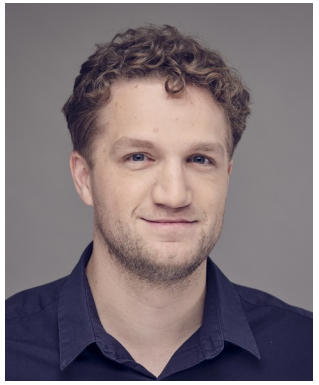
TECHNISCHE UNIVERSITÄT DRESDEN

CeTI Centre for Tactile Internet with Human-in-the-Loop

Zu Risiken und Anonymisierungen von Verhaltensbiometrie

Simon Hanisch, Julian Todt, Melanie Volkamer, Thorsten Strufe

Vorstellung



Simon Hanisch
Center for Tactile Internet (CeTI)
Technische Universität Dresden

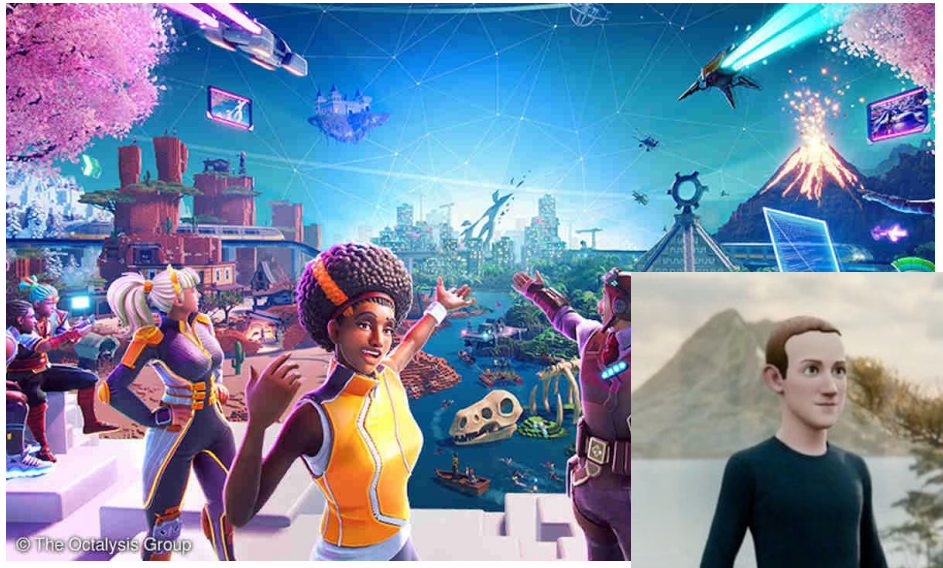
Julian Todt
Praktische IT-Sicherheit
Karlsruhe Institut für Technologie

Prof. Dr. Melanie Volkamer
SECUSO
Karlsruhe Institut für Technologie

Prof. Thorsten Strufe
Praktische IT-Sicherheit
Karlsruhe Institut für Technologie

Schöne neue Datenwelt?

- Neue Qualität:
  - Höhere Auflösungen,
  - Zuzätzliche Informationen (z.B. Tiefe)
- Neue Quantität:
  - Dauerhafte Aufnahme, Aufzeichnung von Dritten, ...
- Neue Arten:
  - Handbewegungen, Augenbewegungen, ...



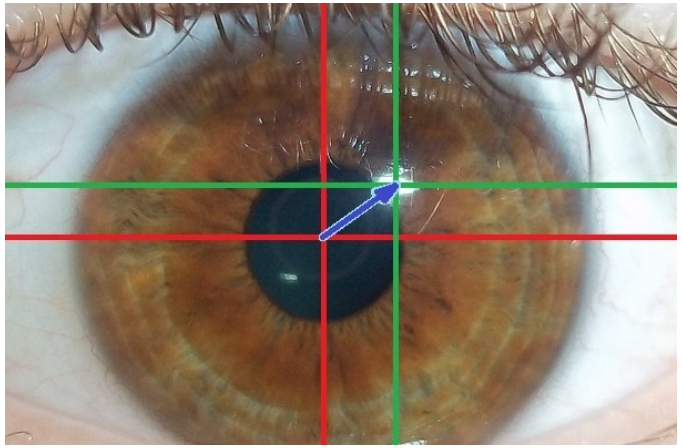
metaverse, octalysisgroup.com, Accessed: 2022

metaverse zuckerberg, meta, Accessed: 2022

Hololens 2, Microsoft, Accessed: 2022

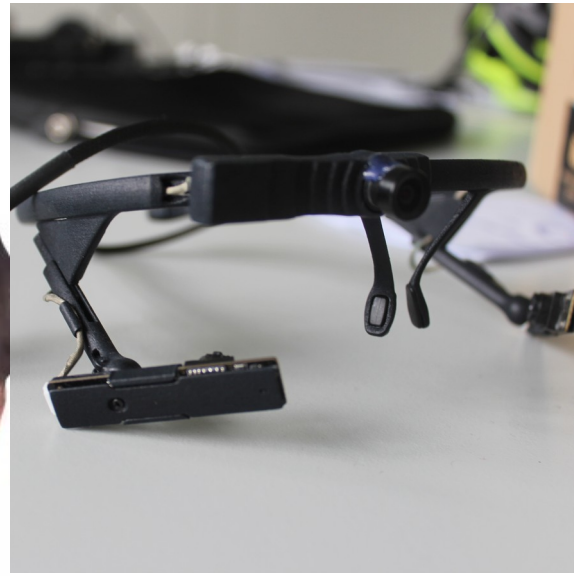
Eye-Tracking + Face-Tracking

- Erfasst in VR/AR Headsets
- Erkennen von Aufmerksamkeit, Emotionen, Geisteszustand ...
  - Liken ohne Likebutton



eye-tracking, wikipedia.org, Björn Markmann, 2015

- Eigenschaften: Augenbewegungen, Pupilenveränderungen, Blinzeln
- Inferenzen: Interessen, geistige Krankheiten, Identität, Drogenkonsum, Alter, Müdigkeit, Persönlichkeitsmerkmale

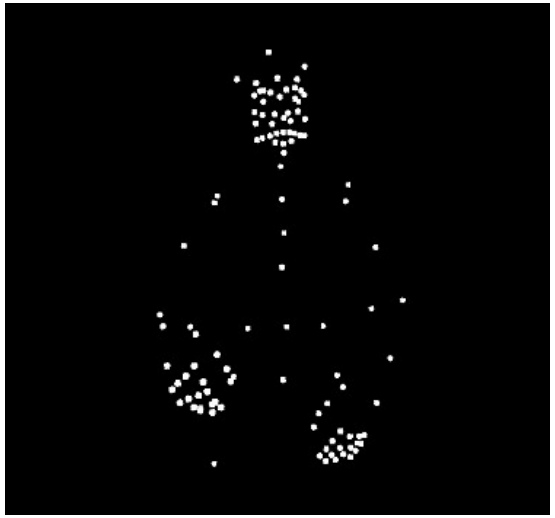


face-tracking, uploadvr.com, Accessed: 2022

Körperbewegungen

- Handbewegungen
- Gangerkennung
- Identifizierung von Personen
- Inferierung von Alter, Geschlecht, Gewicht, ..

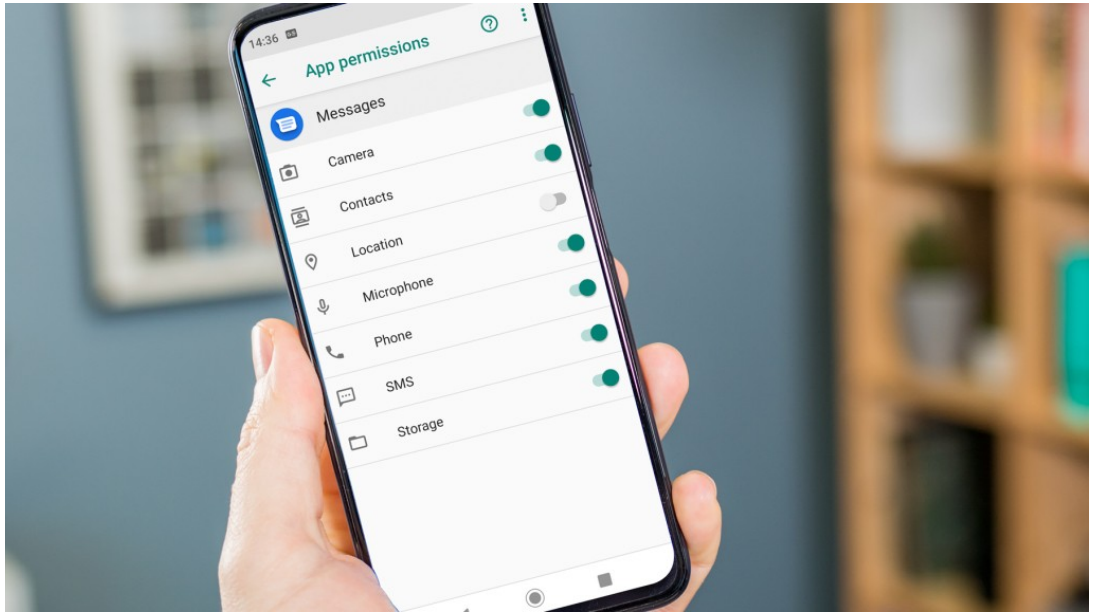
smartgloves, rokoko.com, Accessed: 2022



gait recognition, WildGait, Comas et al., 2021

Datenteilen heute

- Entscheidung über Art der Daten
- Alles oder nichts
- Betrieb ohne Datenteilen nicht möglich
- Problem: Verhalten lässt sich aus verschiedensten Arten von Daten herauslesen



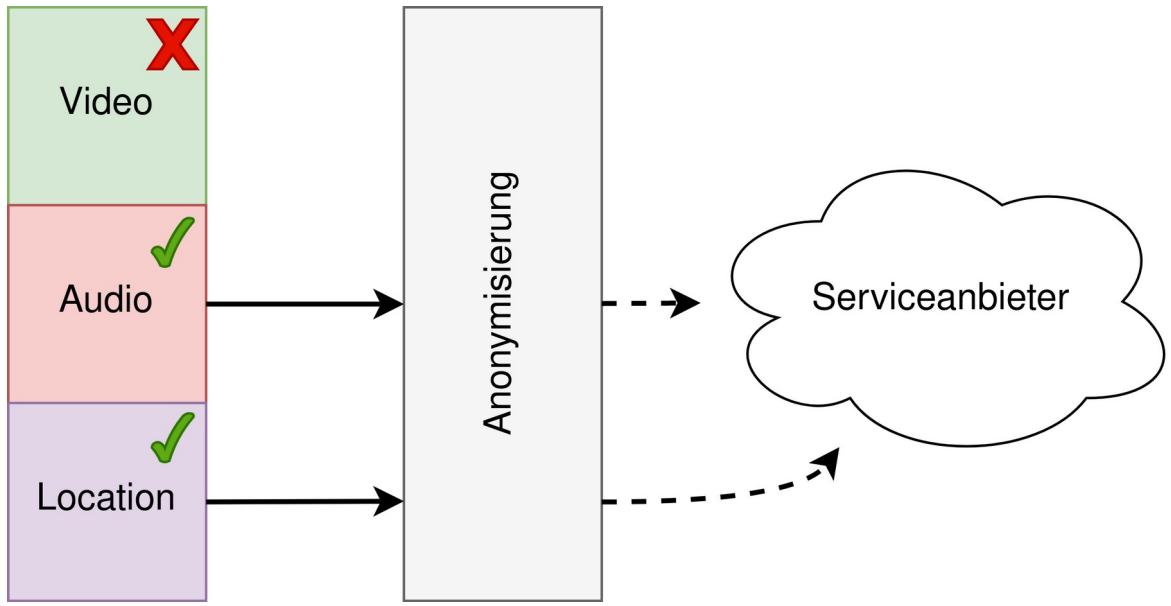
app permissions, techadvisor.com, Accessed: 2022

Feinere Datenteilung

- Nicht nur welche Daten, sondern wo und wofür:
  - Wo: nur auf dem Gerät?
  - Wofür: was darf mit den Daten nicht getan werden?
- Realisierung: Technisch und Rechtlich
  - Technisch: Anonymisierung
  - Rechtlich: Einschränkung an Daten koppeln

Allgemeines Szenario

- Kontrolle über Daten wird abgegeben
- Anonymisierung von Eigenschaften: Identität, Alter, Geschlecht, ..
- Kombinierung von Ansätzen möglich

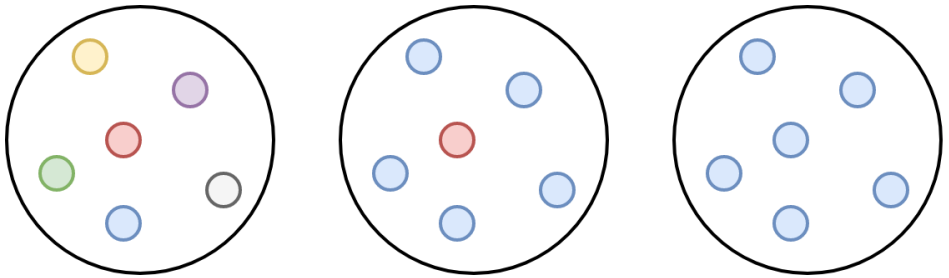


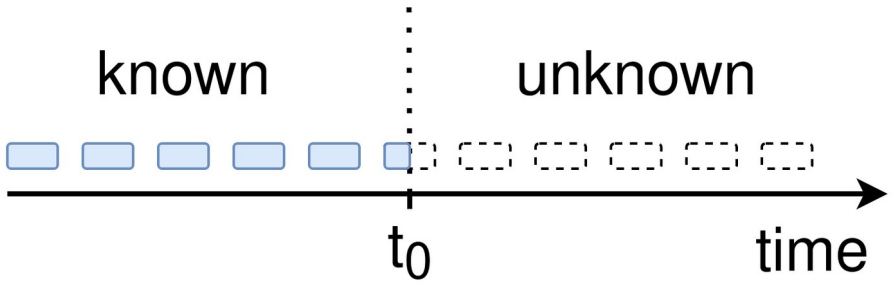
Einfache Anonymisierungsansätze

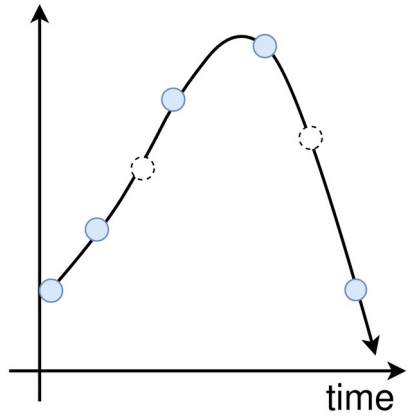
- Problem: sensible Daten sind nicht explizit
- Reduzierung
- Verrauschen
- Vergröbern

Anonymisierung von Verhaltensbiometrie

- Verhalten sind Aktionen über Zeit
- Rekonstruktion der Ursprungsdaten
- Hohe Vielfalt von Verhalten
- → Einfache Anonymisierungen funktionieren nicht für Verhalten

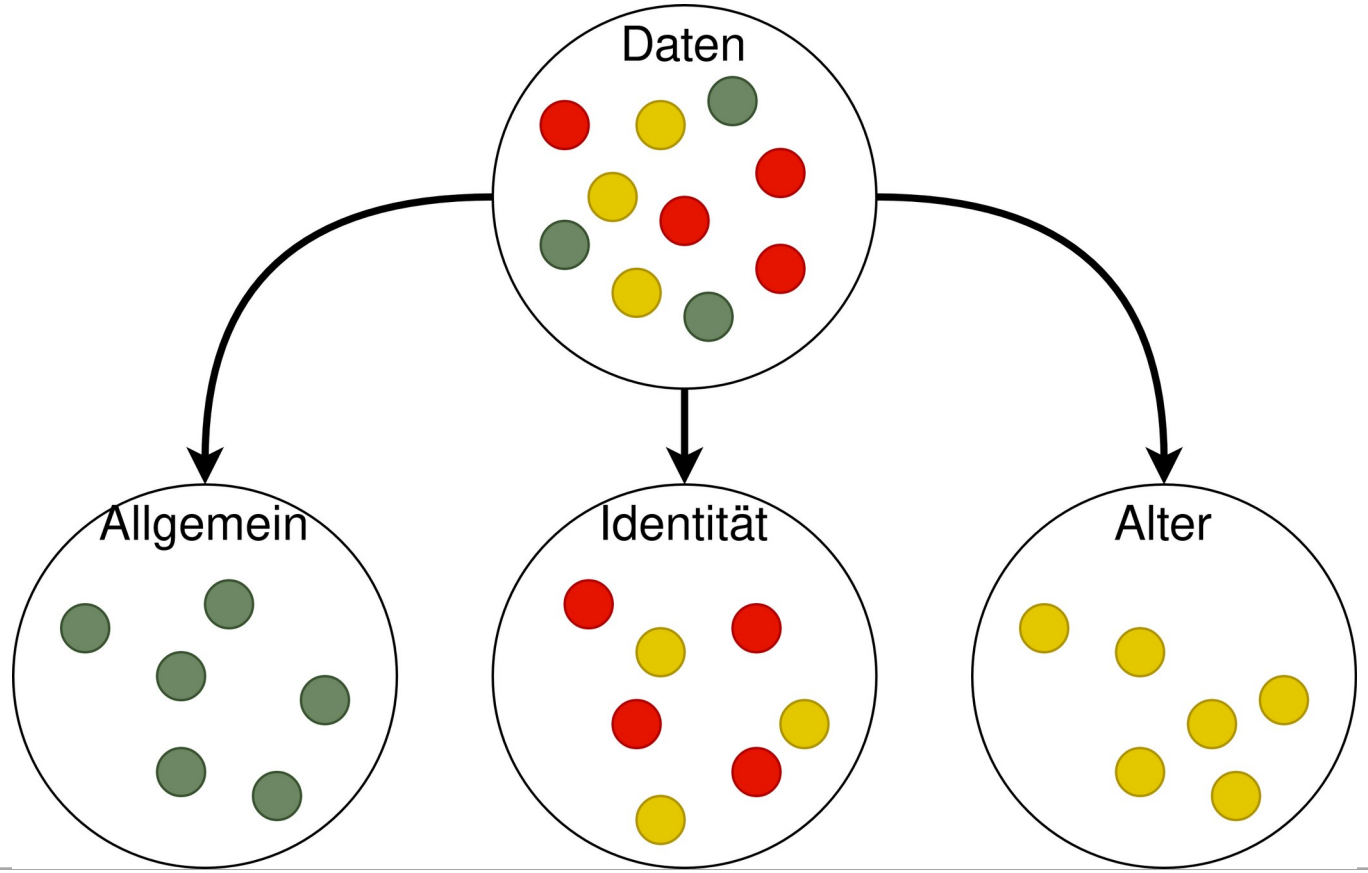






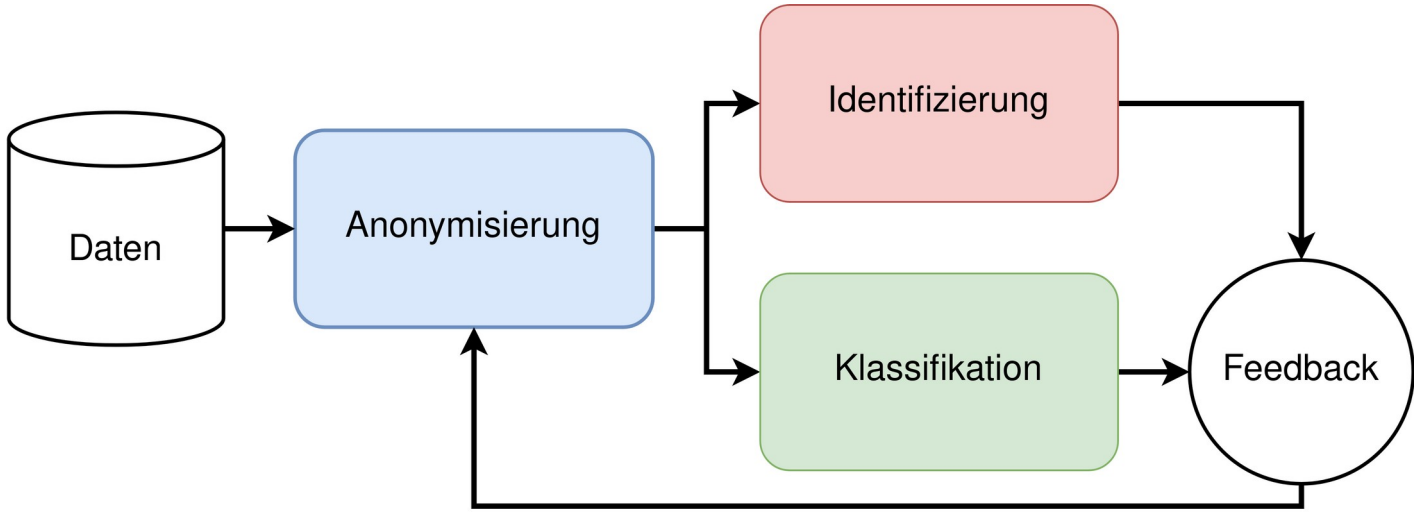
Welche Daten sind personenbezogen?

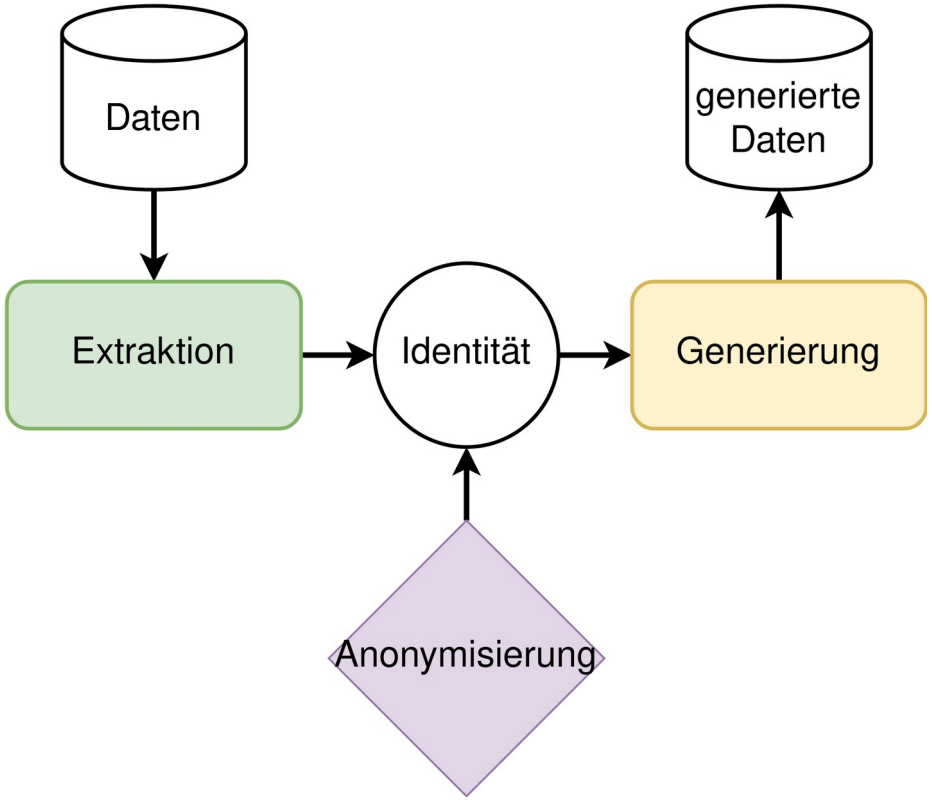
- Trennung der Daten in allgemeine und sensible Daten



Komplexere Anonymisierungen

- Synthetische Daten
- Feature entfernen mit Machine Learning





Zusammenfassung

- Höhere Qualität und Quantität von identifizierbaren Daten
- Teilen von Daten ist heute zu grob
- Nutzer schränkt ein wofür Daten genutzt werden dürfen/können
  - Mit rechtlichen und technischen Möglichkeiten realisierbar
- Neue Anonymisierungsmethoden benötigt