Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

NFDI × CS

GESELLSCHAFT FÜR INFORMATIK

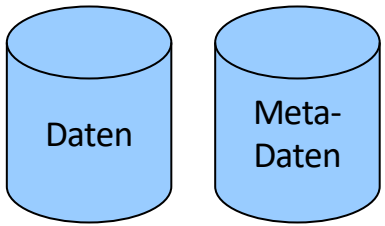
Datensicherheit im Forschungsdatenmanagement

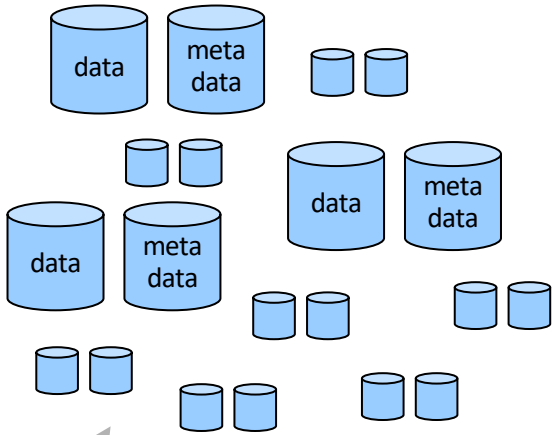
Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de

Forschungsdaten-Soiree #1: Forschungsdaten im Hochleistungsrechnen (HPC) und Datensicherheit,
19. August 2021

Datensicherheit im Forschungsdatenmanagement

- Systeme haben
  - Primäreigenschaften





F A I R principles
- reusable
- interoperable
- accessible
- findable

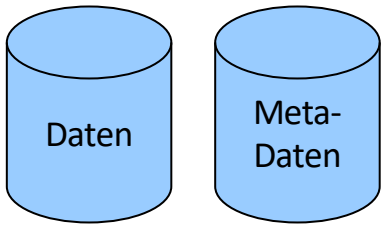
  - Sekundäreigenschaften
    - Verteiltheit
    - Datensicherheit

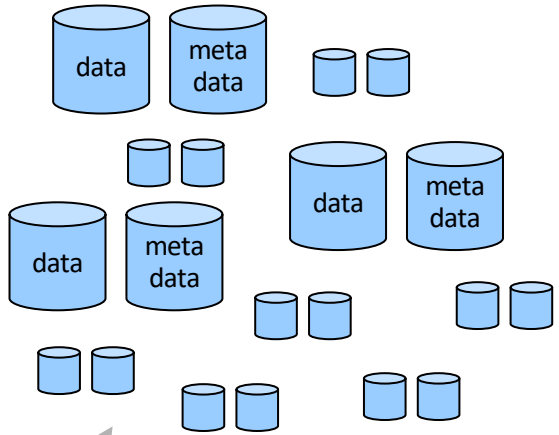
Bedrohungen:
- unbefugter Informationsgewinn
- unbefugte Modifikation
- unbefugte Beeinträchtigung von Funktionalität

Schutz der
- Vertraulichkeit
- Integrität
- Verfügbarkeit

Datensicherheit im Forschungsdatenmanagement

- Systeme haben
  - Primäreigenschaften





  - Sekundäreigenschaften
    - Verteiltheit
    - Datensicherheit

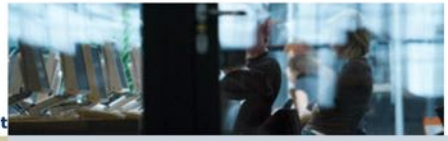
Angreifermodell

1. Wer könnte welche Schutzziele und Prinzipien wie verletzen wollen?
2. Welche Schutzmaßnahmen schützen vor dem Angreifer?

F A I R principles
- reusable
- interoperable
- accessible
- findable

Datensicherheit
- Security
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
- Safety
  - Fehlertoleranz
  - Korrektheit

Ethische Aspekte, Datenschutz, Urheberrecht und verwandte Schutzrechte



HUMBOLDT-UNIVERSITÄT ZU BERLIN

Forschungsdatenmanagement
- Willkommen
- Mit Forschungsdaten arbeiten
- Forschungsdaten teilen
  - Repositorium finden
  - Dokumentation und Metadaten
  - **Rechtliche Aspekte**
    - Lizenz wählen
  - Persistente Identifikation
- Informationen
- Support
- Störungsmeldungen

Studierende | Mitarbeiter/innen

Humboldt-Universität zu Berlin | Computer- und Medienservice | Forschungsdatenmanagement | Forschungsdaten teilen | Rechtliche Aspekte

Rechtliche Aspekte

Hier werden Übersichten zu den relevanten Rechtsgebieten und Paragraphen, zu Ansprechpartnern innerhalb der Humboldt-Universität sowie Literaturempfehlungen gegeben.

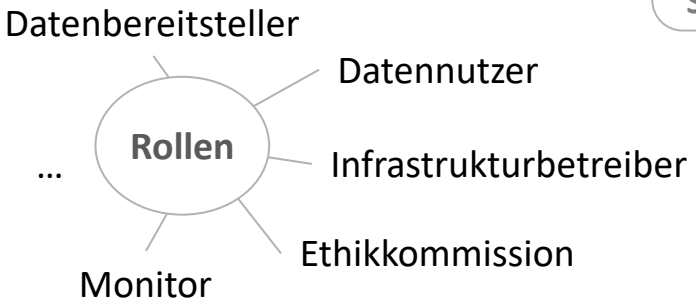
Vor allem, wenn eine Publikation von Forschungsdaten erfolgen soll, sind bestimmte rechtliche Bedingungen vorab zu klären. Aber auch die reine Verarbeitung von Daten kann mit rechtlichen Einschränkungen einhergehen. Es sollte daher vorab geprüft werden, welche der nachfolgenden Rechtsgebiete gegenfalls berücksichtigt werden müssen. Darüber hinaus können weitere Rechtsgebiete von Bedeutung sein, die hier nicht aufgeführt sind. Welche Rechte und Gesetze zu beachten sind, ist daher immer als Einzelfallprüfung anzusehen.

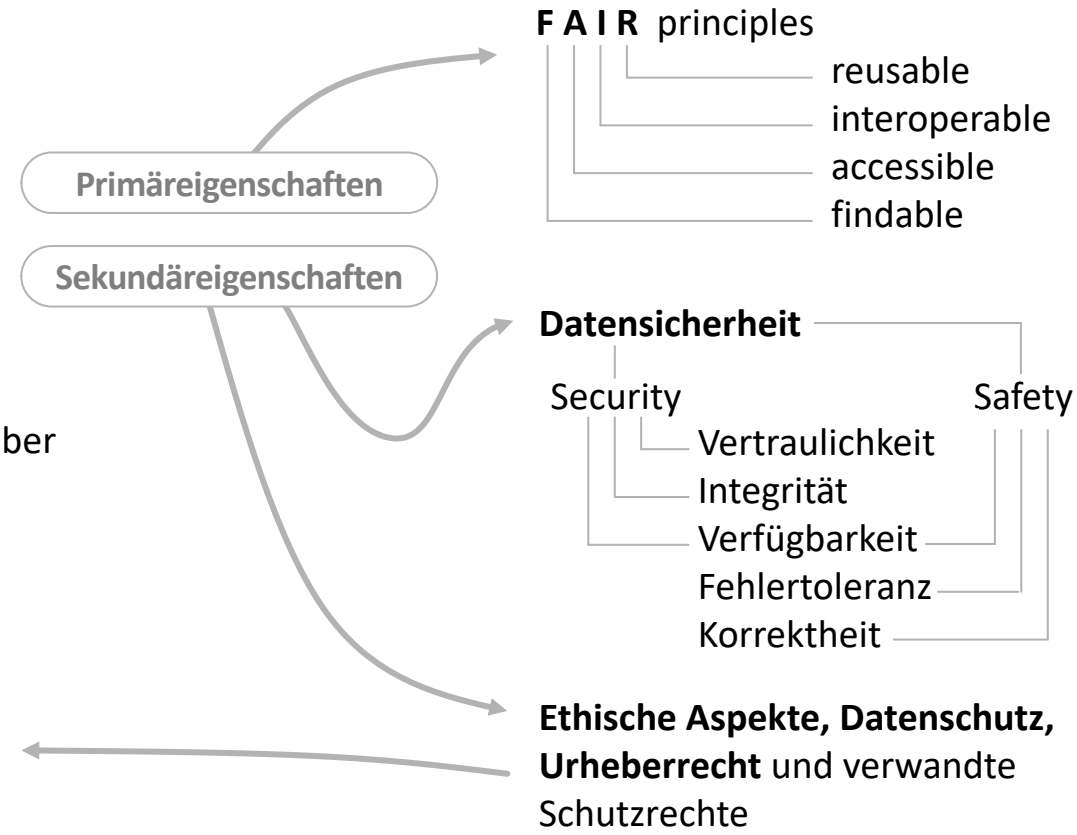
Relevante Rechtsgebiete im Forschungsdatenmanagement:

- **Urheberrecht** (z. B. Schutzfähigkeit: §2 UrhG, §3 Satz 1 UrhG; Miturheberschaft: §8 UrhG; Ablauf der Schutzfrist: §64 UrhG, §72 Abs. 3 UrhG)
- **Persönlichkeitsrecht** (z. B. Recht am eigenen Bild: §22 KunstUrhG)
- **Datenschutz** (z. B. Rechtmäßigkeit der Verarbeitung: u. a. §27 BDSG, Art. 6 DSGVO, Art. 17 Abs. 3 lit. d DSGVO; informierte Einwilligung: u. a. §36 BlnDSG, Art. 13 DSGVO)
- **Datensicherheit** (u. a. §64 BDSG)
- **Datenbankrichtlinien** (z. B. Schutzfähigkeit: EU-Richtlinie 96/9/EG, §4 Abs. 2 UrhG, §87a UrhG; Ablauf der Schutzfrist: §87d UrhG)
- **Softwarerecht** (UrhG Abschnitt 8)
- **Lizenzierung*** (u. a. §31 UrhG, z. B. Creative Commons Lizenzen)
- **Policies** (Universität, disziplinär, Verlage)
- **Förderbedingungen** (z. B. Drittmittelprojekte: BMBF, DFG, EU)
- **Arbeits- und Dienstrecht** (z. B. Nutzungs- und Verwertungsrechte, die im Arbeitsvertrag geregelt werden: u. a. §43 UrhG)
- **Vertragsrecht** (u. a. BGB Abschnitt 3, z. B. Kooperationsverträge oder Geheimhaltungsabreden)
- **Patentrecht** (PatG)
- **Wettbewerbsrecht** (UWG, z. B. bei Kollaborationen mit Unternehmen)
- **Internationales Recht** (z. B. Gültigkeit nationaler Vorschriften bei Forschung mit ausländischen Kooperationspartnern)
- **Grundrechte** (z. B. Wissenschaftsfreiheit: Art. 5 Abs. 3 Satz 1 GG)

Datensicherheit im Forschungsdatenmanagement

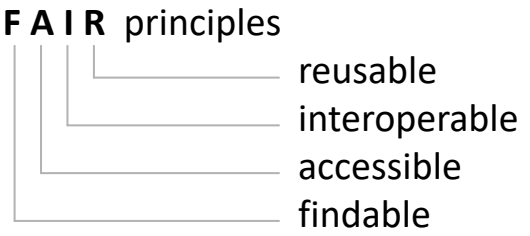
- Herausforderungen
  - heterogene Systemumgebungen
  - viele verschiedene Player
  - kompliziertes Rollenmodell

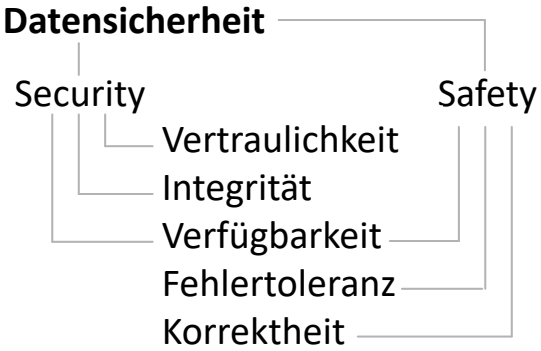




Daten sind für die Ewigkeit offen im System gespeichert

- Was geschieht, wenn Daten zurückgezogen werden müssen?
  - z. B. weil Privatheit (doch) verletzt wurde?
- Antwort: Präventiv alles unternehmen, um es nicht erst so weit kommen zu lassen



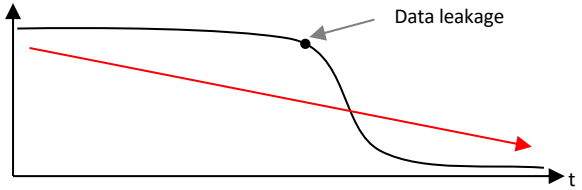


Ethische Aspekte, Datenschutz, Urheberrecht und verwandte Schutzrechte

Beobachtungen zum Monotonieverhalten

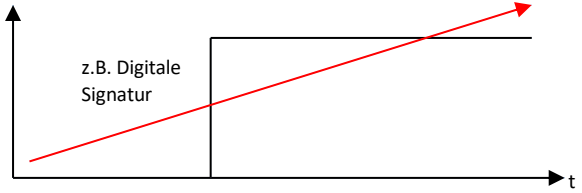
- Das Monotonieverhalten von Schutzzielen gibt Hinweise auf die Prioritäten bei der Umsetzung von Schutzzielen und das praktisch erreichbare Schutzniveau.

Vertraulichkeit



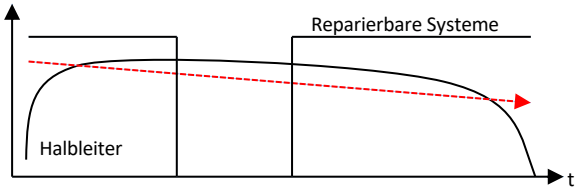
Vertraulichkeit, Verdecktheit, Anonymität und Unbeobachtbarkeit können nur geringer werden. Sensible Daten müssen besonders sorgsam und mit hoher Priorisierung geschützt werden

Integrität



Integrität, Zurechenbarkeit und Rechtsverbindlichkeit können nur größer werden. Ist einmal die Authentizität von Daten (auf technischer Ebene) festgestellt, geht sie nicht mehr verloren.

Verfügbarkeit

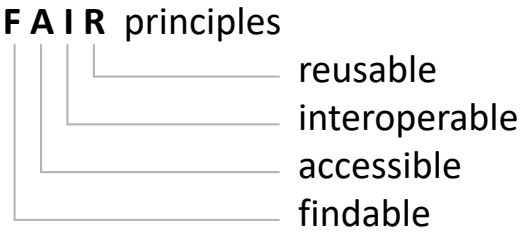


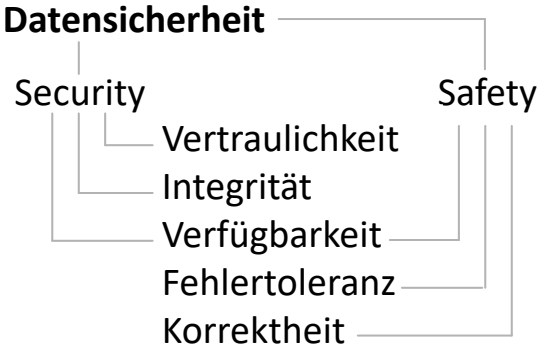
Verfügbarkeit und Erreichbarkeit verhalten nicht monoton (häufig unstetig und doch langfristig meist regressiv). Es sind nur probabilistische Aussagen zur Verfügbarkeit möglich.

Daten sind für die Ewigkeit offen im System gespeichert

- Was geschieht, wenn Daten zurückgezogen werden müssen?
  - z. B. weil Privatheit (doch) verletzt wurde?
- Antwort: Präventiv alles unternehmen, um es nicht erst so weit kommen zu lassen, d.h.
    - Pseudonymisierung und Anonymisierung

Hinsichtlich der Wirksamkeit von Pseudonymisierung und Anonymisierung sollten man aber nicht zu optimistisch sein.





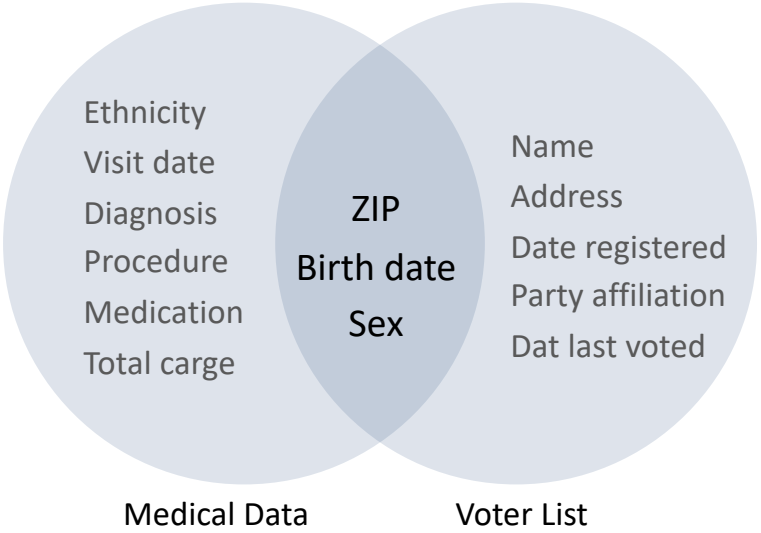
Ethische Aspekte, Datenschutz, Urheberrecht und verwandte Schutzrechte

Verknüpfung von Datensätzen gefährdet Anonymität

Latanya Sweeney, 2000

Vermeintlich anonymes medizinisches Register mit Daten von US-Bürgern…

…wurde verknüpft mit öffentlich zugänglichen US-Wählerverzeichnissen



Beide Datensätze enthalten Geschlecht, Geburtsdatum, Postleitzahl.

Ergebnisse:

- Identifizierung der Krankenakte des ehem. Gouverneurs von Massachusetts, William Weld, war möglich
- Insgesamt 87 Prozent der US-Bevölkerung kann re-identifiziert werden

Latanya Sweeney entwickelte das Konzept der k-Anonymität.

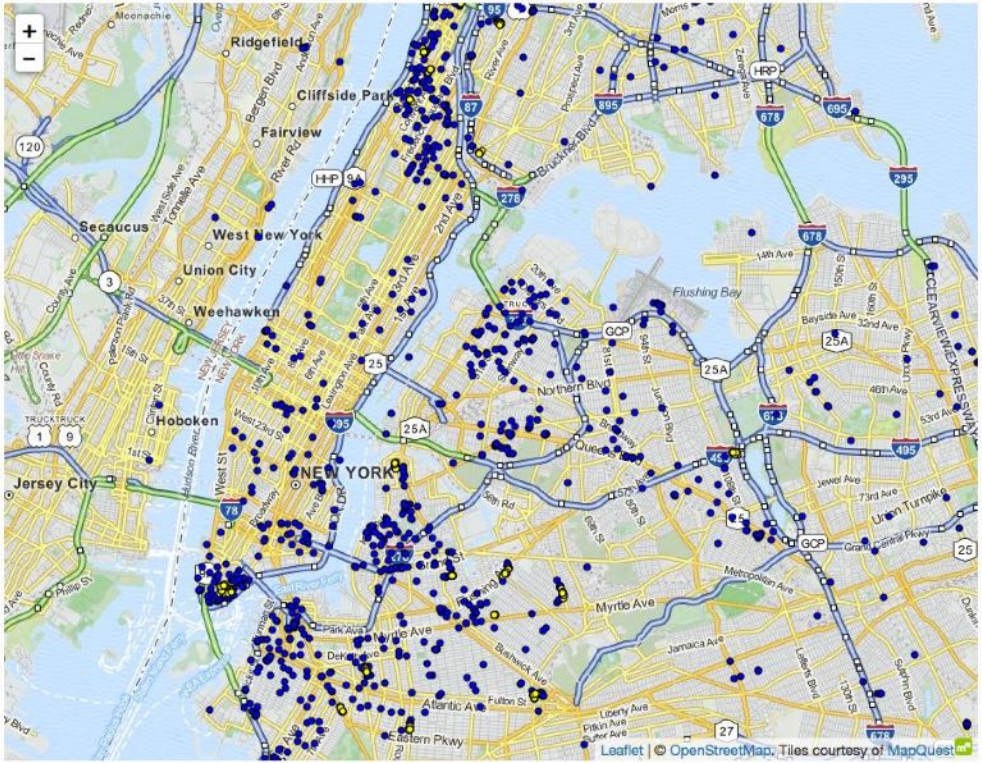
Pseudonymisierte Daten…

…können Persönlichkeitsrechte verletzen.

20 GByte of pseudonymisierter Daten von 170 Mio. Taxifahrten der New Yorker Taxi-gesellschaft

Daten öffentlich abrufbar unter:

http://www.andresmh.com/nyctaxitrips/



Drop-off locations for trips starting at Larry Flynt's Hustler Club between midnight and 6 am during 2013.

Source: http://content.research.neustar.biz/blog/differential-privacy/stripRaw.html

Neubestimmung des Begriffs personenbezogene Daten

Nach: Hoffmann-Riem 2018, S.55

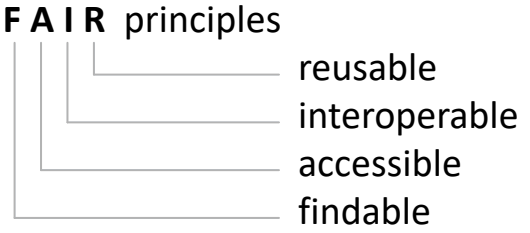
- Personenbezogene Daten sind auch Daten, die als Ergebnis einer Big-Data-Analyse entstehen.
  - allgemein und ohne Herleitung aus Daten speziell der konkret betroffenen Person
  - Beispiele: Person wohnt in einem bestimmten Stadtteil; daraus Ableitung von Finanzkraft, Herkunft, sexueller Orientierung, Gesundheit
- Personenbezogene Daten sind auch Daten, deren Personenbezug durch Anonymisierung entfällt.
  - Möglichkeiten der Deanonymisierung und Ableitung von Eigenschaften dürften nicht unterschätzt werden
  - Beispiele: New York Taxi Data Analytics, Strava Heatmap
- ebenso kritisch pseudonymisierte, aggregierte, perturbierte, verschlüsselte Daten betrachten

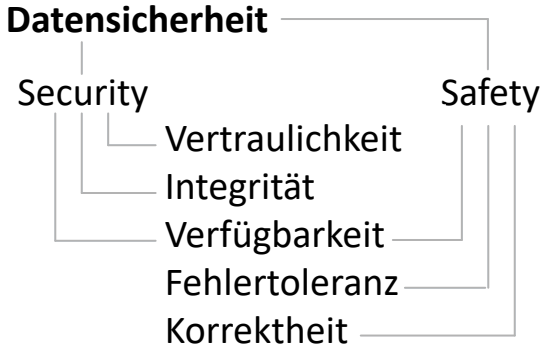
Daten sind für die Ewigkeit offen im System gespeichert

- Was geschieht, wenn Daten zurückgezogen werden müssen?
  - z. B. weil Privatheit (doch) verletzt wurde?
- Antwort: Präventiv alles unternehmen, um es nicht erst so weit kommen zu lassen, d.h.
    - Pseudonymisierung und Anonymisierung

Hinsichtlich der Wirksamkeit von Pseudonymisierung und Anonymisierung sollten man aber nicht zu optimistisch sein.

- Wenn Prävention nicht die Lösung ist:
  - Protokollierung und Monitoring
- Neue Fragen: Wer darf auf die Protokolle zugreifen? Wie lange die Protokolle aufbewahren?





Ethische Aspekte, Datenschutz, Urheberrecht und verwandte Schutzrechte

inf.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

DEPARTMENT OF INFORMATICS
SECURITY AND PRIVACY

HOME COURSES THESES RESEARCH PEOPLE SERVICE

UHH → MIN-Fakultät → Fachbereich Informatik → Einrichtungen → Arbeitsbereiche → Security and Privacy → Home

WORKING GROUP ON «SECURITY AND PRIVACY»

Security and Privacy

Information systems become more and more important in critical infrastructures, while the Internet has evolved to a critical infrastructure itself. The secure operation of these infrastructures is vital and their failure can have severe impacts up to the loss of human lives.
Security refers to the fact that protection goals are achieved in the presence of malicious attacks and system failures. Typical security goals can be confidentiality, integrity, accountability, and availability. Security and privacy in information systems addresses both technical and organizational aspects, such as building and establishing security concepts and security infrastructures as well as risk analysis and risk management.
Privacy can be a conflicting goal to security, but they can also benefit from each other. Hence, it is necessary to balance both when developing secure information systems.

Prof. Dr. Hannes Federrath
Fachbereich Informatik
Universität Hamburg
Vogt-Kölln-Straße 30
D-22527 Hamburg

Telefon +49 40 42883 2358

federrath@informatik.uni-hamburg.de

https://svs.informatik.uni-hamburg.de

Der Arbeitsbereich Sicherheit in Verteilten Systemen (SVS)

- Unsere Forschungsthemen (Auswahl)
  - IT-Sicherheitsmanagement, und -Grundschutz, ISO 27001
  - Privacy im Internet, Schutz vor Beobachtung, IT-Forensik
  - Sichere und datenschutzfreundliche Vernetzung von Fahrzeugen
  - Sicherheit und Datenschutz in mobilen Systemen

- Beiträge und (interdisziplinäre) Ergebnisse
  - Begleitung von Gesetzgebungsverfahren aus technischer Sicht
  - Erforschung des Spannungsfeldes von Freiheit und Sicherheit
  - Technische Lösungen zum Grundrechtsschutz
  - Informatik als gesellschaftliche Aufgabe

- Weitere Informationen
  - https://svs.informatik.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG