

PRiME – PRivatheit im MEtaverse

Fachgespräch am 3. Juni 2026



ERGEBNISSE DES PROJEKTS



Bundesministerium
für Forschung, Technologie
und Raumfahrt

Gliederung der Präsentation

1. Überblick über das Projekt
2. Risiken des Metaverse für die Privatsphäre und rechtliche Einordnung
3. Designs für Datenschutz und Persönlichkeitsrechte
4. Metriken zur Bewertung der Privatsphäre Auswirkungen
5. Fazit

Überblick über das Projekt

Dr. Otmar Lell, ConPolicy-Institut für Verbraucherpolitik



1



PRiME – Privatheit im Metaversum



Bundesministerium
für Forschung, Technologie
und Raumfahrt



Projektpartner



Hintergrund



“Metaverse”: Das zweite Leben in virtuellen Welten als nächste Entwicklungsstufe des Internet?



Breite Anwendungsmöglichkeiten und wirtschaftliches Potential in Alltag, Kultur, Gesellschaft



Neuartige Risiken für die Privatsphäre
mit Blick auf Datenschutz und Persönlichkeitsrechte

Projektziele



Entwicklung und Test von Benutzeroberflächen, die Nutzer:innen helfen, ihre Privatsphäre zu schützen, Einwilligungsentscheidungen zu treffen und sich vor Belästigung zu schützen.



Entwicklung von Metriken, zur Unterstützung von Entwickler:innen bei der Gestaltung von privatsphärefreundlichen Umgebungen in virtuellen Welten.



Erforschung von Methoden, um Nutzermeinungen zu Designs und Metriken zu erfassen – sowohl mit klassischen Verfahren als auch direkt in virtuellen Welten.

Forschung im Dialog mit der Bevölkerung



Dialog mit der Bevölkerung:

- 5 Monate Test-Space im Offenen Innovationslabor JOSEHPS
- Erklärvideos, Mitmachexperimente und interaktive Lernwelten
- Lange Nacht der Wissenschaften in Bonn und Göttingen
- Dissemination von Forschungsergebnissen über Verbraucherzentrale und Hate Aid

Dialog mit Fachwelt und Entwickler:innen:

- Intensive Rückkopplung mit Expert:innen (z. B. Auftakt-Expertenworkshop im Metaverse)
- Auftritte auf Fachveranstaltungen und Messen (z. B. XR Days, Plattform Privatheit, GG Bavaria, Gamescom, re:publica)

Privatsphärerisiken und rechtliche Einordnung

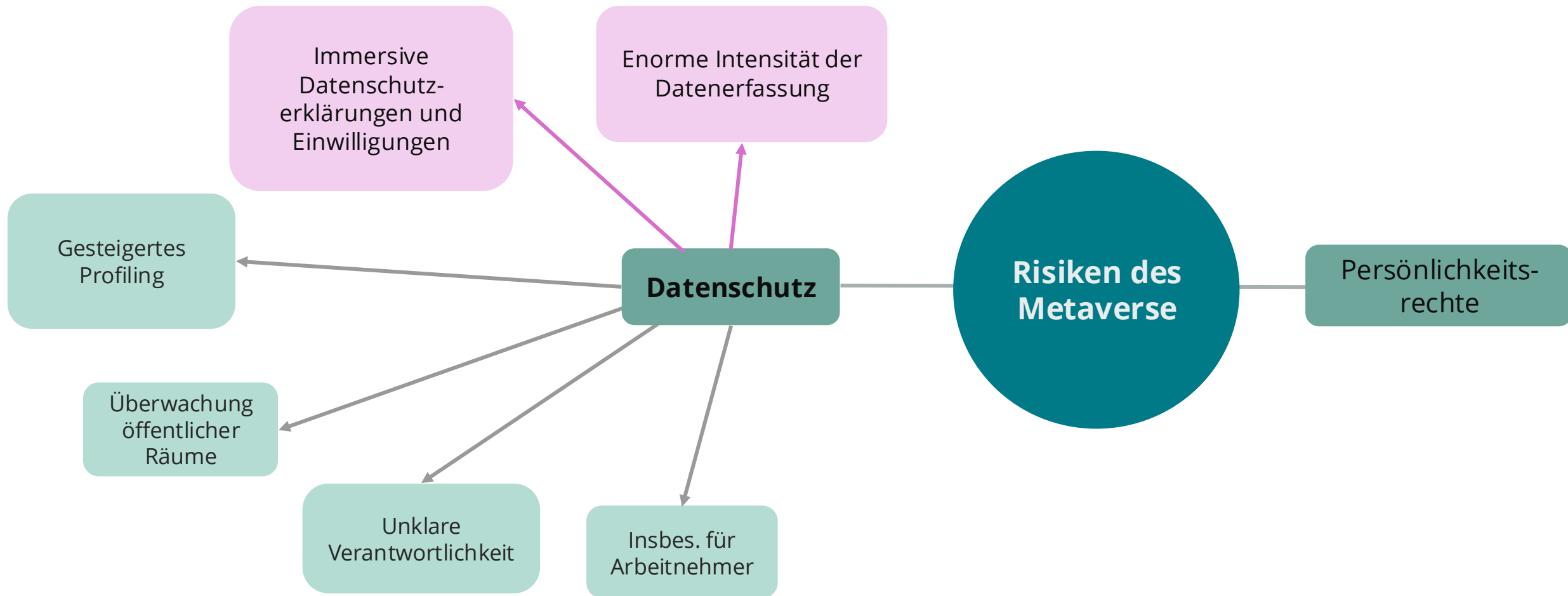


Felix Büning, Uni Göttingen und Daniel Winter, Uni Bonn

2



Risiken des Metaverse für die Privatheit - Datenschutz



Risiken für den Datenschutz



Unklare Verantwortungsbereiche

- Metaverse als dezentrale Vision wird von vielen unbekannten Akteuren anstelle eines greifbaren Verantwortlichen gestaltet
- Gemeinsame Verantwortlichkeit im Metaverse



Beschäftigtendatenschutz

- Besondere Verarbeitungssituation aufgrund der Nähe zum Industrial Metaverse
- Schutzbedürftigkeit des „gläsernen Arbeiters“



Intensität der Datenerfassung

- Mehr Datenpunkte für Profiling durch eine Vielzahl von Sensoren (z.B. Bewegung, Blickrichtung)
- Besonders sensible Daten (wie z.B. Herzfrequenz, Wohnung) betroffen



Immersive Datenschutzerklärungen und -Einwilligungen

- Darstellung von Datenschutzinformationen in 3D-Welt
- Unterbrechungsfreies virtuellen Erlebnisses lädt zum Unterlaufen des Selbstbestimmungsrechts ein



Datenschutzrechtliche Einordnung

Intensität der Datenerfassung



Art. 5 Abs. 1 lit. c-e DSGVO

Art. 25 DSGVO

Pflichtenprogramm nach DSGVO:

- insbes. Datenschutzgrundsätze
 - insbes. Privacy-by-Design
- => **Datensparsame** Konzipierung von Metaverse-Umgebungen

Datenschutzerklärungen und -Einwilligungen



Art. 12 ff. DSGVO

Art. 4 Nr. 11, 7 DSGVO

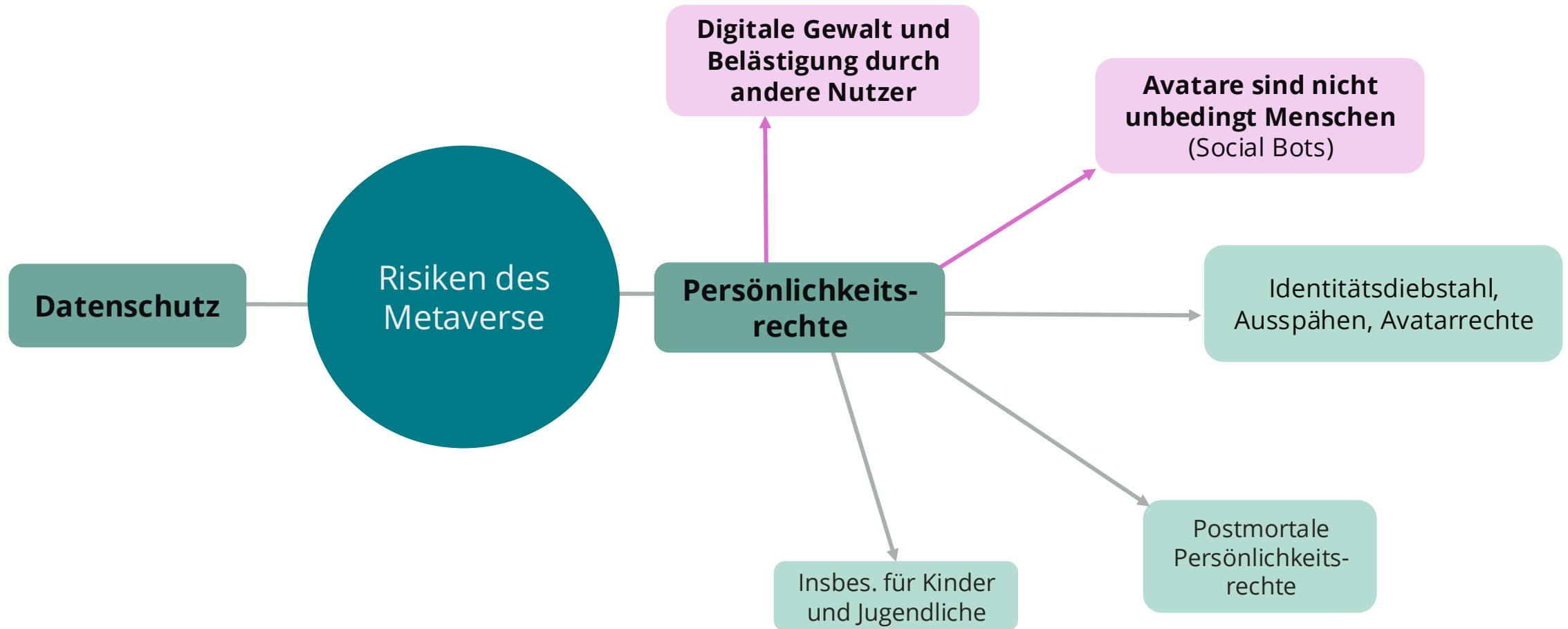
TDDDG / ePrivacy-RL

- **Inhalts-** und **Darstellungsanforderungen** für die Datenschutzerklärungen
- Einwilligung insbes. **freiwillig**, in **informierter** Weise und für den **bestimmten** Fall

Abwägung der Designpraktiken gegenüber dem Geschäftsmodell und der Nutzerfreundlichkeit
zur Schaffung eines angemessenen Datenschutzniveaus



Risiken des Metaverse für die Privatheit - Persönlichkeitsrechte



Risiken für Persönlichkeitsrechte



Totalüberwachung, Avatare und Identitätsdiebstahl

- Umfangreiche Sensordaten ermöglichen Rückschlüsse auch über Psyche und Emotionen des Nutzers
- Hochrealistische Avatare liefern detaillierte Informationen
- Identitätsdiebstahl, "Social Engineering" und Deep Fakes/"Avatar-Cloning"



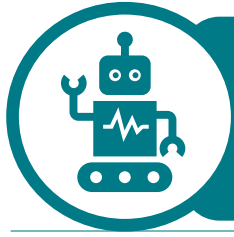
Postmortale Persönlichkeitsrechte

- Virtueller Ruf bzw. virtuelle Identität, postmortales Persönlichkeitsrecht
- Vererbbarkeit und Nutzungsrechte an dem Avatar



Digitale Gewalt und Belästigung

- Virtuelle Übergriffe wie Belästigung, Beleidigung und Begrabschen
- Gesteigerte Intensität aufgrund der zusätzlichen Verletzlichkeit virtueller Avatare

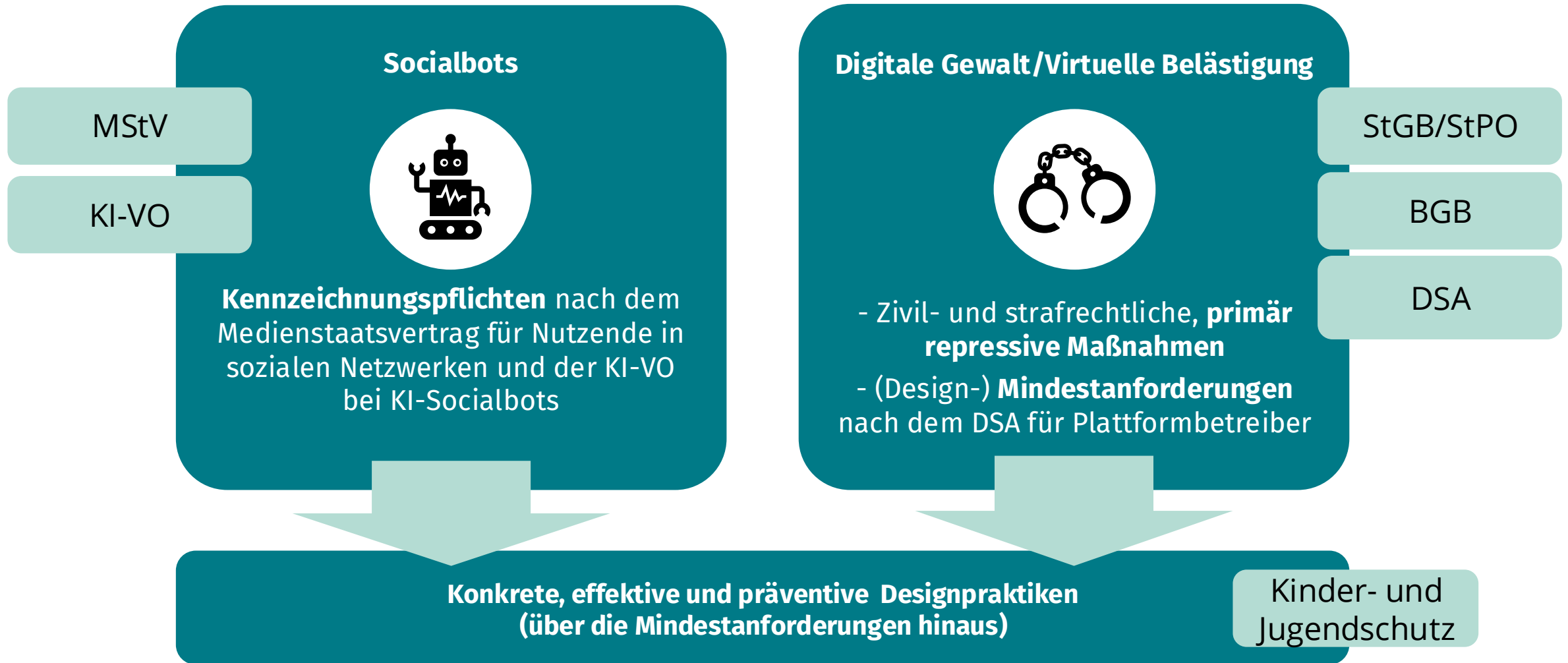


(KI) Social Bots

- Vorspiegelung echter Identität, Manipulation und Verbreitung von Desinformation
- Hyperrealistische, anpassungsfähige KI-gesteuerte Avatare



Persönlichkeitsrechtliche Einordnung



Privatsphärefreundliche Designs im Metaverse



Runjiie Xie, Universität Bamberg

3



Fokussierte Schwerpunktthemen

Datenschutzrechtlicher Bereich

Intensität der Datenerfassung

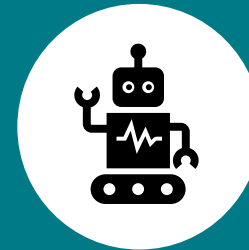


Intransparente und störende Einwilligungsprozesse



Persönlichkeitsrechtlicher Bereich

Irreführung und Manipulation durch Social Bots



Belästigungen und virtuelle Gewalt



Methoden

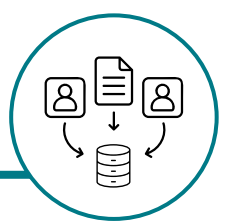
Desk Research / Literaturanalysen

- Umfangreiche Analyse der wissenschaftlichen und grauen Literatur
- Relevante europäische und nationale Gesetze und Rechtsprechung
- Analyse ausgewählter Metaverse-Plattformen
- Bewertung der Gestaltung von Metaverse-Plattformen

Empirische Methoden

- Expert:inneninterviews und -workshops
- Fokusgruppengespräche mit Nutzer:innen
- Online-Befragung mit Nutzer:innen zu Gestaltungsempfehlungen
- Studien und Experimente mit Nutzer:innen (auf Metaverse-Plattformen)

Intensität der Datenerfassung



Beispiele für entwickelte und evaluierte Designvorschläge:



Cookie-Banner-System



Sensor-Hinweis



Sensor-Erinnerung



Sensor-Hinweis mit Erklärung

Erkenntnisse:

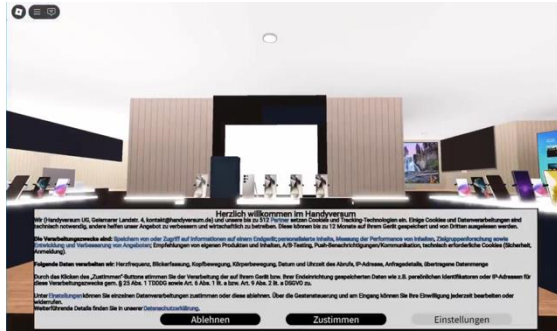
- Mechanismen zur Echtzeit-Information über Datenerhebungen werden grundsätzlich positiv bewertet
- Allerdings sollten sie sorgfältig gestaltet und nicht überladen sein, um die Immersion der virtuellen Umgebung aufrechtzuerhalten
- Sie sollten auch optional (aktivier-/deaktivierbar) und individuell anpassbar sein, um individuellen Nutzerbedürfnissen gerecht zu werden



Intransparente und störende Einwilligungsprozesse



Beispiele für entwickelte und evaluierte Designvorschläge:



Dezentrale Cookie-Banner



Dezentraler Datenschutzassistent (immersiv)



Zentraler Datenschutzassistent (immersiv)

Erkenntnisse:

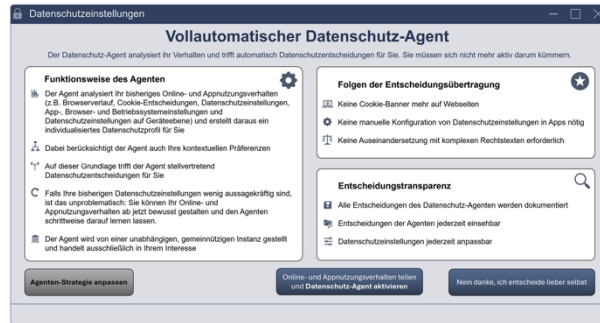
- Cookie-Banner werden als störend empfunden.
- Datenschutzassistenten sollten optional und individuell anpassbar sein
- Ein Bot-basierter Datenschutzassistent kann Skepsis auslösen und Ablehnung bewirken
- Das Konzept eines zentralen Datenschutzverwaltungssystems ist basierend auf unseren Daten nicht nur im Metaverse wünschenswert, sondern grundsätzlich bevorzugt bei der Nutzung digitaler Internetdienste



Intransparente und störende Einwilligungsprozesse



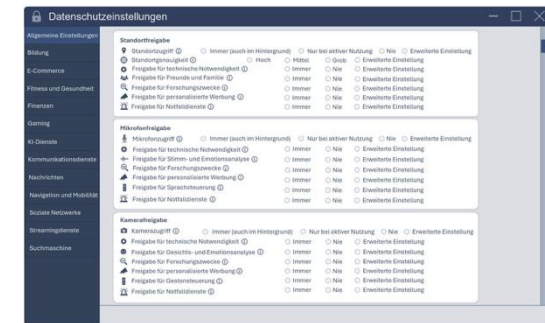
Zentrales Datenschutzverwaltungssystem (PIMS) (allgemein)



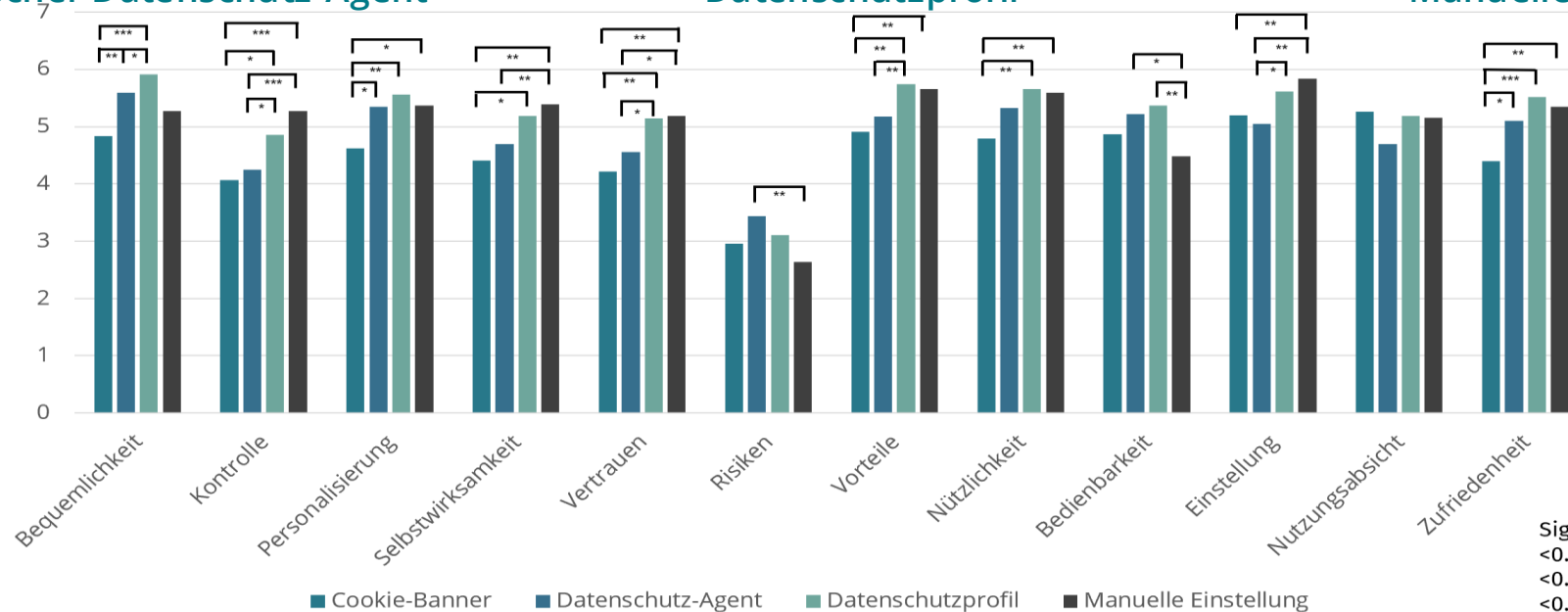
Vollautomatischer Datenschutz-Agent



Datenschutzprofil



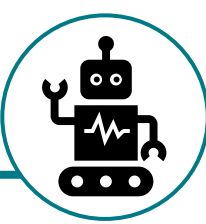
Manuelle Einstellung



Signifikanzniveau
 <0.05*
 <0.01**
 <0.001***



Irreführung und Manipulation durch Social Bots



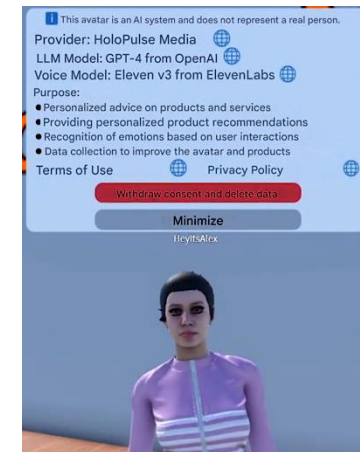
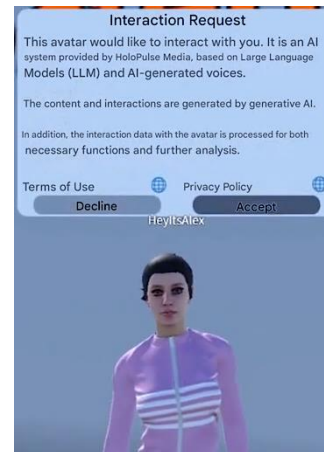
Beispiele für entwickelte und evaluierte Designvorschläge:



Varianten von Bot-Kennzeichnungen



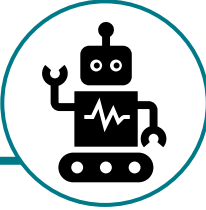
Botfreie Zone



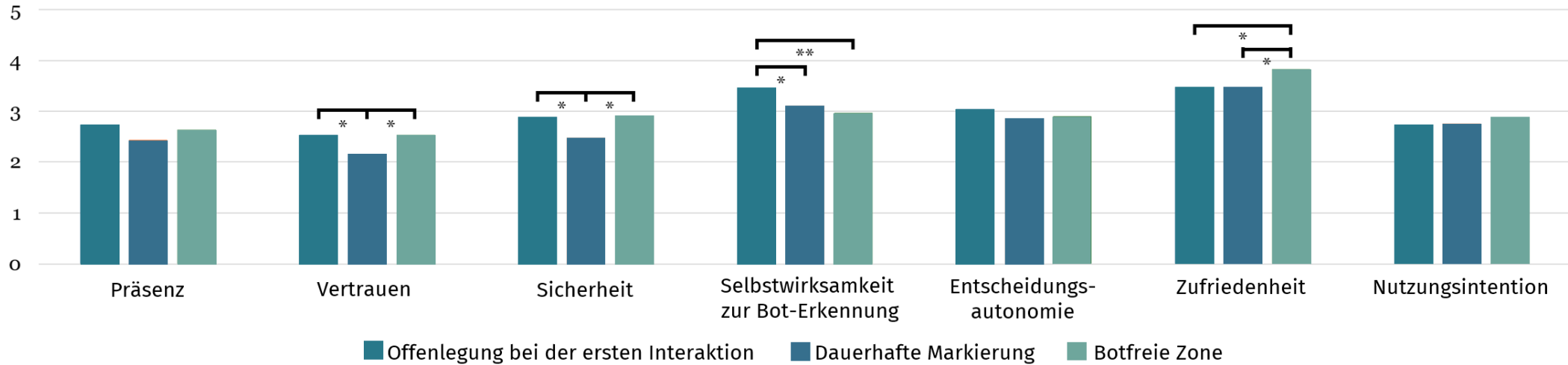
Bot-Kennzeichnung mit transparenter Aufklärung



Irreführung und Manipulation durch Social Bots



Erkenntnisse:



- Konsument:innen präferieren Kennzeichnungen von Bots, zweifeln jedoch an deren zuverlässiger Umsetzbarkeit
- Persistente Kennzeichnung kann negative Konsequenzen haben, aufgrund dauerhafter Wahrnehmung von Bots (z.B. Vertrauen, Sicherheit)
- Unser Online-Experiment hat gezeigt: Konsument:innen empfinden bei als Bots wahrgenommenen Avataren signifikant weniger soziale Präsenz, Wohlwollen, Integrität und soziale Attraktivität
- In Metaverse-Einkaufssituationen werden als Bots wahrgenommene Avatare und ihre Empfehlungen daher als weniger glaubwürdig eingestuft → Unternehmen haben Interesse dies zu verbergen
- Über Kennzeichnungen hinaus bevorzugen Konsument:innen explizite „botfreie Zonen“

Belästigungen und virtuelle Gewalt



Beispiele für entwickelte und evaluierte Designvorschläge:



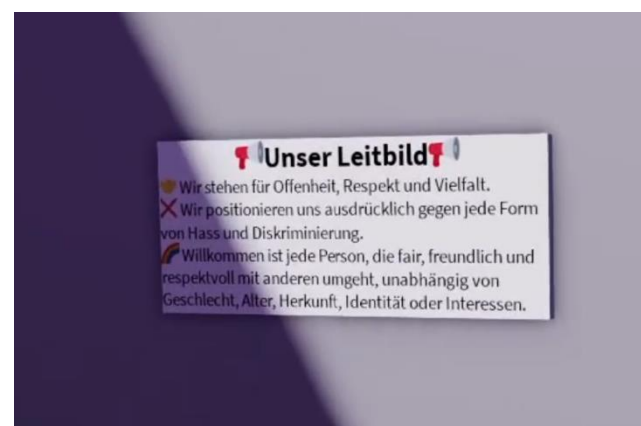
Beleuchtung



Safety Bubble



Schutzmechanismen und -maßnahmen



Normative Hinweise



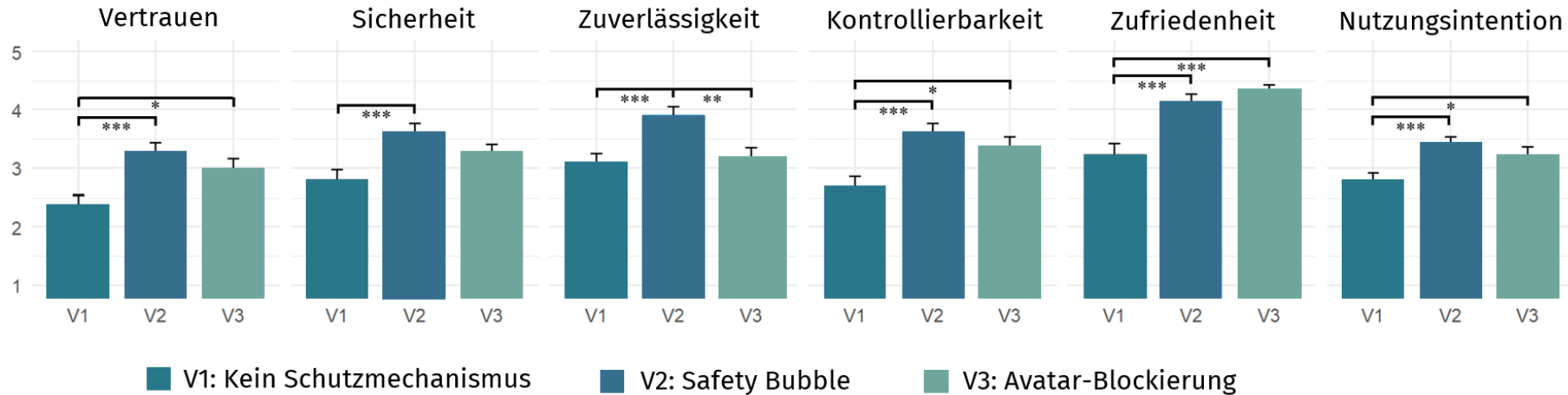
SOS-Notruf



Belästigungen und virtuelle Gewalt



Erkenntnisse:



- Die Möglichkeit, Schutzmechanismen in Belästigungssituationen im Metaverse zu nutzen, wird grundsätzlich positiv bewertet
- Präventive Mechanismen wie Safety Bubbles gelten als wirksamer als rein reaktive Maßnahmen, da sie Nutzer:innen proaktiv schützen und selbstbestimmte Interaktionen ermöglichen
- Auch die Einbeziehung von anderen Nutzer:innen in der Nähe kann Betroffene unterstützen (z.B. virtueller Notruf)
- Unterschiedliche Belästigungsformen erfordern unterschiedliche Maßnahmen und eine Kombination vielfältiger Schutzmechanismen ist notwendig für eine selbstbestimmte und sichere virtuelle Umgebung

Metriken für Privatsphärefreundlichkeit

Dr. Julius Rauber, ConPolicy-Institut für Verbraucherpolitik



4



Metriken für Privatsphärefreundlichkeit

Ziel der Metriken:

- Unterstützung von Entwickler:innen bei der Gestaltung von privatsphärefreundlichen Umgebungen in virtuellen Welten
- Bewertung der Privatsphärefreundlichkeit existierender Metaverseumgebungen

Dimensionen der Metriken:

- Rechtliche Anforderungen des Datenschutzes und der Persönlichkeitsrechte **(20)**
- Darüber hinausgehende Umsetzungsempfehlungen und Designvorschläge **(21)**

Anwendungsfelder:

- Primär b2c-Anwendungen in Spieleumgebungen und Shoppingwelten

<https://privacy-metaverse.de/metriken/>

<https://privacy-metaverse.de/designvorschlaege/>

Metriken für Privatsphärefreundlichkeit

Datenschutz

– Was wird getan, damit personenbezogene Daten nur in möglichst geringem Umfang erhoben werden?

+ Personenbezogene Daten werden nur verarbeitet, wenn hierfür eine Rechtsgrundlage wie eine Einwilligung oder ein berechtigtes Interesse vorhanden ist.

+ Es werden nur personenbezogene Daten verarbeitet, die für den jeweiligen Verarbeitungszweck erforderlich sind. Dies wird durch geeignete technische und organisatorische Maßnahmen sichergestellt.

+ Nutzer:innen haben die Möglichkeit, die Datenerhebung durch Ein- und Ausschalten von Sensoren zu steuern und zu minimieren.

Metriken für Privatsphärefreundlichkeit

— Nutzer:innen haben die Möglichkeit, die Datenerhebung durch Ein- und Ausschalten von Sensoren zu steuern und zu minimieren.

+ Juristische Erläuterung

— Designvorschlag "Nutzerseitige Steuerung von Datenerfassung durch Sensoren"

Plattformen bieten Nutzer:innen Einstellungsoptionen für physische und virtuelle Sensoren (z.B. Mikrofon, Kamera, Körperbewegung, Blickerfassung) an.

Nutzer:innen können damit eigenständig festlegen, welche Sensoren für Funktionalität und Datenerfassung aktiviert oder deaktiviert werden, und so die Datensammlung gezielt selbst steuern.



Metriken für Privatsphärefreundlichkeit

Schutz der Persönlichkeitsrechte

– Was wird getan, um Nutzer:innen vor Belästigung und Missbrauch zu schützen?

+ Es werden Risiken der Belästigung und des Missbrauchs analysiert und bewertet sowie Maßnahmen getroffen, um solche Risiken zu verringern.

+ Nutzer:innen können sich gegen akute Belästigungen oder Missbrauchsabsichten wehren (z.B. durch eine Blockierfunktion)

+ Nutzer:innen können sich systematisch und vorbeugend gegen Belästigungen oder Missbrauchsabsichten schützen (z.B. durch Voreinstellungen zur Sichtbarkeit ggü. Anderen oder zu Mindestabständen zu anderen Nutzer:innen)

+ Es gibt für Nutzer:innen wie in der realen Welt private/geschützte Orte ("Safe Zones"), wo sie sich zurückziehen können.

+ Es werden Verhaltensregeln/Kodices vorgegeben und diese den Nutzer:innen transparent dargestellt.

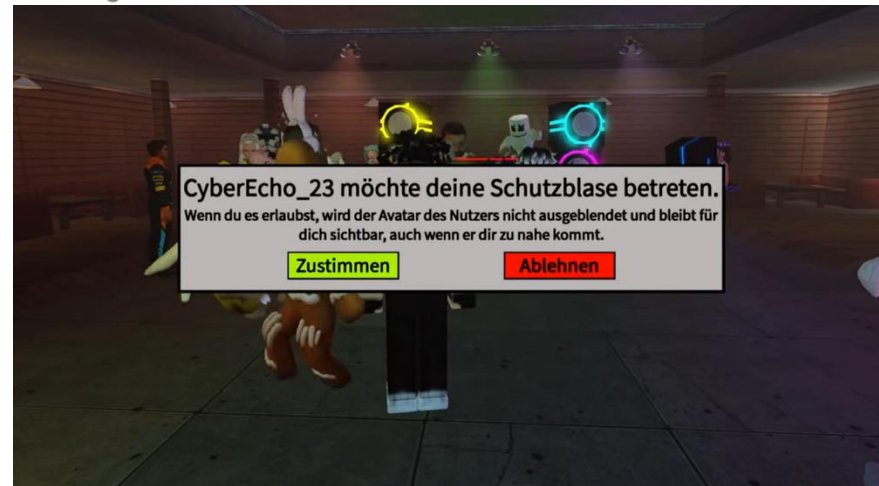
Metriken für Privatsphärefreundlichkeit

– Nutzer:innen können sich systematisch und vorbeugend gegen Belästigungen oder Missbrauchsabsichten schützen (z.B. durch Voreinstellungen zur Sichtbarkeit ggü. Anderen oder zu Mindestabständen zu anderen Nutzer:innen)

+ Juristische Erläuterung

– Designvorschlag "Safety Bubble"

Plattformen sollten den Nutzern Schutzmaßnahmen bereitstellen, mit denen sie sich präventiv vor möglicher Belästigung schützen können, beispielsweise durch die Möglichkeit, Interaktionen mit fremden Nutzern einzuschränken.



Fazit nach drei Jahren Projektlaufzeit

Dr. Otmar Lell, ConPolicy-Institut für Verbraucherpolitik

5



Design als Lösungsansatz für Privatheitsrisiken im Metaverse: Potenziale und Grenzen

Datenschutz

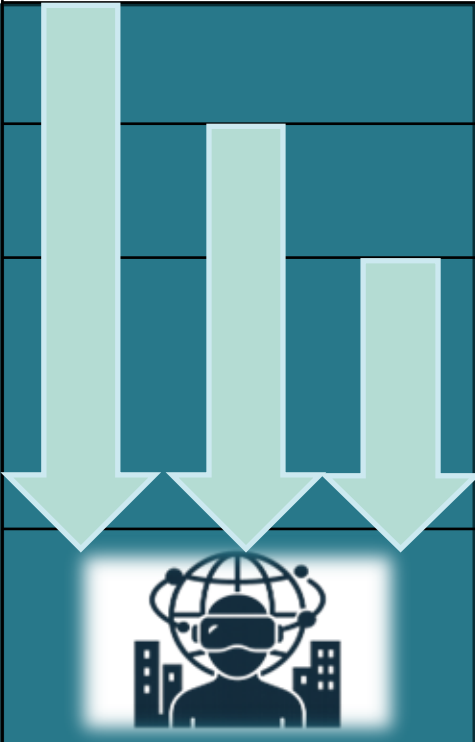
- Fortsetzung von **trackingbasierten Geschäftsmodellen** im Metaverse
- **Einwilligung** funktioniert schon im 2-dimensionalen Internet mehr schlecht als recht, im Metaverse gar nicht.
- Daher: Entweder **Vollzugsdefizit** oder **politische Lösungen**:
- **Einschränkungen von trackingbasierten Geschäftsmodellen** und **PIMS-Vorabereinwilligungen**

Persönlichkeitsrechte

- Risiken für Persönlichkeitsrechte werden von Nutzer:innen als **bedrohlich und akzeptanzgefährdend** empfunden.
- Daher im Prinzip gemeinsames Interesse von Nutzer:innen und Unternehmen, **Übergriffe und Täuschungen durch andere Nutzer:innen** zu vermeiden.
- Andere Interessenlage: **Einsatz von Social Bots von Plattformen / Shopanbietern für Datengenerierung / Kaufanbahnung**
- Daher: **Rechtsdurchsetzung und Politik** gefordert



Perspektiven für Rechtsdurchsetzung und Gesetzgebung

	Lösungsweg	Räumlicher Bezug		
		Deutschland	EU	International
	Gesetzesrecht	+	++	-
	Normung	(+)	++	(+)
	Unternehmensinterne Regelungen	(+)	+	+++
	Rechtsdurchsetzung	+++	+	-

