

PRIVACY



Administratives

Leistungsnachweis

- 30% Gruppenarbeit
 - 10% Executive Summary
 - 10% Präsentation
 - 10% Executive Summary (Recht)
- 70% Prüfung (Form: TBD)

Gruppenarbeit Note ist eine Gruppennote

Deadlines

-  03. März: Gruppenbildung
-  10. März: Executive Summaries

Inhalt

Big Data

collect massive amounts of (different) data from many different people.

Examples:

- Sensors (smart watch)
- Web Data, E-Commerce
- Mobile phones
 - GPS
 - Search entries
- E-mails, Social networks

Dimensions:

- Volume (amount of data)
- Velocity (speed of generation of the data)

- Variety (different kind of data)
- Veracity (quality of data)
- Value (commercial value of data)

Privacy

1. Personal privacy

Schutz einer Person vor unangemessenen Eingriffen die ihr moralisches Empfinden und Privatsphäre verletzen

2. Territorial privacy

Schutz eines physischen Bereichs um eine Person herum, der ohne Zustimmung der Person nicht verletzt werden darf.

3. Informational Privacy

Schutz vor missbräuchlicher Verarbeitung personenbezogener Daten sowie den Schutz des rechts auf informationelle Selbstbestimmung.

Privacy Control

- Pseudonymität -> seine Identität nicht preisgeben
- Unbeobachtbarkeit -> andere können nicht beobachten
- Unlinkability -> Absender und Empfänger können nicht als miteinander kommunizierend identifiziert werden
- Depersonalisierung -> meist nur wenig verändert (mit 2. er Database umkehrbar)

Digitale Identität

Digitale Identitäten repräsentieren die Nutzer in der Informationsgesellschaft. Solche digitalen Identitäten bestehen aus technisch abgebildeten Attributen der Nutzer.

-diebstahl: die missbräuchliche Nutzung personenbezogener Daten (der Identität) einer natürlichen Person durch Dritte.

Anonymität

Ein Subjekt ist anonym gegenüber einem Angreifer, wenn der Angreifer das Subjekt in einer Menge von Subjekten nicht hinreichend identifizieren kann.

Arten der Anonymität

- Sender und Empfängeranonymität -> Identität
- Ortsanonymität -> Attribute **Anonymisierung**
- der Prozess, um Anonymität zu erreichen

- personenbezogene Daten derart zu verändern, dass Einzelangaben nicht mehr oder nur sehr schwierig einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden.

Warum Anonymität?

- Tracking Vermeiden
- Vertrauliche persönliche Informationen (Abstimmung, politische Meinung)

Nicht einfach anonym geblieben:

- Netzwerk IP
- Web App
 - Cookies
 - Flash

Absolute Anonymisierung

Diese liegt vor, wenn niemand mehr in der Lage ist, den Personenbezug wiederherzustellen. Dies kann bspw. durch die Löschung von Identifikationsmerkmalen in einer Datenbank erfolgen.

Tracking

Cookies

- Werden unter den Domainnamen des Webserver abgespeichert und bei jeder neuen Abfrage an diesen Webserver zurückgeschickt.
- Zweck: HTTP selbst ist zustandslos

1st Party cookies

- von der Website gesetzt auf der ein User gerade surft
- werden von Browsern nicht

3rd Party Cookies

- Durch einen Dritten gesetzt, also nicht durch die eigentliche Website, auf der man sich befindet.
- Häufig von Advertisern gespeichert, die Werbung auf

Cookie syncing

- Firmenübergreifende Daten, gespeichert mit Cookies

Fingerprint

Browser-Fingerprinting

- Reguläre Web-Interaktionen werden benutzt um Informationen über dich zu sammeln und dich zu identifizieren

Vermeiden

- Javascript deaktivieren
- Cookies deaktivieren

Mobile Tracking



Location Tracking

TPEG-Zugriff (Transport Protocol Experts Group)

ist eine Serie von Datenprotokollen für die Übertragung von Verkehrs- und Reiseinformationen.

Gesichtserkennung

1. Gesichtsfindung
2. Referenzpunktdetektor (Augen, Nase, Mund, etc.)
3. Gesichtserkennung
 - Identifikation
 - Verifikation
 - Analyse

RFID

Short	meaning
RFID	radio frequency identification
NFC	near field contact

E-Passport

Für das Auslesen von Fingerabdrücken / einfordern von sensiblen Daten wird ein Auslese-zertifikat benötigt.

Access Control

Basic Access Control (BAC) ermöglicht den Zugriff auf grundlegende Passdaten, während Extended Access Control (EAC) verschlüsselte Kommunikation und Zugriff auf biometrische Daten ermöglicht.

Crowds

Webanfragen hinter anderen Crowds Dienstenutzer verbergen. Jeder Benutzer hat eine Applikation installiert (Jondos). Der Traffic wird über zufällige "Jondos" weitergeleitet.

Mix

Nachrichten werden nicht direkt an den Empfänger gesendet, sondern werden über zufällige Mixes gesendet.

Grundfunktionen:

1. Löschen von Duplikaten
2. Sammeln von Nachrichten
3. Umkodierung der Nachrichten
4. Umsortieren der Nachrichten

Anonymisierung

Generalisieren

Beispiel PLZ:

4012 4011 4019 -> 401*

k-Anonymität

k-Anonymität tritt immer dann auf wenn ein Eintrag k-mal in einer Liste auftaucht. Beispiel PLZ: für 3-k tritt der Eintrag 401* drei mal auf.