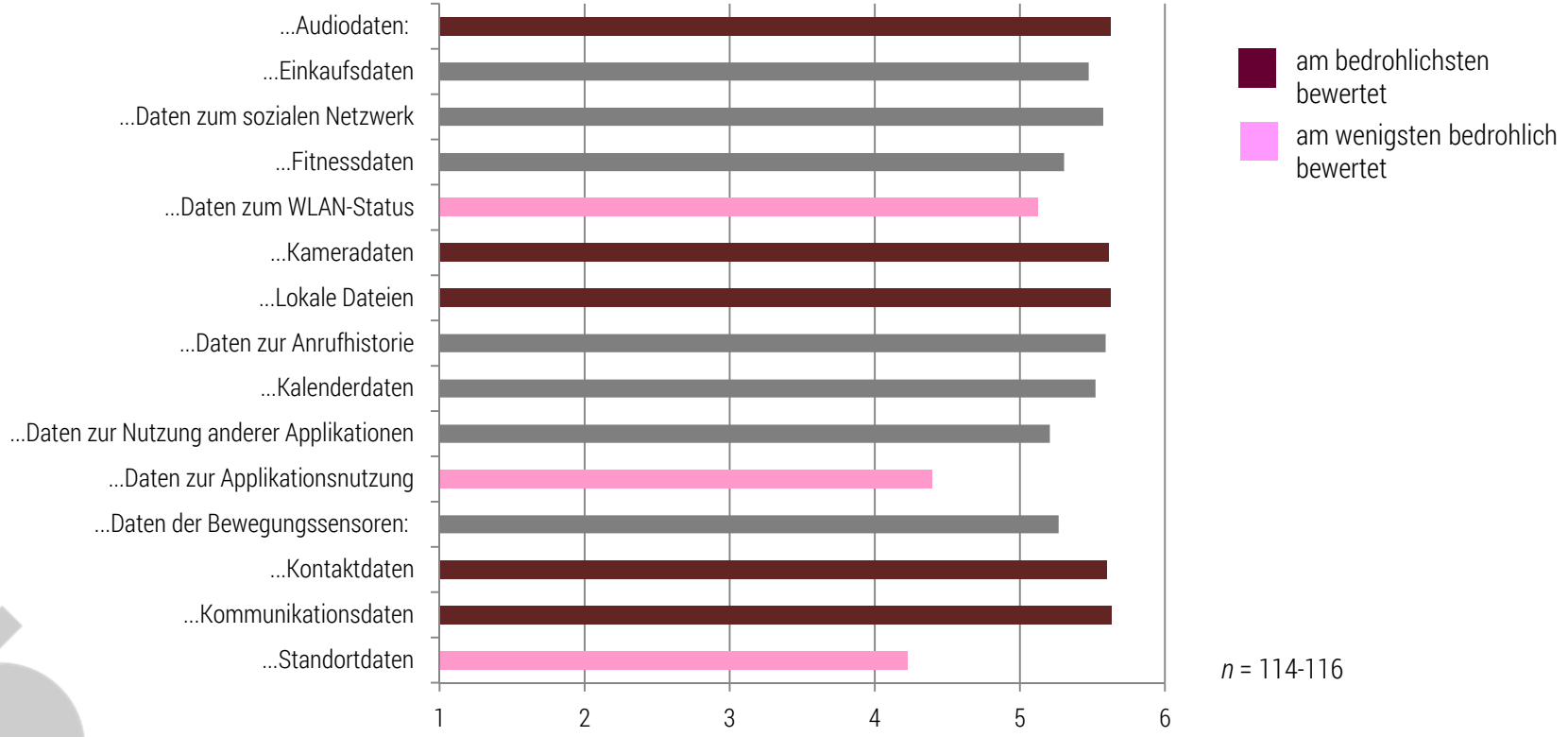
(1 = *stimmt gar nicht*, 2 = *stimmt weitgehend*, 3 = *stimmt eher nicht*, 4 = *stimmt eher*, 5 = *stimmt weitgehend*, 6 = *stimmt völlig*)

Zwischenfazit: Messenger-App

Die Befragten bewerten die Verwendung von **Einkaufsdaten am bedrohlichsten** für die eigene Privatsphäre. **Daten zu Applikationsnutzung** werden dagegen als **am wenigsten bedrohlich** eingeschätzt. An dieser Einschätzung verändert sich nur wenig im Falle der Verwendung bei Interaktion bzw. kontinuierlicher Verwendung im Hintergrund. Allerdings zeigt sich auch für die Messenger -App ein deutlicher Unterschied hinsichtlich der Bedrohlichkeitsbewertungen für alle Datenarten bei Interaktion vs. kontinuierlichem Tracking. Auch hier bewerten die Befragten das kontinuierliche Verwenden von Daten im Hintergrund durch eine Messenger-App als bedrohlicher.

Die Nutzungshäufigkeit bzw. Wichtigkeit der Messenger-App hängt dabei nicht mit den Bedrohlichkeitsbewertungen zusammen.

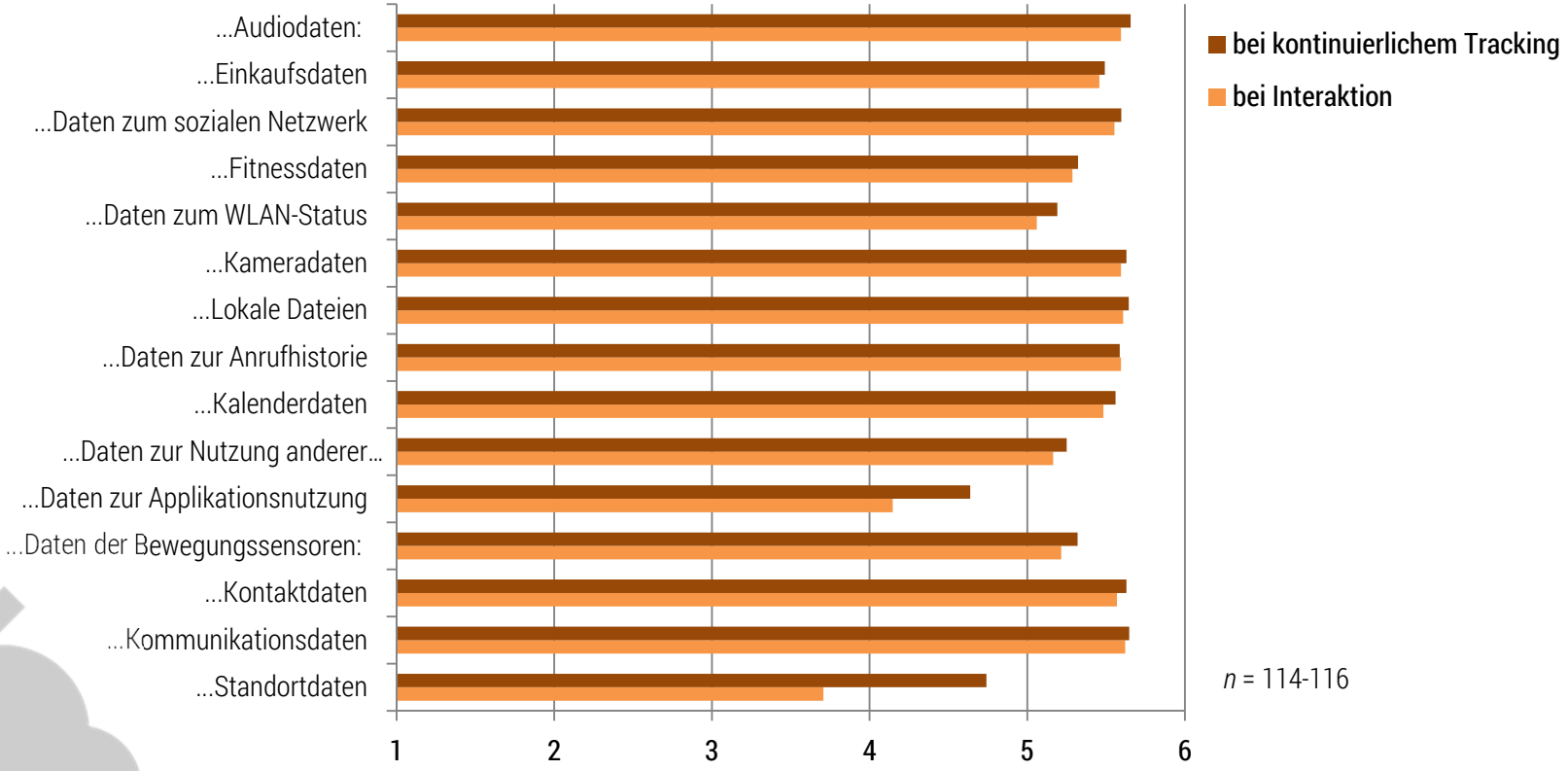
Wetter-App



n = 114-116

(1 = *stimmt gar nicht*, 2 = *stimmt weitgehend*, 3 = *stimmt eher nicht*, 4 = *stimmt eher*, 5 = *stimmt weitgehend*, 6 = *stimmt völlig*)

Wetter-App

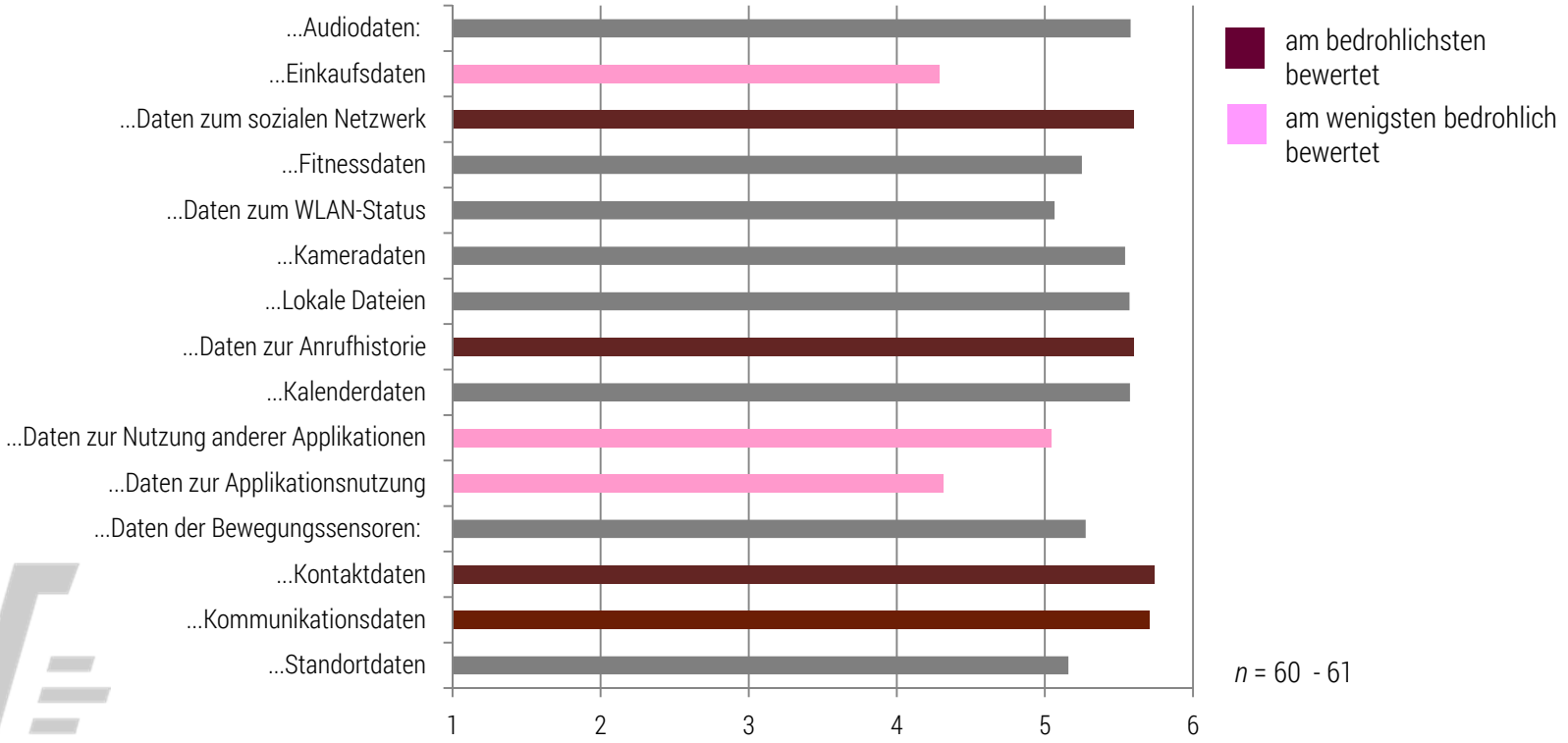


(1 = *stimmt gar nicht*, 2 = *stimmt weitgehend*, 3 = *stimmt eher nicht*, 4 = *stimmt eher*, 5 = *stimmt weitgehend*, 6 = *stimmt völlig*)

Zwischenfazit: Wetter-App

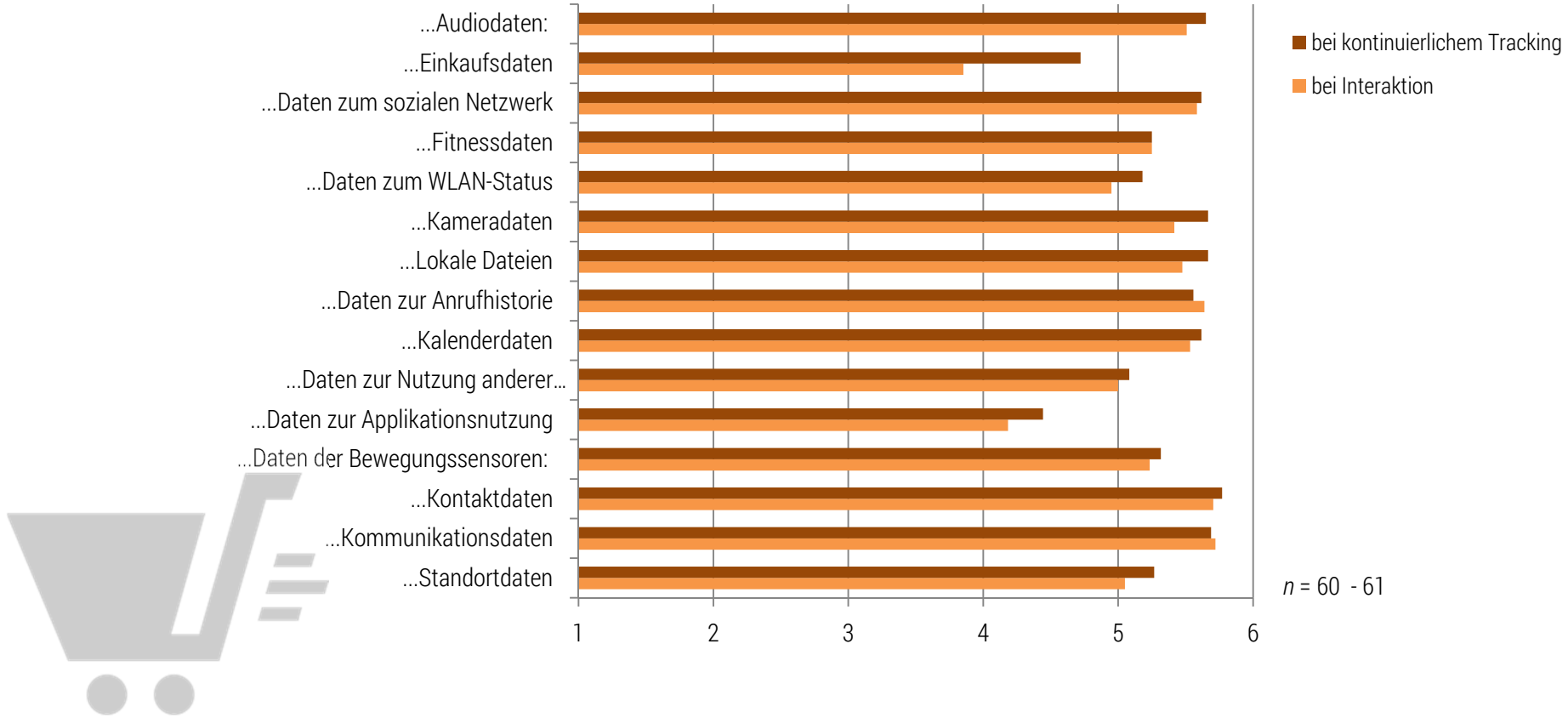
Die Befragten bewerten die Verwendung von **lokalen Dateien, Kommunikationsdaten und Audiodaten** für die eigene Privatsphäre. **Standortdaten** werden dagegen als **am wenigsten bedrohlich** eingeschätzt. An dieser Einschätzung verändert sich nur wenig im Falle der Verwendung bei Interaktion bzw. kontinuierlicher Verwendung im Hintergrund.
Allerdings zeigt sich auch für die Wetter-App ein deutlicher Unterschied hinsichtlich der Bedrohlichkeitsbewertungen für alle Datenarten bei Interaktion vs. kontinuierlichem Tracking.
Die Nutzungshäufigkeit bzw. Wichtigkeit der Wetter-App hängt dabei erneut nicht mit den Bedrohlichkeitsbewertungen zusammen.

Shopping-App



(1 = *stimmt gar nicht*, 2 = *stimmt weitgehend*, 3 = *stimmt eher nicht*, 4 = *stimmt eher*, 5 = *stimmt weitgehend*, 6 = *stimmt völlig*)

Shopping-App



(1 = *stimmt gar nicht*, 2 = *stimmt weitgehend*, 3 = *stimmt eher nicht*, 4 = *stimmt eher*, 5 = *stimmt weitgehend*, 6 = *stimmt völlig*)

Zwischenfazit: Shopping-App

Die Befragten **Amazon** bewerten die Verwendung von **Kontaktdaten am bedrohlichsten** für die eigene Privatsphäre. **Einkaufsdaten** werden dagegen als **am wenigsten bedrohlich** eingeschätzt. An dieser Einschätzung verändert sich nur wenig im Falle der Verwendung bei Interaktion bzw. kontinuierlicher Verwendung im Hintergrund.
Allerdings zeigt erneut auch für die Shopping-App ein deutlicher Unterschied hinsichtlich der Bedrohlichkeitsbewertungen für alle Datenarten bei Interaktion vs. kontinuierlichem Tracking.
Die Nutzungshäufigkeit bzw. Wichtigkeit der Shopping-App hängt dabei erneut nicht mit den Bedrohlichkeitsbewertungen zusammen.

Fazit: App-Gruppen

Für alle App-Gruppen separat wird **das kontinuierliche Verwenden** der präsentierten Daten als **bedrohlicher für die eigene Privatsphäre** empfunden **als** die Verwendung der präsentierten Daten **bei Interaktion**.

Die jeweils am bedrohlichsten und am wenigsten bedrohlichen Datenarten variieren von App-Gruppe zu App-Gruppe. Dies lässt darauf schließen, dass die Befragten „ein gewisses Gespür" für die Erforderlichkeit der Datenarten für die Verwendung haben (Testung siehe folgende Folien). So bewerten sie scheinbar ihre Privatsphäre als weniger bedroht, wenn eine App erforderliche Datenarten erfasst (Testung siehe folgende Folien).

Es besteht überwiegend **kein Zusammenhang zwischen der Nutzungshäufigkeit**, der **Wichtigkeit** der jeweiligen App, **und den Bedrohlichkeitsbewertungen** der Befragten. Dies bedeutet, dass die wahrgenommene Bedrohung der Privatsphäre unabhängig von der jeweiligen „Bedeutsamkeit der App" ist.

Erforderlichkeit der Datenarten für App-Gruppen

Die Einschätzung hinsichtlich der Erforderlichkeit der 15 Datenarten wurde anhand von drei Kategorien vorgenommen:

1 = Ja; Daten sind erforderlich um grundlegende Funktionalitäten der Apps aus dieser Gruppe zu gewährleisten
2 = Zum Teil; Daten sind für bestimmte zusätzliche Funktionen einzelner Apps dieser App-Gruppe erforderlich
3 = Nein; Daten sind nicht erforderlich um grundlegende oder zusätzliche Funktionen von Apps aus dieser Gruppe zu gewährleisten

Die Übereinstimmung der Bewertungen (Interraterreliabiltät) der zwei Expertengruppen (Projektpartner AndProtect und AVARE) variierte zunächst stark zwischen den App-Gruppen:

„Genügende Übereinstimmung“* für Karten/Navigations-App (K = 0,477; p = 0,019)
„Ungenügende Übereinstimmung“* für Messenger-App (K = 0,342; p = 0,060)
„Sehr gute Übereinstimmung“* für Wetter-App (K = 1,000; p = 0,000)
„Sehr gute Übereinstimmung“* Shopping-App (K = 1,00; p = 0,000)

Erforderlichkeit der Datenarten für App-Gruppen

Im Folgenden wurden die Urteile der zwei Gruppen iteriert und eine Konsenslösung generiert (siehe Tabelle), die für die folgenden Auswertungen zugrunde gelegt wurde.

Datenart	Erklärung für Probanden	Karten-App	Messenger-App	Wetter-App	Shopping-App
Standortdaten	Information wo ich mich aktuell befinde.	1	2	2	3
Kommunikationsdaten	Dialoge, die ich mit anderen Personen führe in Form von Text-, Bild-, Video- oder Audionachrichten	3	1	3	3
Kontaktdaten	Meine im Adressbuch gespeicherten Kontaktinformationen (z.B. Vorname, Nachname, Telefonnummern und E-Mail-Adresse des Kontaktes)	2	1	3	3
Daten der Bewegungssensoren	Welche Bewegungen ich ausführe (z.B. Treppensteigen, Rennen, Gehen)	1	3	3	3
Daten zur Applikationsnutzung	Wann und wie häufig ich meine [Gruppe]-App nutze	3	3	3	3
Daten zur Nutzung anderer Applikationen:	Welche anderen Apps ich installiert habe	3	3	3	3
Kalenderdaten	Welche Termine (Inhalt und Zeit) ich mir eingetragen habe.	3	3	3	3
Daten zur Anrufhistorie	Mit wem ich wann telefoniert habe	3	3	3	3
Lokale Dateien	Dateien, die auf meinem Mobiltelefon gespeichert sind (z.B. Fotos, Audioaufzeichnungen, Download-Dateien aus Browser)	3	2	3	3
Kameradaten	Bilder die im Fokus meiner Handykamera sind	3	2	3	3
WLAN-Status	Informationen in welchem WLAN ich gerade eingeloggt bin, ob ich mein aktuell genutztes WLAN schon zuvor benutzt habe, welche WLANs ich registiert habe und/oder welche WLANs mein Gerät sucht.	3	3	3	3
Fitnessdaten	Informationen über meine physischen Aktivitäten (z.B. Schrittzähler, Herzfrequenz, Schlafphasen).	3	3	3	3
Daten zum sozialen Netzwerk	Informationen wen ich kenne, z.B. die Namen meiner Kontakte, Zugriff auf persönliche Daten von meinen Kontakten (Pinnwand, Bilder, Status der Person) sowie meine Daten (identisch, aber ohne Beschränkungen des Zugriffs).	3	3	3	3
Einkaufs-Daten	Informationen welche Produkte ich beobachte, welche Produkte ich gekauft habe, welche Zahlungsmittel und Lieferadressen ich verwende.	3	3	3	1
Audiodaten	Ton, den mein Smartphone-Mikrofon aufnimmt	3	2	3	3

Erforderlichkeit der Datenarten für App-Gruppen

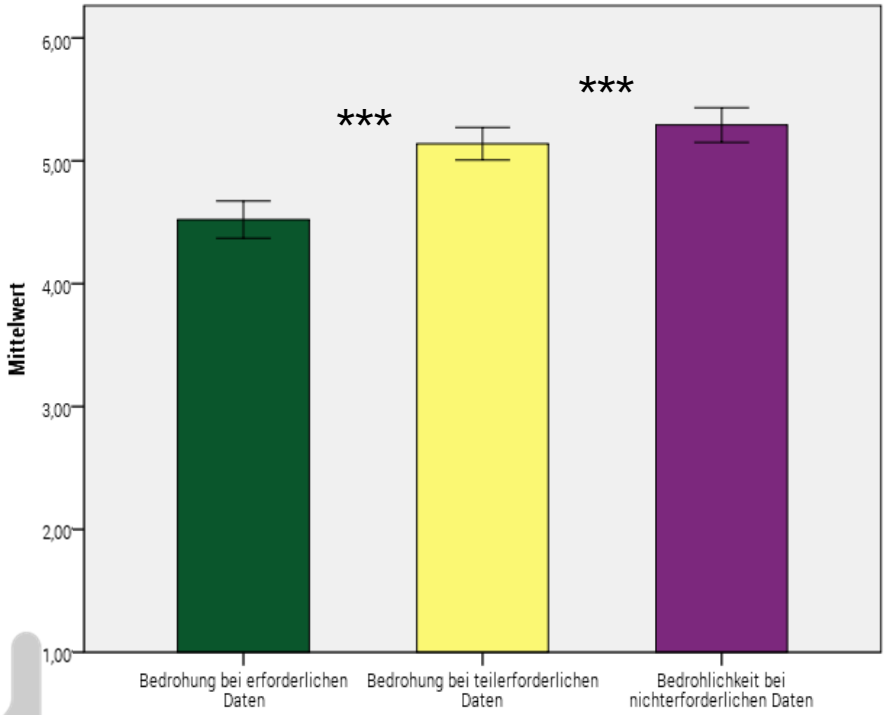
Zunächst wurden alle Bewertungen der Befragten hinsichtlich der Bedrohlichkeit für die eigene Privatsphäre für ‚erforderliche', ‚zum Teil erforderliche', und ‚nicht erforderliche' Daten (unabhängig von der App-Gruppe) gemittelt und verglichen.

Erforderliche Daten wurden erwartungskonform am wenigsten bedrohlich für die eigene Privatsphäre eingeschätzt (*MW* = 4,53; *SD* = 1,13), gefolgt von zum Teil erforderlichen Daten (*MW* = 5,14; *SD* = 0,99) und nicht erforderlichen Daten (*MW* = 5,29; *SD* = 1,05)

Hierbei zeigten sich signifikante Unterschiede jeweils zwischen erforderlichen, zum Teil erforderlichen und nicht erforderlichen Daten.

Siehe Abbildung folgende Folie…

Erforderlichkeit der Datenarten für App-Gruppen



Der Unterschied der Bedrohlichkeitsbewertungen der Befragten zwischen erforderlichen, teilerforderlichen, und nicht erforderlichen Daten war dabei jeweils statistisch signifikant:
Erforderlich vs. teilerforderlich (z = 9,737; p = 0,000; r =0,66).
Teilerforderlich vs. nichterforderlich (z = 3,048; p = 0,002; r =0,21).

n = 218-219

Erforderlichkeit der Datenarten für App-Gruppen

Im Folgenden wurden die App-Gruppen untereinander auf den Stufen der Erforderlichkeit (unabhängig von kontinuierlichem Datentracking/bei Interaktion) verglichen:

- Betrachtet man nur die Bewertungen der Befragten für erforderliche Daten, wird die Messenger-App im Mittel signifikant bedrohlicher bewertet als die Shopping/Karten-App.
- Betrachtet man nur die Bewertungen der Befragten für zum Teil erforderliche Daten, wird die Karten-App im Mittel signifikant bedrohlicher bewertet als die Messenger-App und diese signifikant bedrohlicher als die Wetter-App.
- Betrachtet man nur die Bewertungen der Befragten für nicht erforderliche Daten, wird die Wetter-App/Shopping-App im Mittel signifikant bedrohlicher bewertet als die Messenger-App und diese bedrohlicher als die Karten-App.

Fazit: Erforderlichkeit

Erforderliche Daten wurden insgesamt über alle App-Gruppen hinweg erwartungskonform **am wenigsten bedrohlich** für die eigene Privatsphäre eingeschätzt, **gefolgt von zum Teil erforderlichen Daten** und **nicht erforderlichen Daten**. Der Grad der Erforderlichkeit der Datenerhebung steht also direkt in Verbindung mit der Bewertung der Bedrohlichkeit für die eigene Privatsphäre.

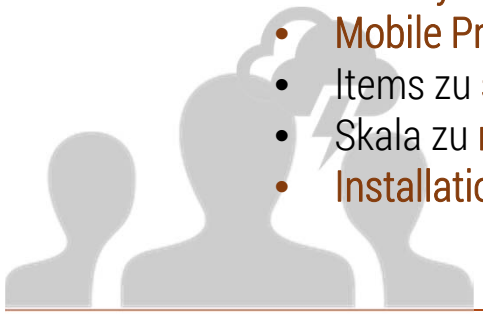
Die Messenger-App wurde bei der Erfassung von erforderlichen Daten als deutlich bedrohlicher wahrgenommen als andere App-Gruppen. Dies ließ sich aber für zum Teil erforderliche Daten und nicht erforderliche Daten nicht bestätigen. Hier werden jeweils die Karten-App und die Wetter/Shopping-App als bedrohlicher als die anderen App-Gruppen eingeschätzt.

Das heißt, die wahrgenommene Bedrohung der eignen Privatsphäre wird nicht durch die App-Gruppe sondern lediglich durch die Erforderlichkeit der Datenerhebung beeinflusst.

Personeneigenschaften und Bedrohlichkeitsbewertungen

Um zu prüfen ob bestimmte selbstbeschreibende Angaben der Befragten mit der Einschätzung der Bedrohlichkeit der Datenarten für bestimmte App-Gruppen zusammenhängen, wurden folgende Variablen korreliert bzw. Gruppenunterschiede getestet:

- Alter
- Geschlecht
- TAEG Skalen
- Privacy Concern Skalen
- Mobile Privacy Concern Skalen
- Items zu selbst eingeschätzem Wissen über Apps
- Skala zu negativen Erfahrungen
- Installationsprozess (App selbst installiert vs. vorinstalliert)



Personeneigenschaften und Bedrohlichkeitsbewertungen

Für die Variablen Alter, TAEG-Skalen , selbsteingeschätztes Wissen und negative Erfahrungen ergaben sich nur wenige schwach-signifikante Korrelationen, die keinen eindeutigen Nachweis für einen Zusammenhang zulassen. Zudem ergaben sich keine signifikanten Unterschiede in den Bewertungen zwischen Männern und Frauen oder zwischen selbstinstallierten bzw. vorinstallierten Apps.

Für die Privacy Concern sowie die Mobile Privacy Concern Skalen konnte überwiegend ein mittel-stark signifikanter, positiver Zusammenhang festgestellt werden.
Das heißt, je besorgter sich die Befragten selbst beschreiben, desto bedrohlicher bewerten sie auch die verschiedenen Datenarten.

Fazit: Personeneigenschaften, Installation und Bedrohlichkeitsbewertungen

Für die Skalen **Privacy Concerns** und **Mobile Privacy Concerns** ergab sich ein **bedeutsamer Zusammenhang mit den Bewertungen der Bedrohlichkeit** der verschiedenen Apps. Befragte, die sich selbst als besorgter beschrieben, gaben für alle App-Gruppen und sowohl bei kontinuierlichem Tracking als auch bei Interaktion höhere Werte an.

Bei allen anderen untersuchten Variablen **Alter, Geschlecht, Technikaffinität, Wissen und negative Erfahrungen konnte kein eindeutiger Zusammenhang** zu den **/Unterschied** zwischen den Bewertungen der Bedrohlichkeit nachgewiesen werden.

Auch für den **Installationsprozess** (selbstinstalliert oder vorinstalliert) konnten **keine konsistenten Unterschiede hinsichtlich der Bedrohlichkeitsbewertung** identifiziert werden.

Zusammenfassung der AndProtect Befragungsergebnisse

- Die Smartphone-Nutzer wünschen sich (neben Transparenzerhöhung, gesetzlichen Ahndungen von Privatsphärenverstößen, und Wertewandel) aktiv sicherheitstechnische Maßnahmen und detaillierte Funktionen nutzen zu können um ihre Privatsphäre zu schützen.

- Die Messenger-App ist für Smartphone-Nutzer zentral.
- Trotz dass eine bestimmte App häufig genutzt wird und für den Nutzer wichtig ist, kann diese als privatsphärenbedrohlich bewertet werden.

- Jegliche Verwendung von Daten wird von den befragten Smartphone-Nutzern kritisch bewertet.
- Das kontinuierliche Verwenden von Daten wird von den Smartphone-Nutzern nochmal als deutlich bedrohlicher bewertet, als das Verwenden von Daten bei Interaktion.
    - Dies gilt für alle untersuchten App-Gruppen.

Zusammenfassung der AndProtect Befragungsergebnisse

- Die Wahrnehmung der Bedrohung der Privatsphäre ist verknüpft mit der Erforderlichkeit von Daten, die die jeweilige App erhebt.
- Nutzer, die besorgter hinsichtlich ihrer eigenen Privatsphäre sind, bewerten das Verwenden von Daten auch als bedrohlicher.
- Alter, Geschlecht, Technikaffinität, Wissen, negative Erfahrungen oder der Installationsgegebenheiten spielen keine Rolle für die Bewertung der Bedrohung der eigenen Privatsphäre.

AndProtect

Kontakt

Susen Döbelt
Allgemeine- und Arbeitspsychologie, TU Chemnitz
Tel.: 0371 531 33615
E-Mail: susen.doebelt@psychologie.tu-chemnitz.de

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

secuvera

DAI-Labor TU Berlin

ALLGEMEINE UND ARBEITSPSYCHOLOGIE TU CHEMNITZ

Icons used within this presentation: http://iconmonstr.com/