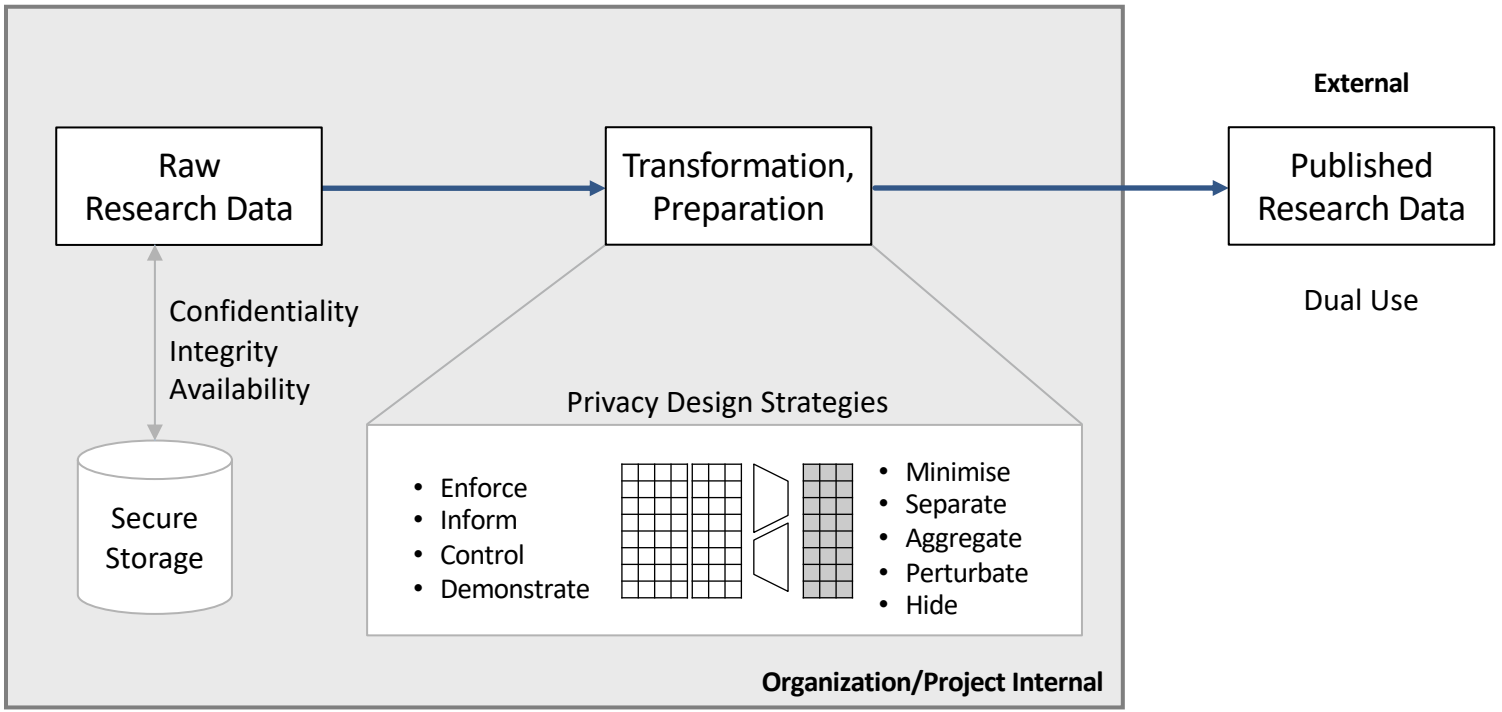
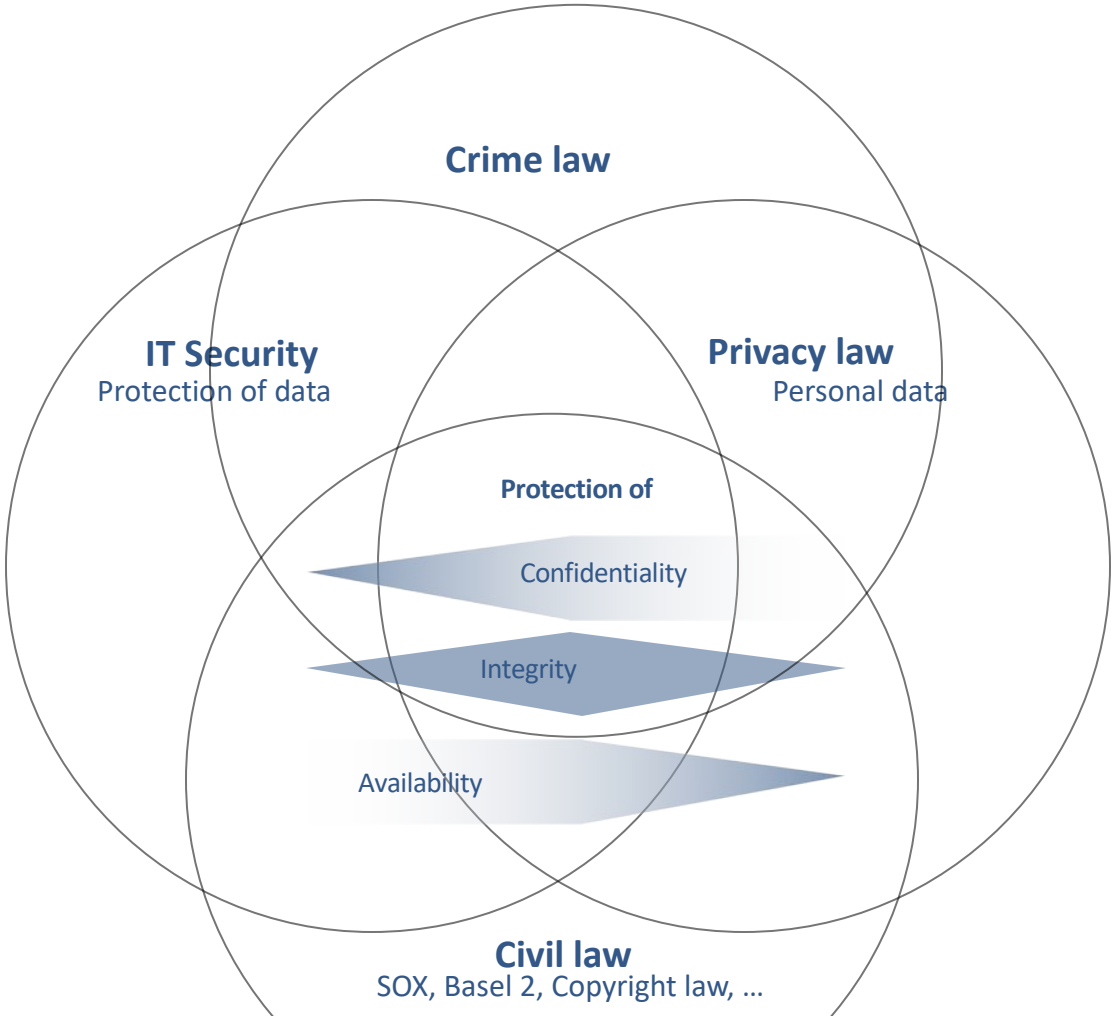
Privacy, Security and Dual Use

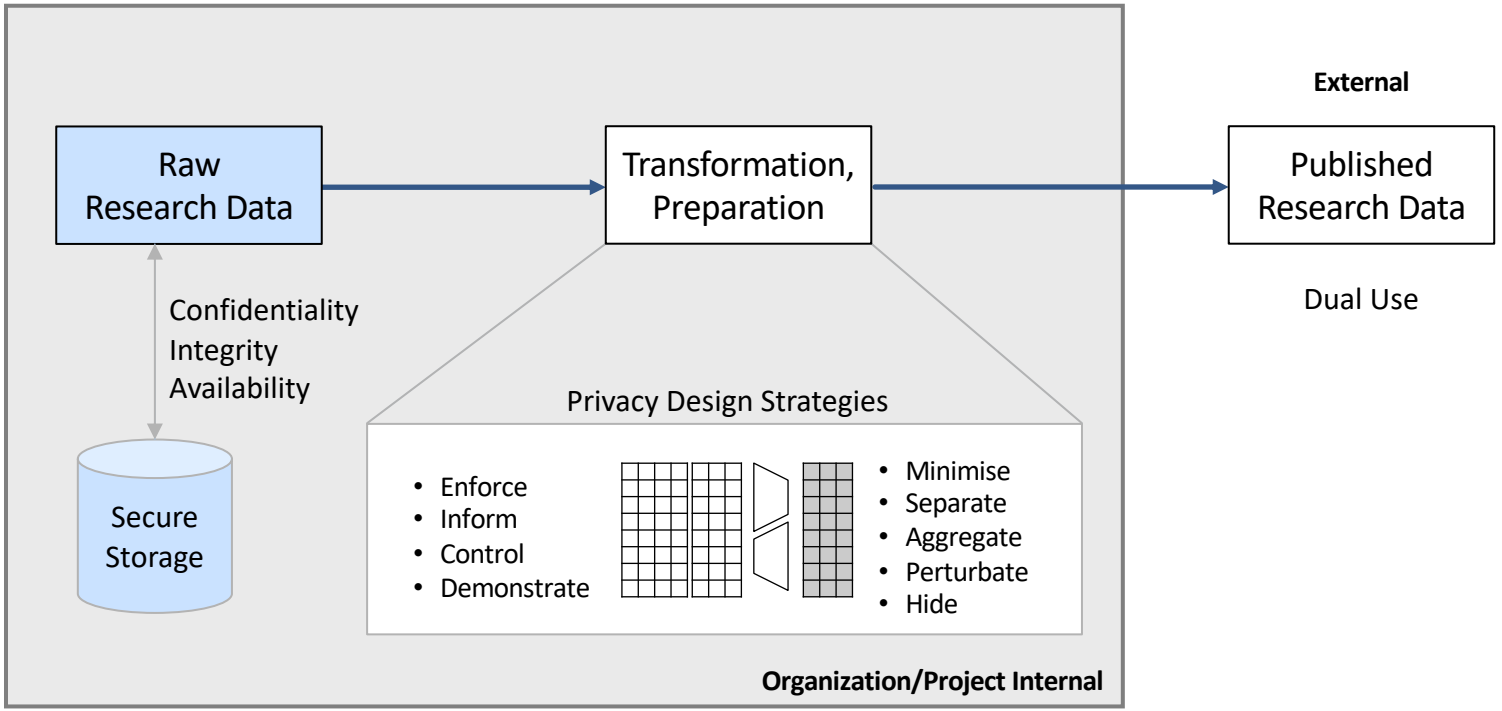
Hannes Federrath, Judith Simon

Data Transformation process

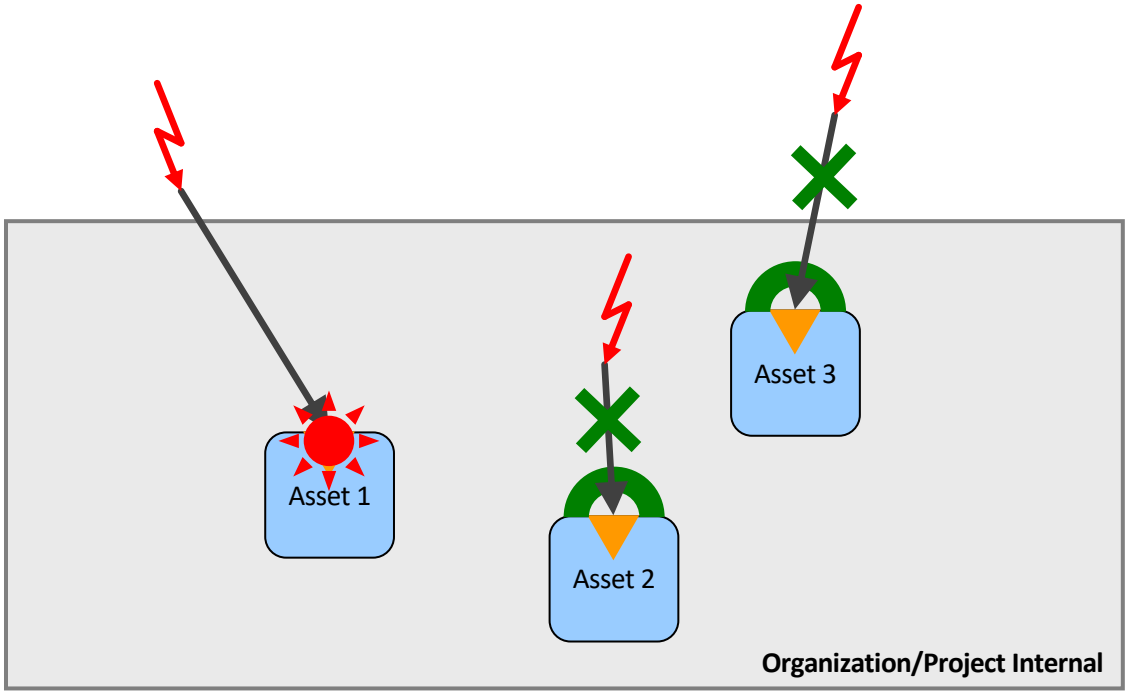



Crime law
IT Security
Protection of data
Privacy law
Personal data
Protection of
Confidentiality
Integrity
Availability
Civil law
SOX, Basel 2, Copyright law, …

Data Transformation process



From threats to a security event



Threats, z.B.
- Viruses, Worms
- DoS
- Hacking
- Espionage
- Social Engineering

Vulnerabilities, z.B.
- Configuration flaws
- Buffer Overflows

Protection Goals
- Confidentiality
- Integrity
- Availability

Security Measures
- Preventive
- Detective
- Reactive

Protection goals of multilateral security

Contents	Metadata
Confidentiality Hiding	Anonymity Unobservability
Contents	Sender, Location, Recipient
Integrity	Accountability Authenticity
Contents	Sender, Payment, Recipient
Availability	Reachability
Contents	Users, Systems

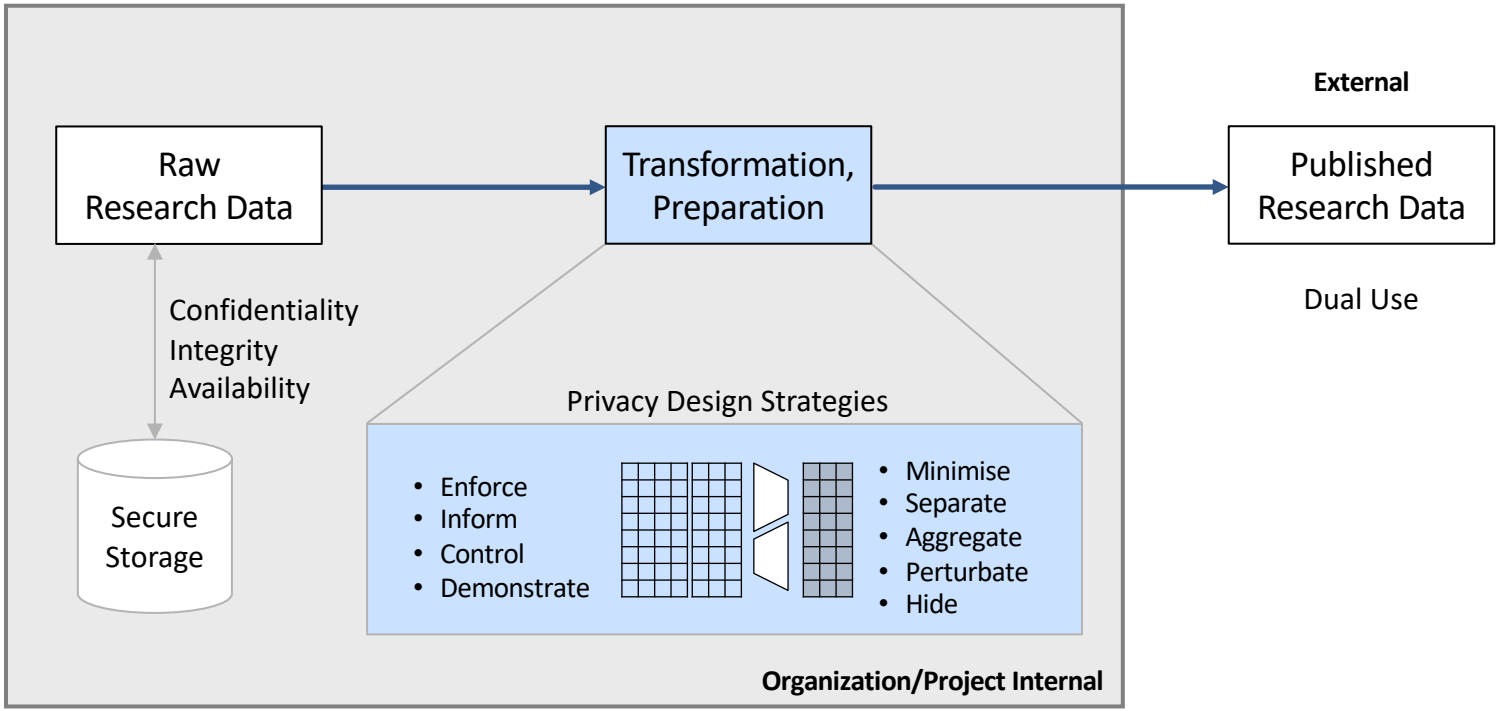
Threats, z.B.
- Viruses, Worms
- DoS
- Hacking
- Espionage
- Social Engineering

Vulnerabilities, z.B.
- Configuration flaws
- Buffer Overflows

Protection Goals
- Confidentiality
- Integrity
- Availability

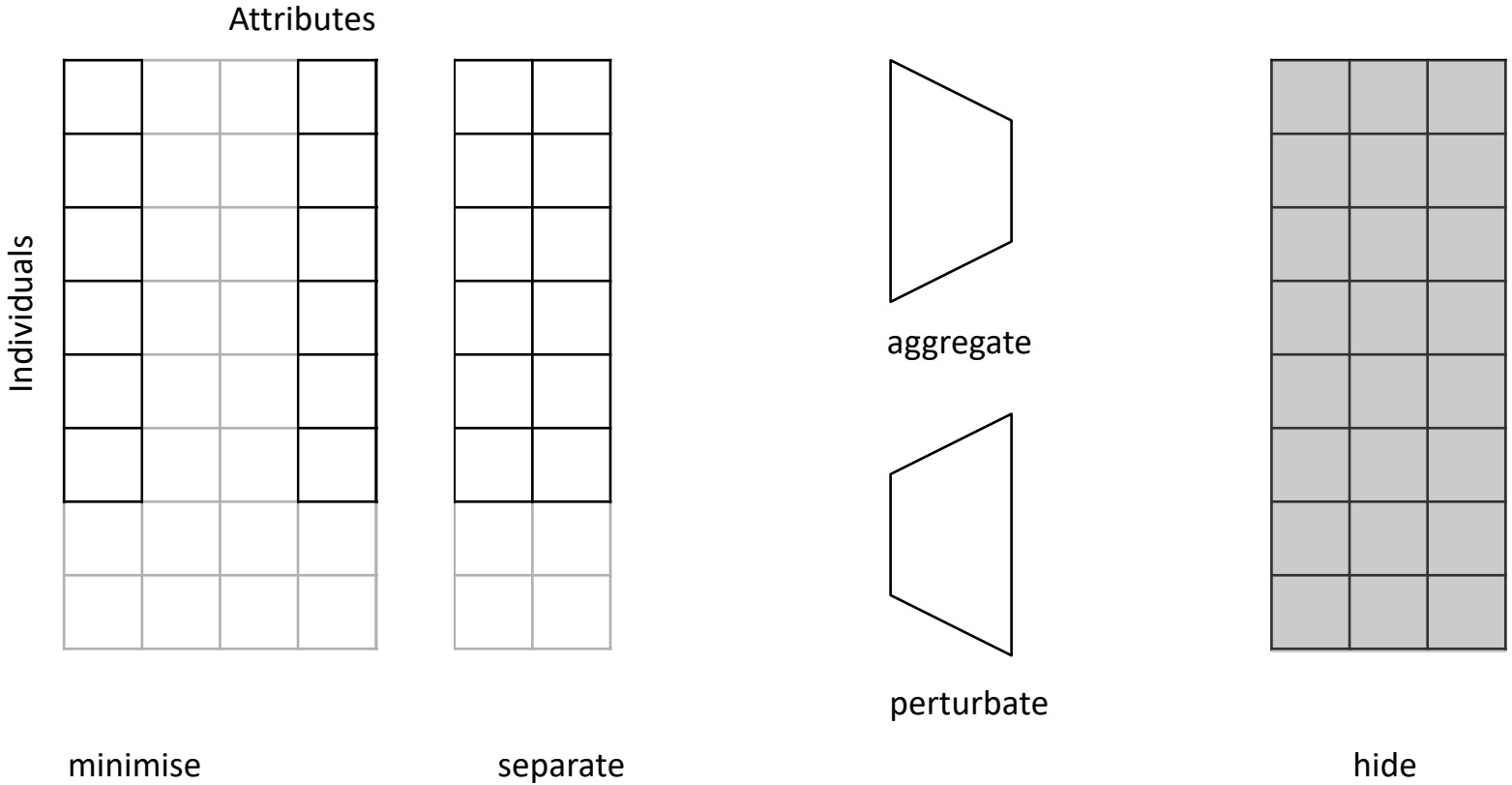
Security Measures
- Preventive
- Detective
- Reactive

Data Transformation process



Privacy design strategies

cf. Hoepman, 2014



Privacy design strategies

cf. Hoepman, 2014

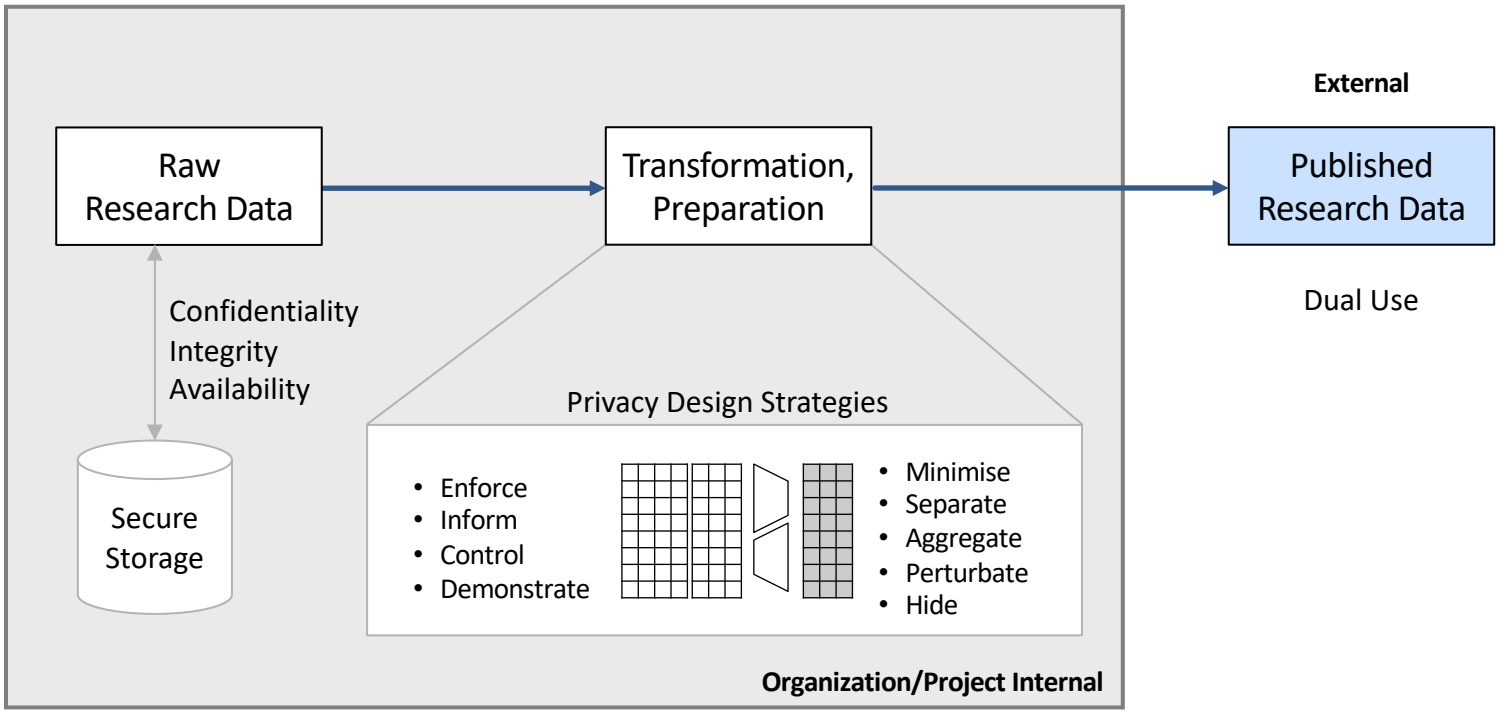
- Technical strategies
  - Minimise:
    - The amount of personal data that is processed should be restricted to the minimal amount possible.
  - Separate:
    - Personal data should be processed in a distributed fashion, in separate compartments whenever possible.
  - Aggregate and Perturbate:
    - Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.
  - Hide:
    - Any personal data, and their interrelationships, should be hidden from plain view.

Privacy design strategies

cf. Hoepman, 2014

- Organizational strategies
  - Enforce:
    - A privacy policy compatible with legal requirements should be in place and should be enforced.
  - Inform:
    - Data subjects should be adequately informed whenever personal data is processed.
  - Control:
    - Data subjects should be provided agency over the processing of their personal data.
  - Demonstrate:
    - Be able to demonstrate compliance with the privacy policy and any applicable legal requirements.

Data Transformation process



Zivil clause in our faculty

An der UHH hat die Fakultät für Mathematik, Informatik und Naturwissenschaft auf Basis eines Fakultätsratsbeschlusses eine „Zivilklausel“ in ihre Satzung aufgenommen (vergleiche § 5 Absatz 4 Grundordnung UHH, § 92 Absatz 1 S. 1 HmbHG):

> „Die MIN-Fakultät will allein zu friedlichen Zielen beitragen und nur zivile Zwecke erfüllen. Ihre Mitglieder richten deswegen Forschung und Entwicklung, Studium und Lehre auf zivile Fragestellungen und Anwendungen aus.“

(Auszug aus der Präambel der Satzung der Fakultät für Mathematik, Informatik und Naturwissenschaften (MIN) der Universität Hamburg vom 01.02.2017).

https://www.fid.uni-hamburg.de/satzung-fak-min.pdf

Dual Use

„Als **Dual-Use-Güter** – also Güter mit doppeltem Verwendungszweck – werden in der Regel Produkte bezeichnet, die sowohl für zivile als auch für militärische Zwecke eingesetzt werden können. Der Wortgebrauch hat sich inzwischen auch auf kriminelle und terroristische Zwecke ausgeweitet. Im Forschungskontext benennt Dual-Use meist solche Forschungsergebnisse und -methoden, die sowohl für friedliche bzw. nützliche Zwecke als auch zum absichtlichen Schädigen von Gesellschaft oder Umwelt eingesetzt werden können.“

https://www.leopoldina.org/ueber-uns/kooperationen/gemeinsamer-ausschuss-dual-use-2/dual-use-faq/#c8475

Dual Use

https://www.leopoldina.org/ueber-uns/kooperationen/gemeinsamer-ausschuss-dual-use-2/

Leopoldina
Nationale Akademie
der Wissenschaften

Freundeskreis EASAC Junge Akademie
English Kontakt Sitemap
Schriftgröße Impressum Datenschutz
Suchbegriff(e) SUCHEN

Über uns | Mitglieder | Themen | Publikationen | Politikberatung | International | Förderung | Veranstaltungen | Presse

Startseite _ Über uns _ Kooperationen _ Dual Use

GEMEINSAMER AUSSCHUSS DUAL USE

Wissenschaft zwischen Freiheit und Verantwortung

Aufgaben und Ziele des Gemeinsamen Ausschusses zum Umgang mit sicherheitsrelevanter Forschung

Illustration: Sisters of Design

Der Gemeinsame Ausschuss zum Umgang mit sicherheitsrelevanter Forschung (GA) ist ein seit 2015 von DFG und Leopoldina eingerichtetes Gremium, das das Bewusstsein für sicherheitsrelevante Aspekte der Forschung, den verantwortungsvollen Umgang mit sicherheitsrelevanter Forschung und die diesbezügliche Selbstregulierung der Wissenschaften nachhaltig stärken soll.

GESCHÄFTSSTELLE

Gemeinsamer Ausschuss zum Umgang mit sicherheitsrelevanter Forschung von DFG und Leopoldina

Geschäftsstelle c/o ABC Business Center (4. OG)
Friedrichstraße 79
10117 Berlin

Dr. Johannes Fritsch
Leiter der Geschäftsstelle

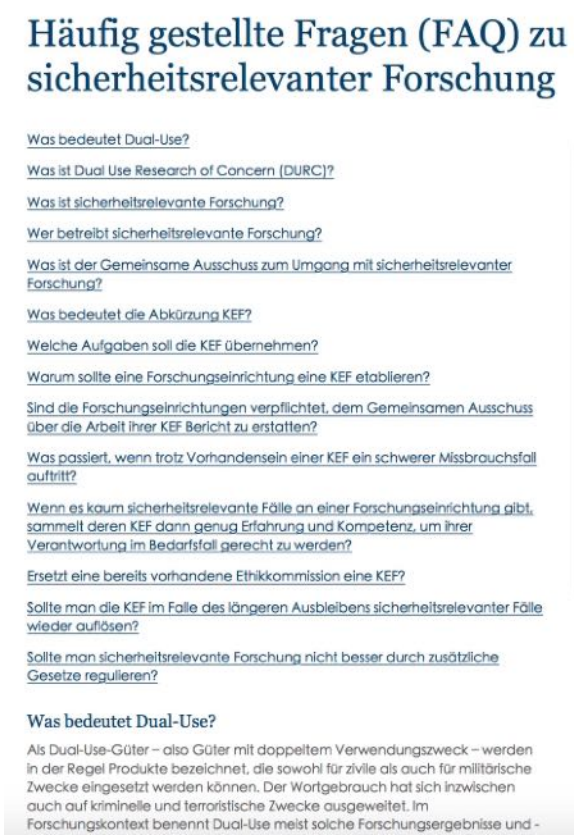
DFG Deutsche Forschungsgemeinschaft

Leopoldina
Nationale Akademie
der Wissenschaften

Wissenschaftsfreiheit und Wissenschaftsverantwortung

Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung

https://www.leopoldina.org/ueber-uns/kooperationen/gemeinsamer-ausschuss-dual-use-2/



Häufig gestellte Fragen (FAQ) zu sicherheitsrelevanter Forschung

Was bedeutet Dual-Use?

Was ist Dual Use Research of Concern (DURC)?

Was ist sicherheitsrelevante Forschung?

Wer betreibt sicherheitsrelevante Forschung?

Was ist der Gemeinsame Ausschuss zum Umgang mit sicherheitsrelevanter Forschung?

Was bedeutet die Abkürzung KEF?

Welche Aufgaben soll die KEF übernehmen?

Warum sollte eine Forschungseinrichtung eine KEF etablieren?

Sind die Forschungseinrichtungen verpflichtet, dem Gemeinsamen Ausschuss über die Arbeit ihrer KEF Bericht zu erstatten?

Was passiert, wenn trotz Vorhandensein einer KEF ein schwerer Missbrauchsfall auftritt?

Wenn es kaum sicherheitsrelevante Fälle an einer Forschungseinrichtung gibt, sammelt deren KEF dann genug Erfahrung und Kompetenz, um ihrer Verantwortung im Bedarfsfall gerecht zu werden?

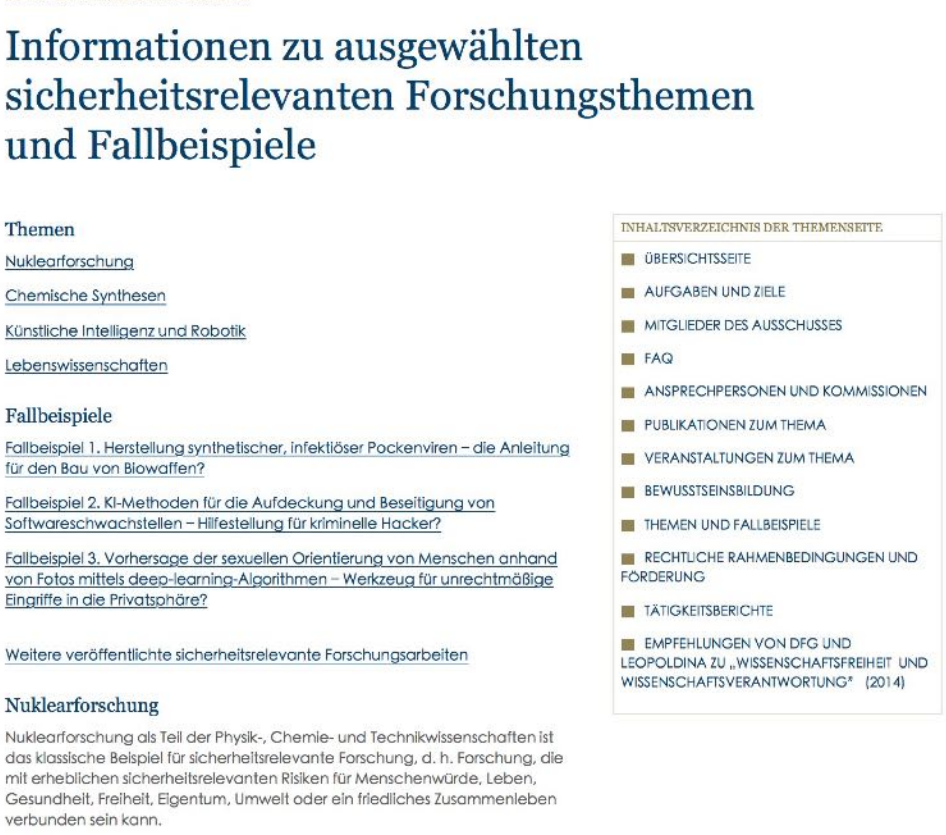
Ersetzt eine bereits vorhandene Ethikkommission eine KEF?

Sollte man die KEF im Falle des längeren Ausbleibens sicherheitsrelevanter Fälle wieder auflösen?

Sollte man sicherheitsrelevante Forschung nicht besser durch zusätzliche Gesetze regulieren?

Was bedeutet Dual-Use?

Als Dual-Use-Güter – also Güter mit doppeltem Verwendungszweck – werden in der Regel Produkte bezeichnet, die sowohl für zivile als auch für militärische Zwecke eingesetzt werden können. Der Wortgebrauch hat sich inzwischen auch auf kriminelle und terroristische Zwecke ausgeweitet. Im Forschungskontext benennt Dual-Use meist solche Forschungsergebnisse und -



Informationen zu ausgewählten sicherheitsrelevanten Forschungsthemen und Fallbeispiele

Themen

Nuklearforschung

Chemische Synthesen

Künstliche Intelligenz und Robotik

Lebenswissenschaften

Fallbeispiele

Fallbeispiel 1. Herstellung synthetischer, infektiöser Pockenviren – die Anleitung für den Bau von Biowaffen?

Fallbeispiel 2. KI-Methoden für die Aufdeckung und Beseitigung von Softwareschwachstellen – Hilfestellung für kriminelle Hacker?

Fallbeispiel 3. Vorhersage der sexuellen Orientierung von Menschen anhand von Fotos mittels deep-learning-Algorithmen – Werkzeug für unrechtmäßige Eingriffe in die Privatsphäre?

Weitere veröffentlichte sicherheitsrelevante Forschungsarbeiten

Nuklearforschung

Nuklearforschung als Teil der Physik-, Chemie- und Technikwissenschaften ist das klassische Beispiel für sicherheitsrelevante Forschung, d. h. Forschung, die mit erheblichen sicherheitsrelevanten Risiken für Menschenwürde, Leben, Gesundheit, Freiheit, Eigentum, Umwelt oder ein friedliches Zusammenleben verbunden sein kann.

INHALTSVERZEICHNIS DER THEMENSEITE

https://psyarxiv.com/hv28a/

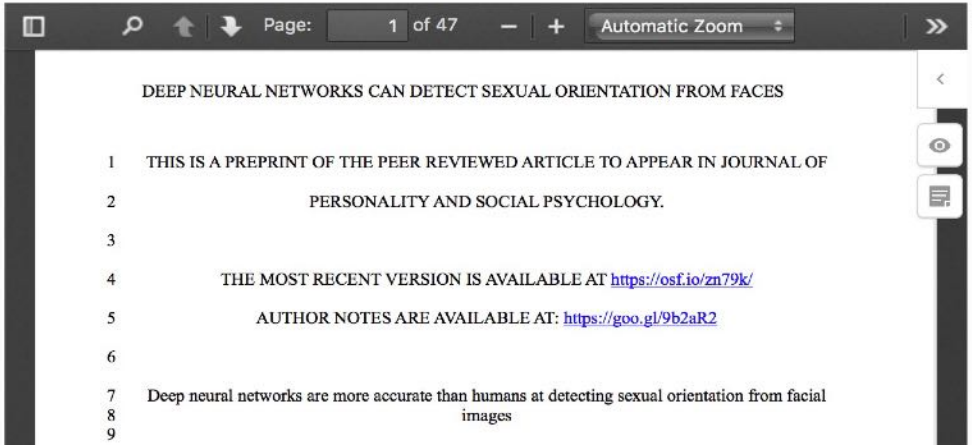
Deep neural networks are more accurate than humans at detecting sexual orientation from facial images.

AUTHORS
Yilun Wang, Michal Kosinski

CREATED ON
September 07, 2017

LAST EDITED
July 02, 2018

SUPPLEMENTAL MATERIALS
osf.io/zn79k/


Page: 1 of 47 Automatic Zoom

DEEP NEURAL NETWORKS CAN DETECT SEXUAL ORIENTATION FROM FACES

1 THIS IS A PREPRINT OF THE PEER REVIEWED ARTICLE TO APPEAR IN JOURNAL OF
2 PERSONALITY AND SOCIAL PSYCHOLOGY.
3
4 THE MOST RECENT VERSION IS AVAILABLE AT https://osf.io/zn79k/
5 AUTHOR NOTES ARE AVAILABLE AT: https://goo.gl/9b2aR2
6
7 Deep neural networks are more accurate than humans at detecting sexual orientation from facial
8 images
9

Download preprint

Downloads: 35995

Abstract

We show that faces contain much more information about sexual orientation than can be perceived and interpreted by the human brain. We used deep neural networks to extract features from 35,326 facial images. These features were entered into a logistic regression aimed at classifying sexual orientation. Given a single facial image, a classifier ...

See more