# Einfluss einer Datenschutzskala auf das Auswahlverhalten in einem App-Markt

Sven BOCK[1], Nurul MOMEN[2]

*[1] Institut für Psychologie und Arbeitswissenschaft*
*Technische Universität Berlin*
*Marchstraße 23, D-10587 Berlin*
*[2] Department of Mathematics and Computer Science*
*Karlstads Universitet*
*Universitetsgatan 2, SWE-65188 Karlstad*

**Kurzfassung:** Beim Herunterladen von Smartphone-Applikationen wird bei den meist genutzten Plattformen kaum über den Datenaustausch und den Datenschutz informiert. Diese Studie zeigt den Einfluss einer im App-Markt implementierten Datenschutzskala auf das Nutzerverhalten. Die hinzugefügten App-spezifischen Informationen zum Datenaustausch und Datenzugriff führten zu einer sachkundigeren Applikationsauswahl bezüglich des Datenschutzes. Insgesamt 82 Teilnehmende wurden gebeten, vorgegebene Aufgaben an einem Smartphone zu erfüllen. Das Auswahlverhalten im einem prototypisierten App-Markt wurde aufgezeichnet und mit Hilfe eines Interviews von den Teilnehmenden reflektiert. Vier Stichproben wurden jeweils verschiedene Bedingungen dargeboten, um den Einfluss auf das Auswahlverhalten näher zu erfassen.

**Schlüsselwörter:** Datenschutz, Privatsphäre, Auswahlverhalten, Transparenz, mobile Endgeräte, Rechtefreigaben

## 1. Einleitung

Derzeit können Nutzer zahlreiche Probleme des täglichen Lebens durch das Herunterladen einer Applikation aus dem App-Markt bequem lösen, dabei besteht jedoch die Gefahr, dass sie Zugang zu persönlichen Daten gewähren können und somit in ihre Privatsphäre eingegriffen wird (Gross & Acquisti 2005, Watson et al. 2015, Acquisti et al.2015). Eine informierte Entscheidungsfindung bezüglich des Datenschutzes ist für die Mehrheit der Nutzer nur schwer zu erreichen. Der heutige App-Markt verfügt über ein auf Bekanntheit basierendes Bewertungssystem, welches jedoch vollständig von der Meinung anderer Nutzer abhängig ist. Bequemlichkeit, Benutzerfreundlichkeit, Funktionsreichtum und Funktionalität sind hierbei die etablierten Kriterien für die Bewertung einer Applikation (Hatamian et al. 2019). Die übermäßige Datensammlung kommt in diesem Bewertungsverfahren kaum vor. Aufgrund der Tatsache, dass dieses Kriterium für den Nutzer nicht ersichtlich ist, spielt es auch meist keine Rolle im Entscheidungsprozess. Ein Lösungsansatz wäre die Bereitstellung einer Datenschutzskala im App-Markt, die dem Benutzer helfen könnte, informierter und somit adäquater Entscheidungen zu treffen. In dieser Studie sollen die Auswirkungen einer Datenschutzskala, die bereits vor der Auswahl und Installation bei der Auflistung der Applikationen angezeigt wird (Murmann & Fischer-Hübner 2017), auf den Entscheidungsprozess der Nutzer untersucht werden, um folgende Fragen beantworten:

a) Kann die Datenschutzskala die Applikationsauswahl erleichtern und die Beurteilung der Vertrauenswürdigkeit verbessern?
b) Gibt es einen signifikanten Unterschied im Entscheidungsverhalten bei der Auswahl einer Applikation für bestimmte Aufgaben?
c) Ist die Datenschutzskala ein geeignetes Instrument, um die Aufdringlichkeit von Applikationen bezüglich des Einschreitens in die Privatsphäre zu veranschaulichen?

## 2. Hintergrund

Es wurden bereits Studien über das Bewusstsein und die Bedenken der Nutzer bezüglich des Datenschutzes durchgeführt, um Datenschutzlecks und die Benutzerfreundlichkeit der Datenschutzkontrollen näher zu betrachten. Zur Formulierung des Problems und den damit zusammenhängenden Hypothesen werden relevante Studien und deren Ergebnisse kurz erwähnt.

Das Thema Sicherheit und Datenschutz bei Android-Applikationen ist ein bekanntes Untersuchungsobjekt, weil es eine große Nutzerbasis, eine gute Abdeckung über eine Vielzahl von Geräten und eine Open-Source-Plattform bietet. Das Android-Betriebssystem basiert auf einem berechtigungsbasierten Zugangskontrollmodell, das die Benutzerdaten und Sensoren schützt. Je nach Typ ist bei der Nutzung der Applikation stets erst die Zustimmung des Nutzers für die Gewährung des Zugriffs auf die entsprechenden Ressourcen erforderlich (Android Developers Documentation 2019). Weil die Plattform lediglich eine binäre Wahlmöglichkeit anbietet (akzeptieren / ablehnen), ist es für die Verbraucher schwer die Konsequenzen der Gewährung des Zugangs zu überblicken und das Risiko zu bewerten. So wird der Applikation das permanente Recht auf den Zugriff der verfügbaren Systemressourcen und somit möglicherweise auch der Zugriff auf sensible persönliche Daten gegeben. In mehreren früheren Arbeiten wurde auf dieses Problem hingewiesen, wobei vor allem der Umfang des Datenzugriffs, die Häufigkeit, die Folgen und die Auswirkungen auf die Privatsphäre im Vordergrund standen (Hatamian et al. 2017, Franzen & Aspinall 2016, Momen et al. 2017).

In einer Studie verwendeten Rajivan und Camp (2016) visuelle Hinweise, um die Benutzer bei der Entscheidungsfindung zu unterstützen, bevor sie ihre Zustimmung zu den geforderten Zugängen gaben. Kelley et al. (2012) zeigten, dass bestimmte kontextbezogene Hinweise, wie z.B. Datenschutzsymbole, genutzt werden können, um einen Einfluss auf das Auswahlverhalten zu erlangen.

Die Nutzer sind jedoch mehr um ihre Privatsphäre besorgt, wenn sie erkennen, dass sie sich durch ihre Entscheidungen dem Risiko der Datenaushändigung ausgesetzt haben (Thompson et al. 2013, Jung et al. 2012, Felt et al. 2012). Darüber hinaus führt die Komplexität der Datenschutzinformation, z.B. in Form der AGB, zu der Bevorzugung einer einfacheren Applikationsbewertungen wie z.B. der Fünf-Sterne Bewertung.

## 3. Methodologie

Anhand einschlägiger Literatur über Symbolik und Visualisierung von Skalen wurden fünf verschiedene Entwürfe einer farbkodierten Datenschutzskala entworfen: (a) Arrow-Scale Bar, (b) Label-Bar, (c) Arrow-Scale Meter, (d) Smilies, und (e) Bubbles). Anschließend wurde eine Vorstudie in Form einer Onlineumfrage durchgeführt, in der

die Entwürfe bezüglich 1. Unterscheidbarkeit, 2. Mehrdeutigkeit, 3. Lesbarkeit, 4. Verständlichkeit, 5. Farbe und 6. Größe von 1 (am schlechtesten) bis 10 (am besten) evaluiert. Aus den Ergebnissen ist eine deutliche Favorisierung der (b) Label-Bar mit einem Mittelwert von M = 8,25 (SD = 2,28) und ein signifikanter Unterschied von ($\chi^2$= 54.35, p <.000) beim Durchführen des nichtparametrischen Friedman-Tests (Conover & Iman 1981) ersichtlich. Aus diesem Grund und der Tatsache, dass die Skala auch von Menschen mit Farbenblindheit gelesen werden kann, wurde die Label-Bar in dem nun folgenden empirischen Versuch verwendet.

Ziel der Studie war es, das Auswahlverhalten der Nutzer von Applikationen in acht Szenarien mit jeweils unterschiedlichen Aufgaben zu ermitteln. Den Teilnehmenden wurde jedoch das eigentliche Ziel der Studie vorenthalten und die Evaluierung der Benutzerfreundlichkeit eines App-Marktes als Ziel der Studie genannt. Die Stichprobe wurde in vier verschiedene Gruppen unterteilt:

Gruppe A: Datenschutzskala mit einer detaillierten Beschreibung als Einleitung;
Gruppe B: Datenschutzskala mit einer detaillierten Beschreibung auf Bedarf, durch eigenständiges Klicken auf die Datenschutzskala;
Gruppe C: Datenschutzskala ohne eine detaillierte Beschreibung;
Gruppe D: Ohne Datenschutzskala als Kontrollgruppe des Versuchs.

Zur Simulation des alltäglichen Gebrauchs eines mobilen Endgerätes, wurden den Teilnehmenden acht Szenarien präsentiert, in welche sie sich hineinversetzen und eine dazu passende Applikation aus dem App-Markt auswählen, herunterladen und verwenden sollten, um alltagsübliche Aufgaben zu lösen. Die Szenarien beinhalteten bspw. das Schreiben einer Nachricht (Messenger) oder die Führung einer Videokonferenz (Videokonferenz). Die Blickbewegung der Teilnehmenden wurde während des Auswahlverfahrens aufgezeichnet, um dieses später zu analysieren und die Teilnehmenden bei der Beantwortung eines halbstrukturierten Interviews nach der Think-Aloud-Methode zu unterstützen.

Anschließend wurden die Teilnehmenden gebeten einen Fragebogen ausfüllen, um die Einfachheit der Auswahl und Vertrauenswürdigkeit der Applikation zu bewerten. Darüber hinaus wurden sie gebeten in einem weiteren Fragebogen die Datenschutzskala bezüglich der Akzeptanz und der Benutzerfreundlichkeit zu beurteilen. Weiterhin wurden eine angepasste Version des MUIPC-Fragebogens (measuring mobile users' concerns for information privacy) von ihnen ausgefüllt. Ein letzter Fragebogen sollte die demographischen Daten und favorisierten Bewertungssysteme festhalten (Rezension, Sterne, Aufrufe, Downloads und Datenschutzskala).

## 4. Ergebnisse

An der Studie nahmen insgesamt 82 deutschsprachige Personen (davon 38 Frauen, 43 Männer und 1 Divers) teil, die zwischen 18 und 68 Jahren alt waren.

Es wurde angenommen, dass die Implementierung einer Datenschutzskala in einem App-Markt zu einer angemesseneren Auswahl von Applikationen in Bezug auf den Datenschutz führen würde. Um den Einfluss der Datenschutzskala und der detaillierten Beschreibung zu ermitteln, wurden den Applikationen je nach ihrer Kategorisierung (von „sehr kritisch“ bis „sehr sicher“), die entsprechenden Werte (von 1 bis 5) zugeteilt.

Die daraus berechneten Mittelwerte zeigen eine Tendenz zu einem höheren Wert bzw. einer sichereren Einstufung in den Gruppen mit Datenschutzskala (A, B und C)

im Vergleich zur Kontrollgruppe ohne Datenschutzskala (D). Dies bestätigt die Annahme, dass die Teilnehmenden, die eine Datenschutzskala zur Verfügung hatten, Applikationen auswählten, die als weniger kritisch eingestuft wurden. Die nichtparametrischen Daten wurden mit dem Kruskal-Wallis-Test auf signifikante Unterschiede überprüft, welche in folgenden Kategorien gefunden werden konnten:

1. Wetter ($\chi^2$= 14.591, $p < .002$), 2. E-Mail ($\chi^2$= 12.309, $p < .006$), 3. Musik ($\chi^2$= 17.572, $p < .001$), 4. Fitness ($\chi^2$= 15.716, $p < .001$), 5. Spiele ($\chi^2$= 25.720, $p < .000$) und 6. Nachrichten ($\chi^2$= 20.062, $p < .000$). Weiterführende paarweise Vergleiche führten zu ähnlichen Ergebnissen.

Bei näherer Betrachtung der Ergebnisse bezüglich der Einfachheit der Applikationsauswahl sowie der Vertrauenswürdigkeit der Applikation (auf einer Skala von 1 = trifft nicht zu, bis 7 = trifft völlig zu), sind die höchsten Durchschnittswerte, mit Ausnahme der Einfachheit der Auswahl in der Kategorie Messenger, alle in den Gruppen A, B und C zu finden. Dies lässt vermuten, dass die Datenschutzskala die Auswahl der entsprechenden Applikationen erleichtert und die Vertrauenswürdigkeit der ausgewählten Applikation erhöht. Um diese Annahme zu prüfen, wurden die nicht normalverteilten Daten ebenfalls mit dem Kruskal-Wallis-Test auf signifikante Unterschiede in den Kategorien getestet. Es konnte ein signifikanter Unterschied der Vertrauenswürdigkeit bei den folgenden Kategorien gefunden werden: 1. Videokonferenz ($\chi^2$= 8.463, $p < .037$), 2. Wetter ($\chi^2$= 9.854, $p < .020$), 3. E-Mail ($\chi^2$= 12.129, $p < .007$), 4. Fitness ($\chi^2$= 9.152, $p < .027$) und 5. Nachrichten ($\chi^2$= 8.723, $p < .033$). Für die Einfachheit der Applikationsauswahl konnte ein signifikanter Unterschied für die Kategorien Wetter ($\chi^2$= 9.854, $p < .020$) und Fitness ($\chi^2$= 12.892, $p < .005$) gefunden werden.

Die Datenschutzskala wurde insgesamt in Bezug auf Vertrauenswürdigkeit, Benutzbarkeit, Verständnis, Intuitivität, Validität, Zuverlässigkeit, Wirkung, Schutzgefühl, Nachfrage, Nutzungsbereitschaft und der Vertrauenswürdigkeit von Applikationen positiv bewertet. Negative Aspekte, wie Mehrdeutigkeit, Informationsdefizit und Komplexität wurden mehrheitlich abgelehnt. Im Vergleich zu Gruppe B und C, wies Gruppe A eine Tendenz zur besseren Bewertung der Datenschutzskala auf, während bei Gruppe C die schlechtesten Werte zu finden waren. Der nichtparametrische Kruskal-Wallis-Test konnte jedoch nur einen signifikanten Unterschied zwischen den Gruppen, für das Attribut Informationsdefizit ($\chi^2 = 10$, $p < .010$) aufzeigen.

Die Analyse der Antworten der Teilnehmenden durch den MUIPC-Fragebogen zeigte, dass ein hoher Prozentsatz der Teilnehmenden mit den gegebenen Aussagen übereinstimmt. Die Mehrheit war darüber besorgt, dass Applikationen ihr mobiles Endgerät überwachen und ihre Aktivitäten an diesem Gerät aufnehmen. Darüber hinaus hatten sie das Gefühl, dass durch ihr mobiles Endgerät mehr Informationen über ihre Privatsphäre and dritte weitergegeben wurde als sie es sich wünschten. Zusammenfassend war den Teilnehmenden durchausbewusst, dass ihre Daten durch Applikationen in Umlauf gebracht werden, was größtenteils auf Missfallen gestoßen ist. Nichtsdestotrotz gab dreiviertel der Teilnehmenden an, höchstwahrscheinlich weiterhin persönliche Informationen auszuhändigen, um eine Applikation nutzen zu können.

## 5. Diskussion

Allgemein ist zu beobachten, dass die Bedenken um die Privatsphäre umgekehrt proportional zur Bekanntheit der Applikationen sind, was an den Kategorien Messenger und Videokonferenz aufgrund der häufigen Auswahl von „WhatsApp“ und „Skype“ zu erkennen ist. Im Gegensatz dazu, wurden bei den Kategorien Wetter, Fitness und

News vermehrt als „sehr sicher“ gekennzeichnete Applikationen ausgewählt. Die Verfügbarkeit einer detaillierten Beschreibung der Datenschutzskala steigerte dieses Phänomen. Für die Einfachheit der Applikationsauswahl und die Bewertung der Vertrauenswürdigkeit der Applikationen, sind die höchsten Mittelwerte in den Gruppen A, B und C, also mit Datenschutzskala, und die niedrigsten Mittelwerte in der Gruppe D, ohne Datenschutzskala zu finden. In den Kategorien Videokonferenz, Wetter, E-Mail, Fitness und Nachrichten, waren die Teilnehmenden, die eine Datenschutzskala zur Verfügung hatten, signifikant adäquater beim Evaluieren der Vertrauenswürdigkeit der Applikationen.

Diese Ergebnisse können durch die Bekanntheit der Applikationen erklärt werden. Am Beispiel der Anwendung „Skype“ führt eine bekannte Applikation in Kombination mit einer sicheren Kennzeichnung auf der Datenschutzskala, zu einer höheren Bewertung der Vertrauenswürdigkeit als eine bekannte Applikation ohne Datenschutzskala. Eine bekannte Applikation in Kombination mit einer unsicheren Kennzeichnung auf der Datenschutzskala, führt zu einer geringeren Bewertung der Vertrauenswürdigkeit. Trotz der unsicheren Kennzeichnung auf der Datenschutzskala, wird die Applikation aufgrund ihrer Bekanntheit ausgewählt. Durch die Kennzeichnung der Applikation als „unsicher“ wird diese jedoch mit einer geringeren Vertrauenswürdigkeit bewertet. Wenn die Applikation nicht bekannt ist und die Datenschutzskala sie als „sehr sicher“ kennzeichnet, wird die Vertrauenswürdigkeit der Applikation als hoch bewertet. Eine unbekannte Applikation mit einer unsicheren Kennzeichnung auf der Datenschutzskala wird in der Regel nicht ausgewählt und hat somit keinen Einfluss auf die Bewertung. Eine bekannte Applikation ohne Datenschutzskala ist stark von ihrer Reputation abhängig, was aus den Interviews ersichtlich ist. Ein ähnliches Muster ist bei der Einfachheit der Auswahl zu erkennen. Dies hat bei den Kategorien Wetter und Fitness zu einer signifikant einfacheren Applikationsauswahl für die Gruppen A, B und C, mit Datenschutzskala, geführt.

Anhand der Ergebnisse ist ein signifikanter Einfluss der Datenschutzskala auf das Auswahlverfahren in den Kategorien Wetter, E-Mail, Musik, Fitness, Spiele und Nachrichten zu erkennen. Dies führte zu einer Auswahl von weniger invasiven Applikationen. Die fehlende Signifikanz in den Kategorien Messenger und Videokonferenz, lässt sich wiederum durch die Bekanntheit der Applikationen („Skype“ und „WhatsApp“) erklären. Die Interviews zeigten, dass die meisten Teilnehmenden eine Applikation gewählt haben, die sie bereits kannten. Die Datenschutzskala wurde von den Teilnehmenden mehrheitlich positiv bewertet.

## 6. Fazit

Die wichtigsten Erkenntnisse der Studie lassen sich wie folgt zusammenfassen:
a) Eine unilaterale Datenschutzskala kann zu einer besseren Beurteilung der Vertrauenswürdigkeit der Applikationen führen und die Auswahl dieser erleichtern; b) die Gruppen mit einer Datenschutzskala konnten im Vergleich zur Kontrollgruppe eine adäquatere Entscheidung bzgl. der Wahrung der Privatsphäre treffen; und c) aus den Ergebnissen der Fragebögen geht hervor, dass die Datenschutzskala ein geeignetes Instrument ist, um sowohl die Transparenz zu steigern als auch die Privatsphäre der Nutzer zu schützen. Generell wurde die Skala von den Teilnehmenden als positiv und hilfreich empfunden. Darüber hinaus führt die Skala zu einer Sensibilisierung der Nutzer hinsichtlich des Datenschutzes, was zu einem datenschutzfreundlicherem Auswahlverhalten führt. Allerdings kann dieses Phänomen bei bekannten Applikationen

nur teilweise beobachtet werden, weil die Nutzer dazu neigen, die Bekanntheit der Applikationen zu priorisieren und sich somit im Zweifelsfall für eine unsichere jedoch bekannte Applikation entscheiden.

Auch wenn die Datenschutzskala eine kurze Einführung für die richtige Interpretation erfordert, hat sie das Potenzial, Applikationen daran zu hindern immer größere Mengen an Daten zu sammeln und diese an Dritte weiterzugeben. Aggressive Applikationen müssten mit einer kritischen Kennzeichnung rechnen, welche den Nutzer dazu verleitet eine weniger in die Privatsphäre eingreifende Alternative auszuwählen.

## 7. Literatur

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509-514.

Android Developers Documentation. 2019. Dangerous permissions. https://developer.android.com/guide/topics/permissions/overview#dangerous_permission. (2019). Zugriff: 08.01.2020.

Conover, W. J., & Iman, R. L. (1981). Rank transformations as a bridge between parametric and nonparametric statistics. The American Statistician, 35(3), 124-129.

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012, July). Android permissions: User attention, comprehension, and behavior. In Proceedings of the eighth symposium on usable privacy and security (p. 3). ACM.

Franzen, D., & Aspinall, D. (2016). PhoneWrap-Injecting the" How Often" into Mobile Apps. In IMPS@ ESSoS (pp. 11-19).

Gross, R., & Acquisti, A. (2005, November). Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society (pp. 71-80). ACM.

Hatamian, M., Serna, J., Rannenberg, K., & Igler, B. (2017, August). FAIR: Fuzzy alarming index rule for privacy analysis in smartphone apps. In International Conference on Trust and Privacy in Digital Business (pp. 3-18). Springer, Cham.

Hatamian, M., Serna, J., & Rannenberg, K. (2019). Revealing the unrevealed: mining smartphone users privacy perception on Applikation markets. Computers & Security, 83, 332-353.

Jung, J., Han, S., & Wetherall, D. (2012, October). Short paper: enhancing mobile application permissions with runtime feedback and constraints. In Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices (pp. 45-50). ACM.

Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N., & Wetherall, D. (2012, February). A conundrum of permissions: installing applications on an android smartphone. In International conference on financial cryptography and data security (pp. 68-79). Springer, Berlin, Heidelberg.

Momen, N., Pulls, T., Fritsch, L., & Lindskog, S. (2017, August). How Much Privilege Does an App Need? Investigating Resource Usage of Android Apps (Short Paper). In 2017 15th Annual Conference on Privacy, Security and Trust (PST) (pp. 268-2685). IEEE.

Murmann, P., & Fischer-Hübner, S. (2017). Tools for achieving usable ex post transparency: a survey. IEEE Access, 5, 22965-22991.

Rajivan, P., & Camp, J. (2016). Influence of privacy attitude and privacy cue framing on android app choices. In Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016).

Thompson, C., Johnson, M., Egelman, S., Wagner, D., & King, J. (2013, July). When it's better to ask forgiveness than get permission: attribution mechanisms for smartphone resources. In Proceedings of the Ninth Symposium on Usable Privacy and Security (p. 1). ACM.

Watson, J., Lipford, H. R., & Besmer, A. (2015). Mapping user preference to privacy default settings. ACM Transactions on Computer-Human Interaction (TOCHI), 22(6), 32.

Gesellschaft für
Arbeitswissenschaft e.V.

# Digitale Arbeit, digitaler Wandel, digitaler Mensch?

66. Kongress der
Gesellschaft für Arbeitswissenschaft

TU Berlin
Fachgebiet Mensch-Maschine-Systeme

HU Berlin
Professur Ingenieurpsychologie

16. – 18. März 2020, Berlin

GfA-Press

**Bericht zum 66. Arbeitswissenschaftlichen Kongress vom 16. – 18. März 2020**

**TU Berlin, Fachgebiet Mensch-Maschine-Systeme**
**HU Berlin, Professur Ingenieurpsychologie**

Herausgegeben von der Gesellschaft für Arbeitswissenschaft e.V.
Dortmund: GfA-Press, 2020
ISBN 978-3-936804-27-0

NE: Gesellschaft für Arbeitswissenschaft: Jahresdokumentation

Als Manuskript zusammengestellt. Diese Jahresdokumentation ist nur in der Geschäftsstelle erhältlich.


**Schriftleitung: Matthias Jäger**
im Auftrag der Gesellschaft für Arbeitswissenschaft e.V.



**Screen design und Umsetzung**
© 2020 fröse multimedia, Frank Fröse
**office@internetkundenservice.de · www.internetkundenservice.de**