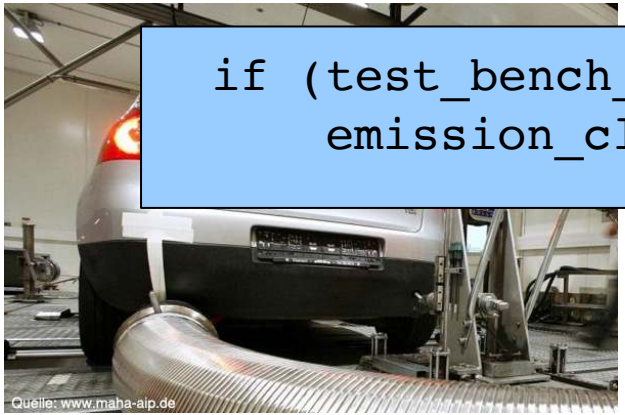
Zur Verantwortung von Informatiker*innen

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

Zur Verantwortung von Informatiker*innen

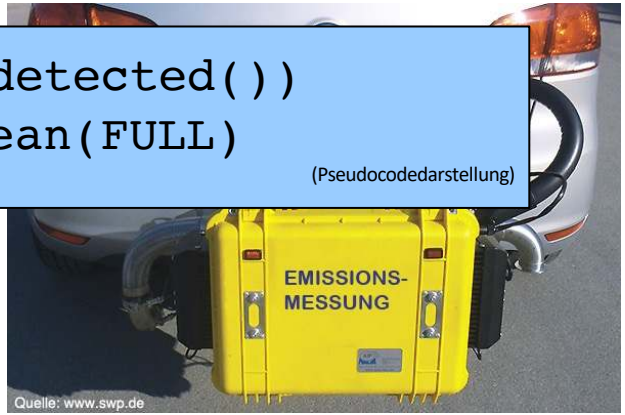
- Wo die Kategorien »Gut und Böse« weiterhelfen
  - Ethische Aspekte
- Wir bezahlen mit unseren Daten
  - Spannungsfeld von Online-Marketing und Datenschutz
- Ich habe doch nichts zu verbergen
  - Innere Sicherheit und Überwachung
- Drohnenkrieg
  - Militärischer Einsatz von Informationstechnologie

Abgasmessungen auf dem Prüfstand und mobil




```
if (test_bench_detected())
    emission_clean(FULL)
```

(Pseudocodedarstellung)

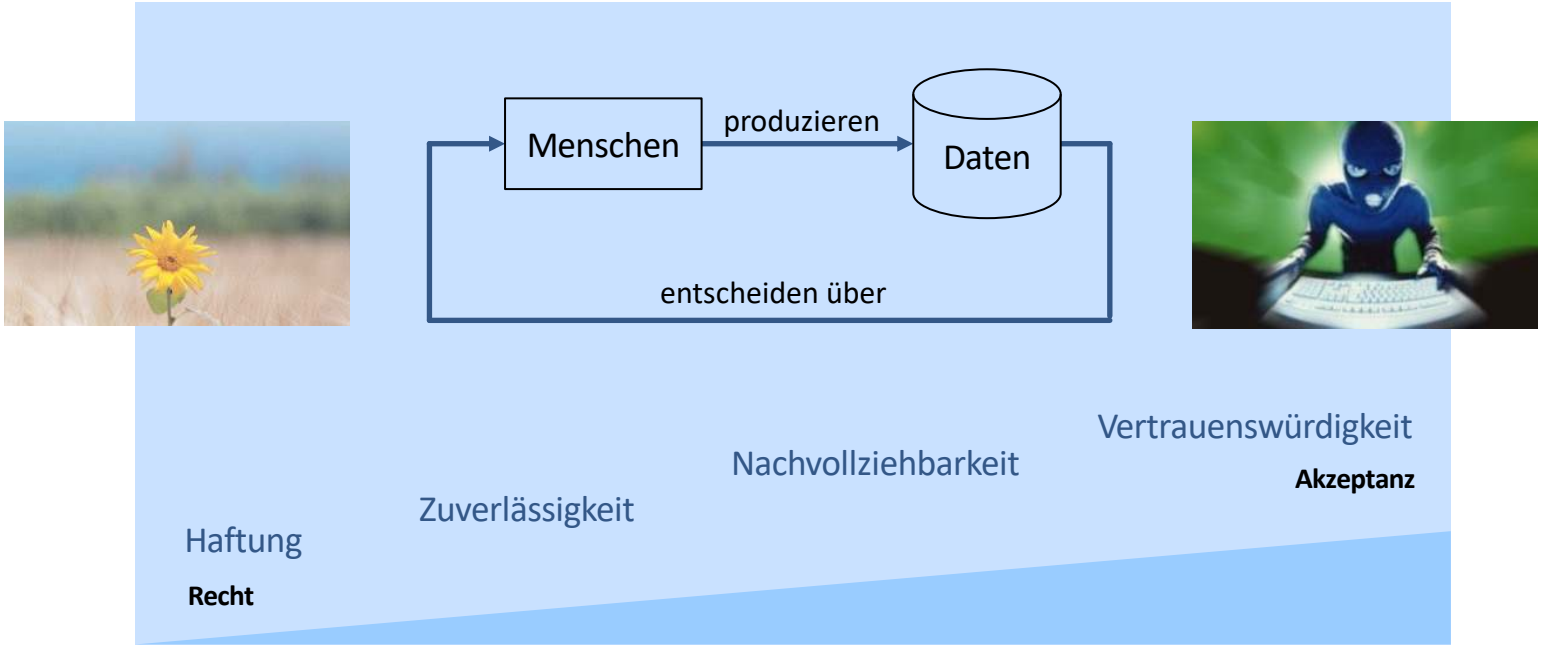


- Adaptive Motorsteuerung erkennt anhand von Lenkradbewegungen, Umgebungsluftdruck, Raddrehzahlen und Motorlaufzeit die Messbedingungen

	Abgasreinigung	Kraftstoffverbrauch
Prüfstand	verbessert	hoch
Straße	reduziert	verringert

Algorithmische Entscheidungssysteme als Blackbox

- Risikoawareness: Spannungsfeld zwischen Haftung und Vertrauenswürdigkeit



Autonome Fahrzeuge

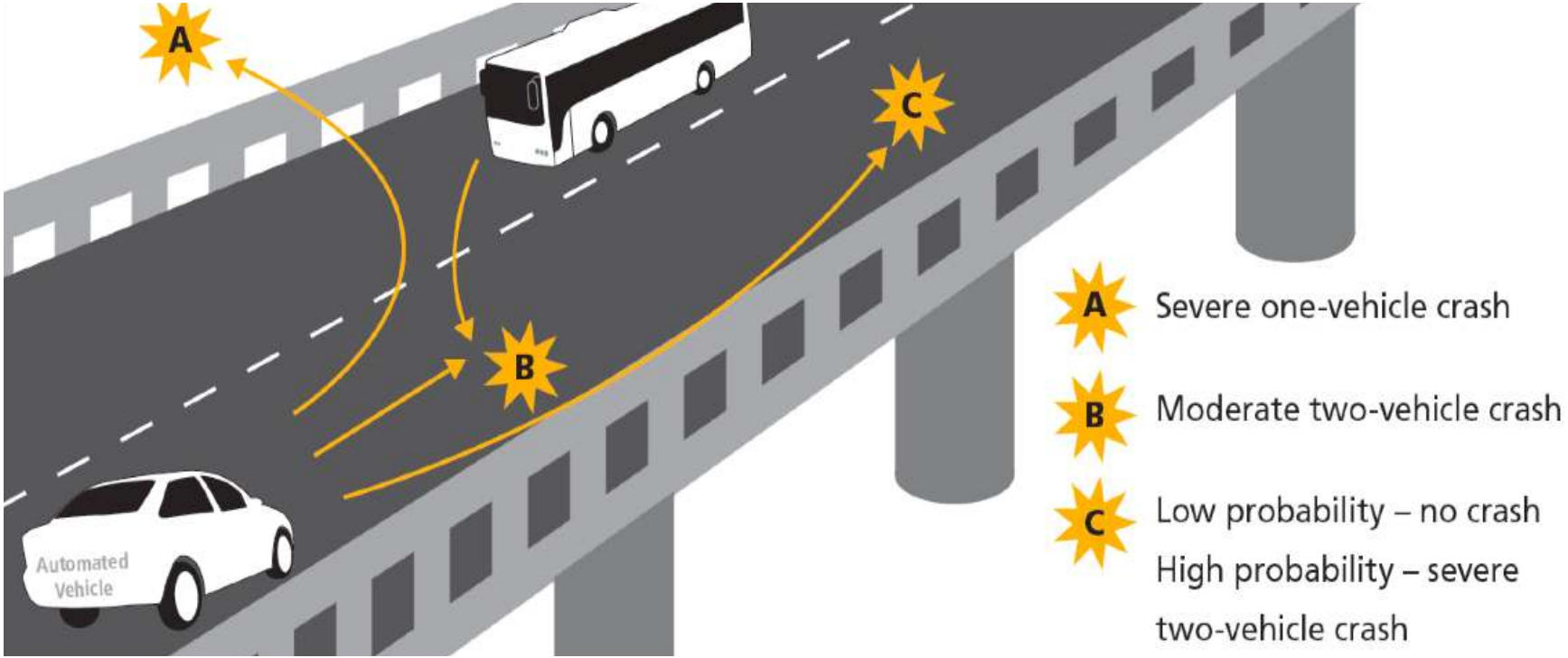
- Haftungsregeln bei Technikversagen
  - juristische Fragen
  - technische Fragen
  - ethische Fragen

    - ohne Helm: höhere Chance, beim Aufprall zu sterben
    - mit Helm: höhere Chance zu überleben

http://www.theguardian.com/environment/green-living-blog/2010/apr/07/david-cameron-cycles-without-helmet

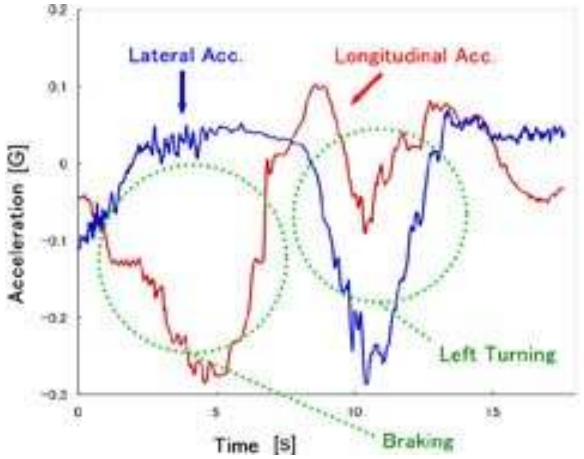
Kontinuierliches Sammeln und Übermitteln von Daten und (ggf. anonymisierte) zentrale Auswertung zur Systemverbesserung, Beweissicherung etc.

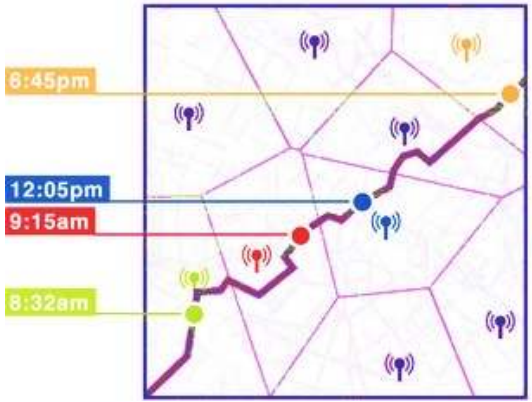
http://people.virginia.edu/~njg2q/ethics.pdf



Kontinuierliches Sammeln und Übermitteln von Daten

http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html
http://www.npa.go.jp/nrips/en/traffic/section3.html





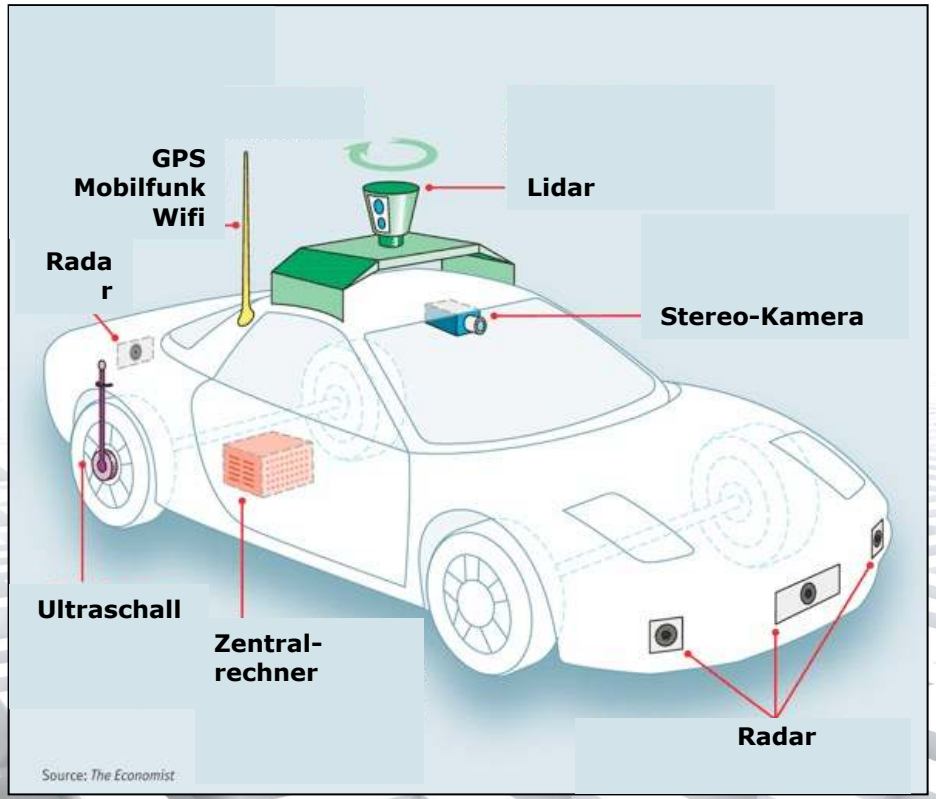
Klärung der Haftung bei Unfällen:

- Rekonstruktion des Fahrverhaltens anhand aufgezeichneter Daten
- Vorteile für den Hersteller, der festlegt, welche Daten gespeichert werden

Gefahr für die Privatsphäre:

- Identifizierung des Fahrers auch anhand anonymisierter Bewegungsdaten möglich; u.U. reichen bereits 4 Ortsangaben aus
- Verräterische Daten wecken Begehrlichkeiten

Sensorik in (autonomen) vernetzten Fahrzeugen

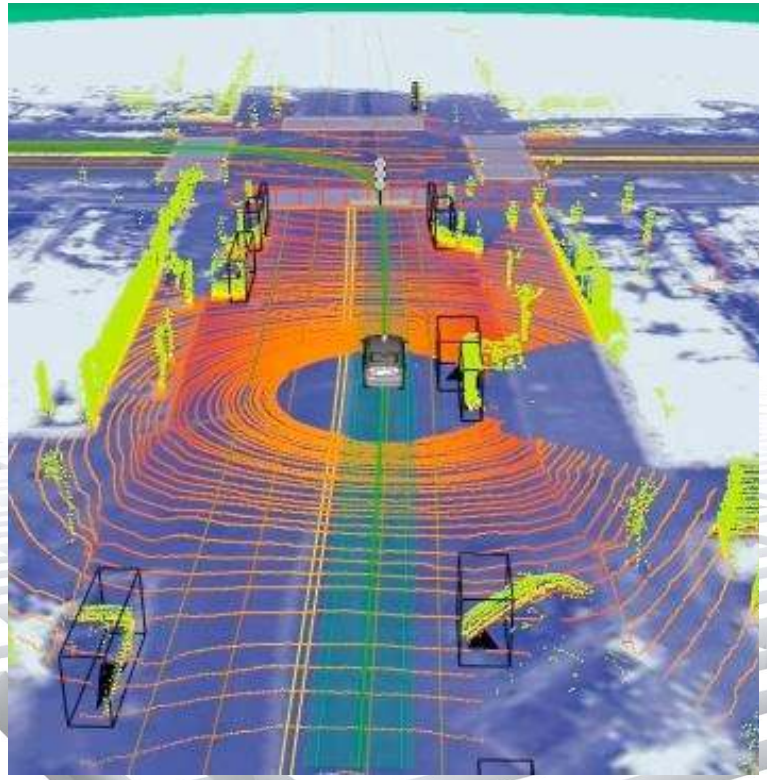


nach: http://econ.st/ZZBLzi

Herausforderungen:

- Wahrnehmung
- Planung
- Entscheidung
- Interaktion

Sensorik in (autonomen) vernetzten Fahrzeugen



http://asset1.cbsistatic.com/cnwk.1d/i/tim2/2013/08/30/Goog-self-driving-1_610x363.jpg

Herausforderungen:

- Wahrnehmung
- Planung
- Entscheidung
- Interaktion

Verkehrszeichenerkennung mittels maschineller Lernverfahren

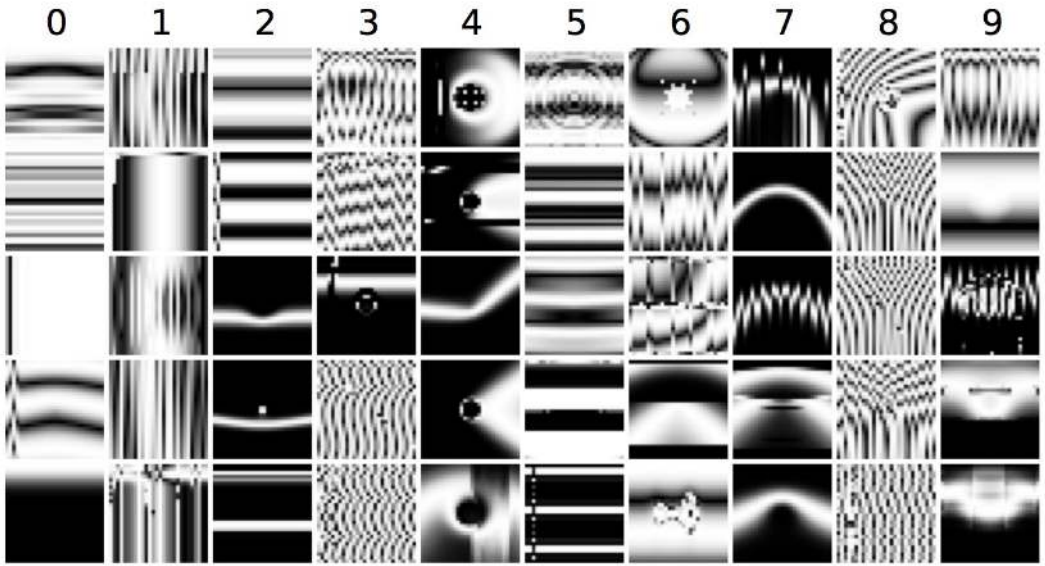
REALITÄT	ERKENNUNG: Gefahr	ERKENNUNG: »normal«
Gefahr	richtig positiv	falsch negativ
»normal«	falsch positiv	richtig negativ

J. Stallkamp, M. Schlipsing, J. Salmen, C. Igel, Man vs. computer: Benchmarking machine learning algorithms for traffic sign recognition, Neural Networks, Volume 32, August 2012, Pages 323-332, ISSN 0893-6080

…klappt leider nicht immer

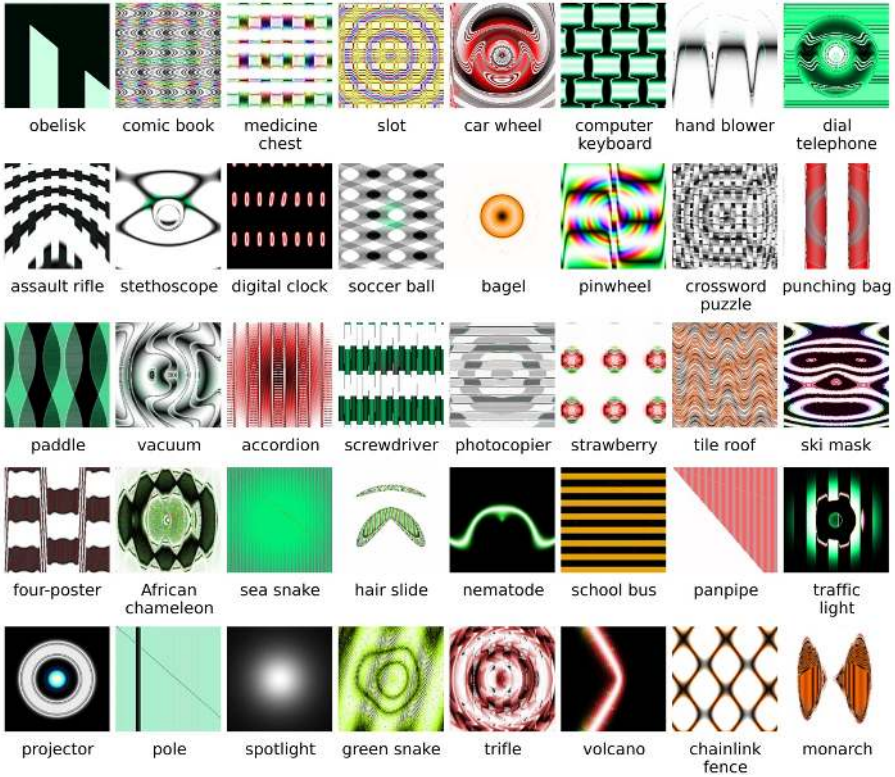
Erkannte Ziffer

Eingabedaten, die fälschlicherweise als Ziffer erkannt werden



Nguyen A, Yosinski J, Clune J. Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images. In CVPR ’15, IEEE, 2015.

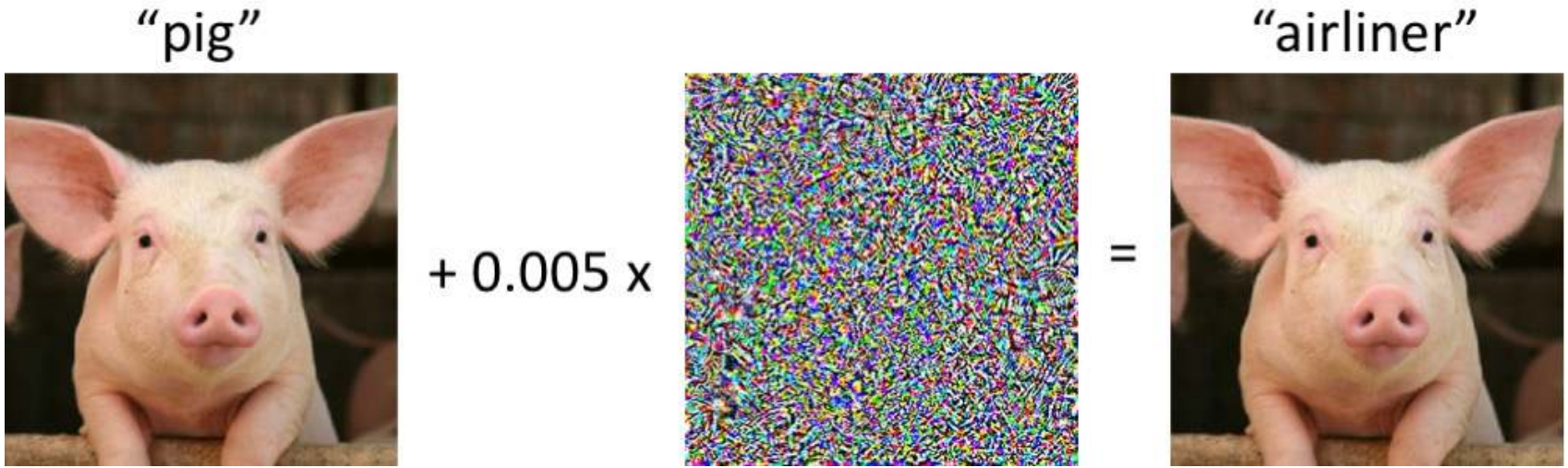
Gezielte Manipulationen eines autonomen Fahrzeugs möglich



Nguyen A, Yosinski J, Clune J. Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images. In CVPR ’15, IEEE, 2015.

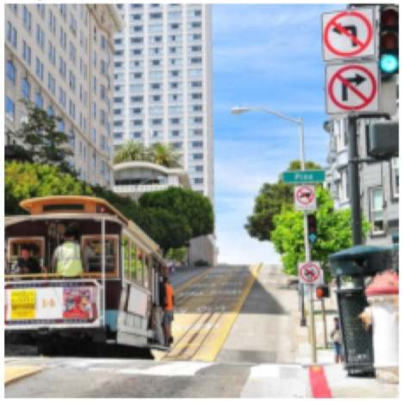
Gezielte Manipulationen

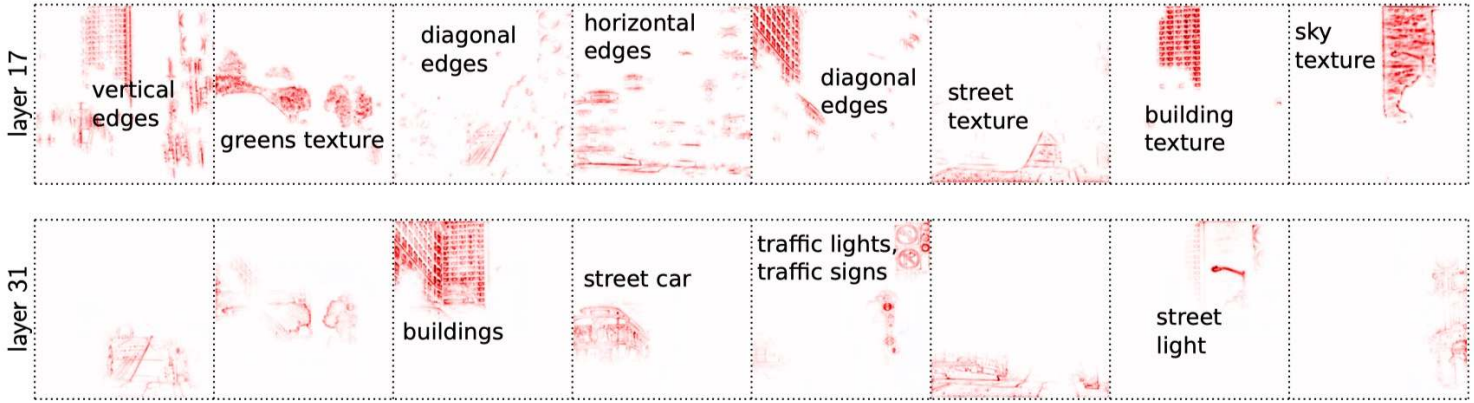
- Adversarial learning



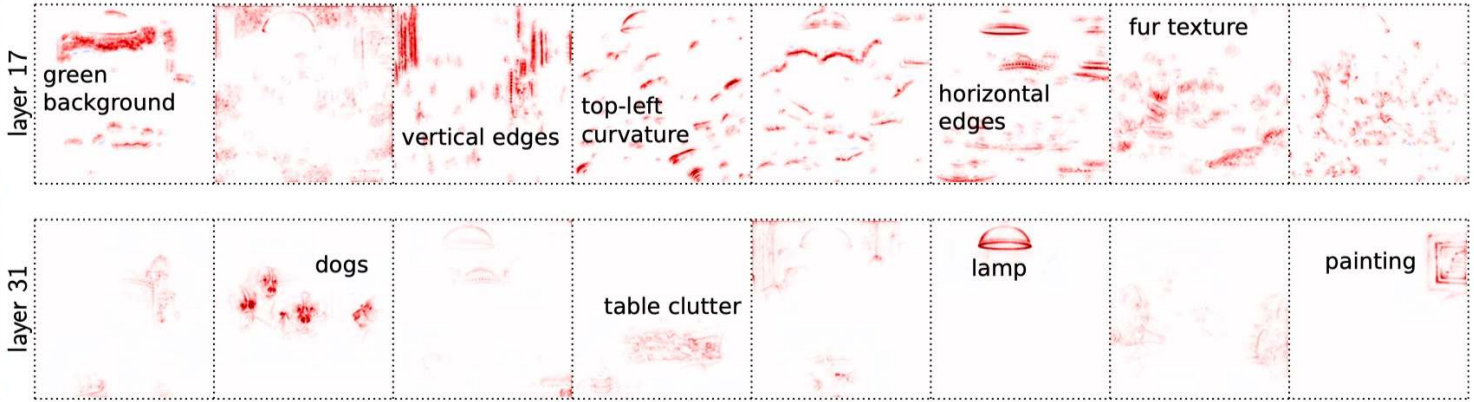
https://www.designnews.com/electronics-test/yes-ai-can-be-tricked-and-its-serious-problem/161652909959780

City and streetcar

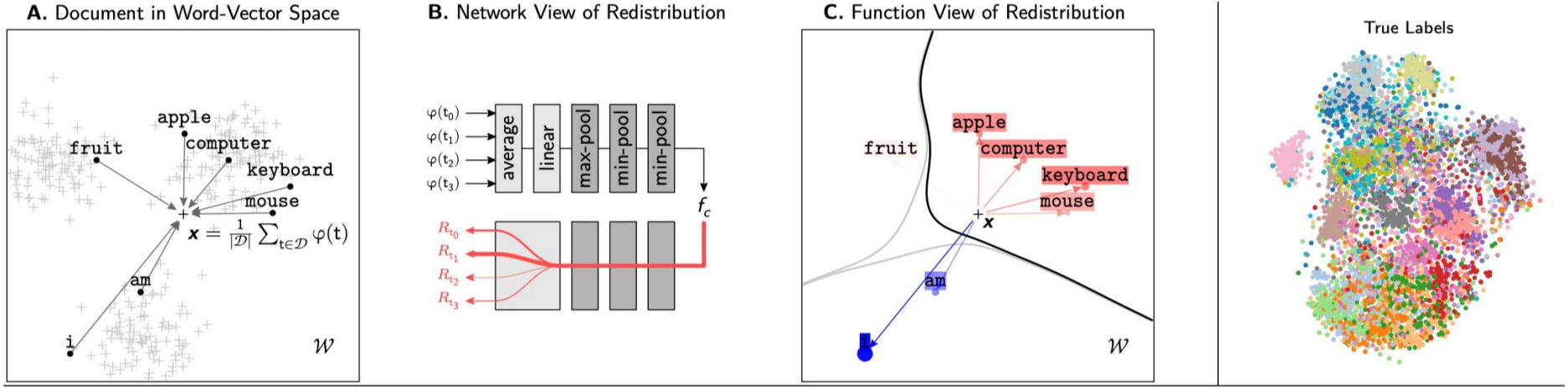




"Poker Game" (Coolidge, 1894)



J. Kauffmann, M. Esders, G. Montavon, W. Samek, K. Müller, From Clustering to Cluster Explanations via Neural Networks CoRR, 2019, https://arxiv.org/abs/1906.07633



Cluster Assignments

D. talk.politics.guns

Even if it were a capital offense, the warrant was not even an arrest warrant, but a search warrant. In other words, there was no evidence of illegal arms, just enough of a suggestion to get a judge to sign a license to search for illegal evidence.

E. sci.crypt

You can find the salient difference in any number of 5th amendment related Supreme Court opinions. The Court limits 5th amendment protections to what they call "testimonial" evidence, as opposed to physical evidence.

The whole question would hinge on whether a crypto key would be considered "testimonial" evidence. I suppose arguments could be made either way, though obviously I would hope it would be considered testimonial.

F. rec.motorcycles

I'm not sure on the older bikes, but the Yamaha Virago 535 has spec'd seat height of 27.6 in. and the Honda Shadow 27.2 in.

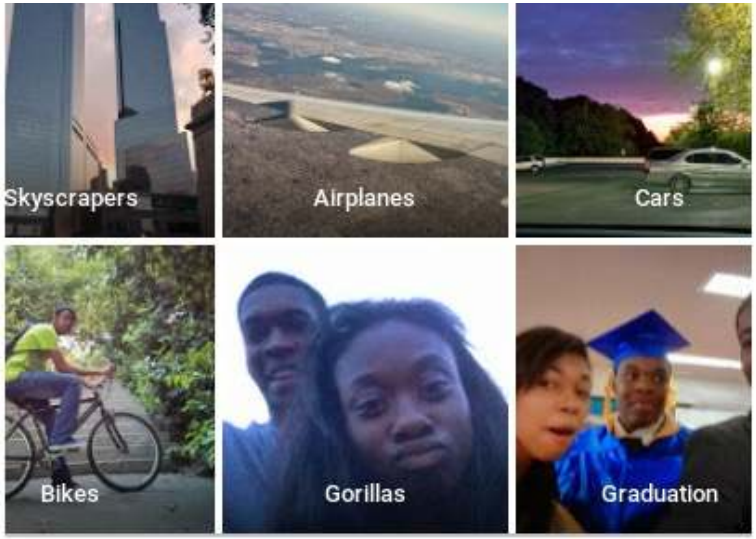
G. misc.forsale

For Sale: A Thule Car rack with 2 bike holder accessories.
Comes with Nissan Pathfinder brackets but you can buy the appropriate ones for your car cheap.
Looking for $100.00 for everything. I live in the Bethesda area.
Thanks for your interest.

J. Kauffmann, M. Esders, G. Montavon, W. Samek, K. Müller, From Clustering to Cluster Explanations via Neural Networks CoRR, 2019, https://arxiv.org/abs/1906.07633

Algorithmen sind nicht neutral, sondern enthalten immer Wertungen

- Machine Learning:
  - Auswahl des Trainingssets erzeugt stereotype Muster
  - verfestigt solche Muster (»algorithmische Normalisierung«)



https://www.cnet.com/news/google-apologizes-for-algorithm-mistakenly-calling-black-people-gorillas/

Ethische Aspekte

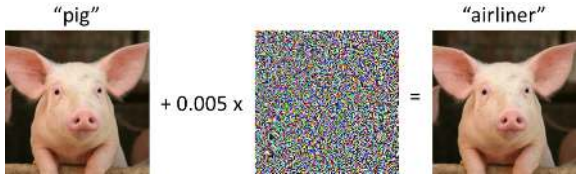
- Verantwortungsethik
  - Entscheidung zwischen Handlungsalternativen: Was sind die tatsächlichen Ergebnisse und deren Verantwortbarkeit?
- Gesinnungsethik
  - Beurteilung von Handlungstypen: Übereinstimmung von Motiv und Absicht mit gegebenen ethischen Werten

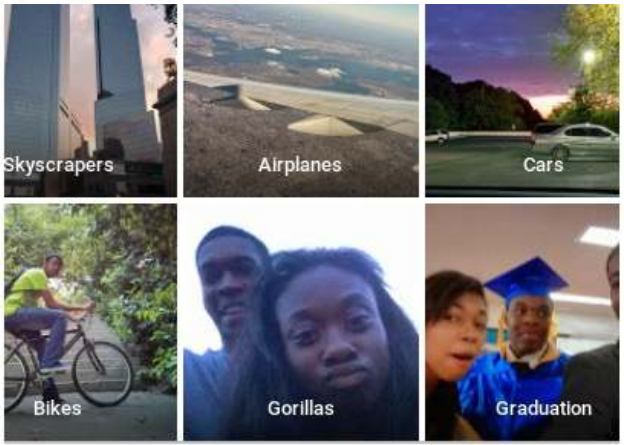
«Wir müssen uns klarmachen, daß alles ethisch orientierte Handeln unter zwei voneinander grundverschiedenen, unaustragbar gegensätzlichen Maximen stehen kann: es kann ‚gesinnungsethisch' oder ‚verantwortungsethisch' orientiert sein. Nicht daß Gesinnungsethik mit Verantwortungslosigkeit und Verantwortungsethik mit Gesinnungslosigkeit identisch wäre. Davon ist natürlich keine Rede. Aber es ist ein abgrundtiefer Gegensatz, ob man unter der gesinnungsethischen Maxime handelt - religiös geredet: ‚Der Christ tut recht und stellt den Erfolg Gott anheim' - oder unter der verantwortungsethischen: daß man für die (voraussehbaren) Folgen seines Handelns aufzukommen hat.»

Max Weber, 1919, https://de.wikipedia.org/wiki/Verantwortungsethik

Ethische Dimensionen

- Dreiteilung nach Simon, 2016:
  - Ethik des Berufs
  - Ethik des Designs
  - Ethik der Nutzung





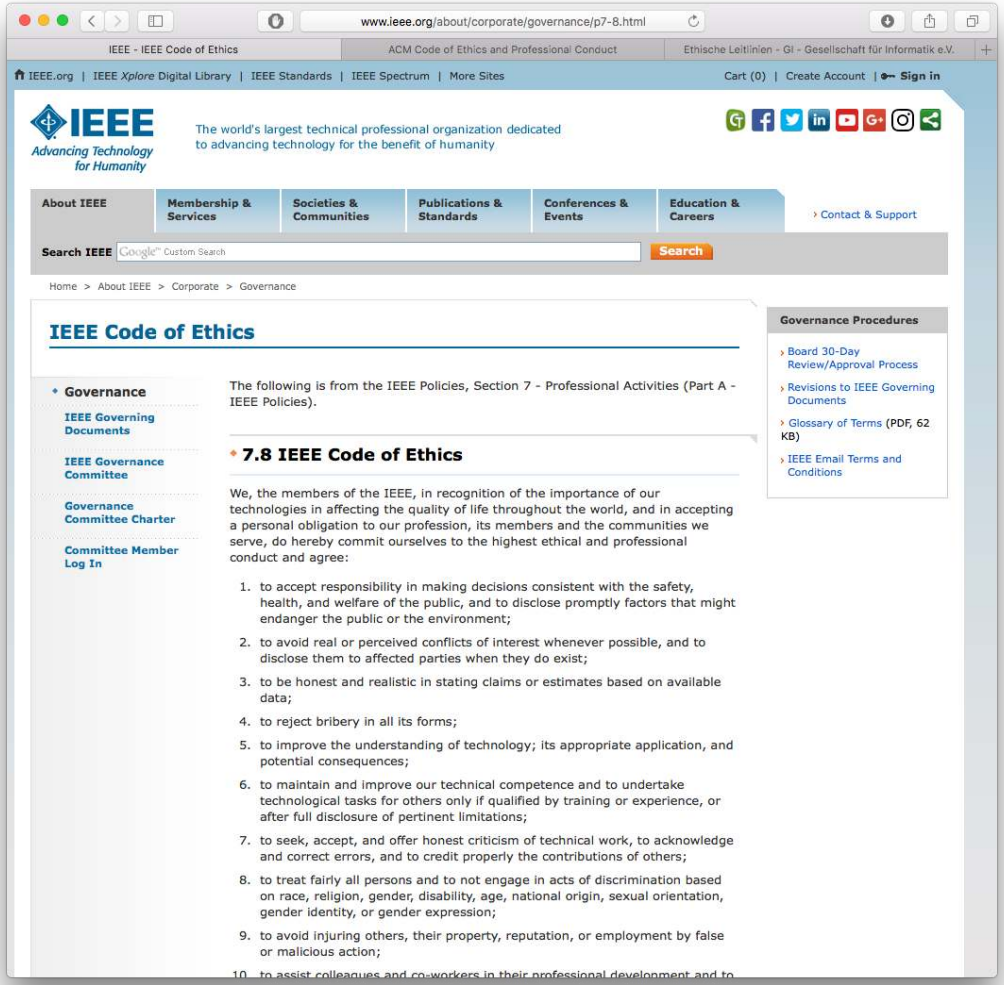
Association for Computing Machinery

IEEE Advancing Technology for Humanity

Ethische Leitlinien der Gesellschaft für Informatik

ACM Code of Ethics and Professional Conduct

IEEE Code of Ethics


www.ieee.org/about/corporate/governance/p7-8.html
IEEE - IEEE Code of Ethics
ACM Code of Ethics and Professional Conduct
Ethische Leitlinien - GI - Gesellschaft für Informatik e.V.
IEEE.org | IEEE Xplore Digital Library | IEEE Standards | IEEE Spectrum | More Sites
Cart (0) | Create Account | Sign in
IEEE
Advancing Technology for Humanity
The world's largest technical professional organization dedicated to advancing technology for the benefit of humanity
About IEEE
Membership & Services
Societies & Communities
Publications & Standards
Conferences & Events
Education & Careers
Contact & Support
Search IEEE
Search
Home > About IEEE > Corporate > Governance
IEEE Code of Ethics
Governance
IEEE Governing Documents
IEEE Governance Committee
Governance Committee Charter
Committee Member Log In
The following is from the IEEE Policies, Section 7 - Professional Activities (Part A - IEEE Policies).
7.8 IEEE Code of Ethics
We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:
1. to accept responsibility in making decisions consistent with the safety, health, and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;
2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
3. to be honest and realistic in stating claims or estimates based on available data;
4. to reject bribery in all its forms;
5. to improve the understanding of technology; its appropriate application, and potential consequences;
6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;
7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
8. to treat fairly all persons and to not engage in acts of discrimination based on race, religion, gender, disability, age, national origin, sexual orientation, gender identity, or gender expression;
9. to avoid injuring others, their property, reputation, or employment by false or malicious action;
10. to assist colleagues and co-workers in their professional development and to
Governance Procedures
Board 30-Day Review/Approval Process
Revisions to IEEE Governing Documents
Glossary of Terms (PDF, 62 KB)
IEEE Email Terms and Conditions

www.acm.org/about-acm/acm-code-of-ethics-and-

IEEE - IEEE Code of Ethics | ACM Code of Ethics and Professional Conduct | Ethische Leitlinien - GI - Gesellschaft für Informatik e.V.

Association for Computing Machinery

ACM Code of Ethics and Professional Conduct

Adopted by ACM Council 10/16/92.

Preamble

Contents & Guidelines

Preamble

Commitment to ethical professional conduct is expected of every member (voting members, associate members, and student members) of the Association for Computing Machinery (ACM).

This Code, consisting of 24 imperatives formulated as statements of personal responsibility, identifies the elements of such a commitment. It contains many, but not all, issues professionals are likely to face. Section 1 outlines fundamental ethical considerations, while Section 2 addresses additional, more specific considerations of professional conduct. Statements in Section 3 pertain more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer capacity such as with organizations like ACM. Principles involving compliance with this Code are given in Section 4.

The Code shall be supplemented by a set of Guidelines, which provide explanation to assist members in dealing with the various issues contained in the Code. It is expected that the Guidelines will be changed more frequently than the Code.

The Code and its supplemented Guidelines are intended to serve as a basis for ethical decision making in the conduct of professional work. Secondarily, they may serve as a basis for judging the merit of a formal complaint pertaining to violation of professional ethical standards.

It should be noted that although computing is not mentioned in the imperatives of Section 1, the Code is concerned with how these fundamental imperatives apply to one's conduct as a computing professional. These imperatives are expressed in a general form to emphasize that ethical principles which apply to computer ethics are derived from more general ethical principles.

It is understood that some words and phrases in a code of ethics are subject to varying interpretations, and that any ethical principle may conflict with other ethical principles in

Die ethischen Leitlinien der Gesellschaft für Informatik

Präambel

Art. 1 Fachkompetenz

Art. 2 Sachkompetenz und kommunikative Kompetenz

Art. 3 Juristische Kompetenz

Art. 4 Urteilsfähigkeit

Art. 5 Arbeitsbedingungen

Art. 6 Organisationsstrukturen

Art. 7 Lehre und Lernen

Art. 8 Forschung

Art. 9 Zivilcourage

Art. 10 Soziale Verantwortung

https://gi.de/ueber-uns/organisation/unsere-ethischen-leitlinien/

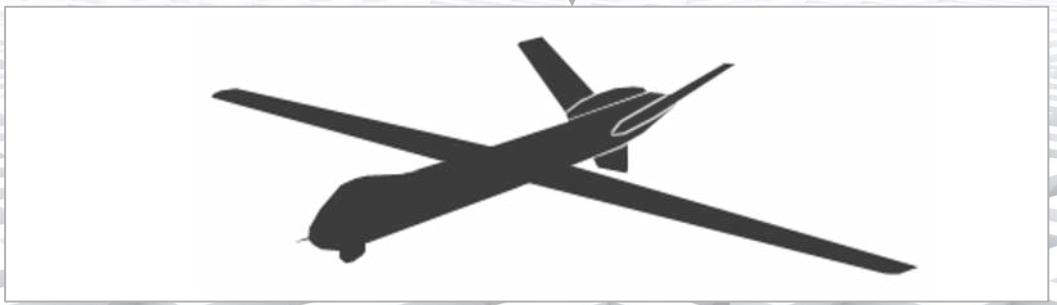
Ethische Dimensionen

- Dreiteilung nach Simon, 2016:
  - Ethik des Berufs
  - Ethik des Designs
  - Ethik der Nutzung

```
if (test_bench_detected())
    emission_clean(FULL)
else
    <ignore_laws>
```

Ethische Dimensionen

- Dreiteilung nach Simon, 2016:
  - Ethik des Berufs
  - Ethik des Designs
  - Ethik der Nutzung



Zur Verantwortung von Informatiker*innen

- Wo die Kategorien »Gut und Böse« weiterhelfen
  - Ethische Aspekte
- Wir bezahlen mit unseren Daten
  - Spannungsfeld von Online-Marketing und Datenschutz
- Ich habe doch nichts zu verbergen
  - Innere Sicherheit und Überwachung
- Drohnenkrieg
  - Militärischer Einsatz von Informationstechnologie

Warum sind Facebook, Twitter, Instagram, Google etc. kostenlos?

zeit.de

Marketing

Wie Werbung wirkt

Seite 2/2 Sieben Dollar Umsatz für einen Dollar Werbung

INHALT Auf einer Seite lesen

Der Einzelhändler stellte ihnen sämtliche Informationen zur Verfügung, die er über seine Kunden gesammelt hatte. Die Forscher hatten zudem Zugriff auf die Nutzerdaten von Yahoo und glichen beide Datenbanken ab. 1,6 Millionen Personen konnten sie eindeutig identifizieren – sie hatten sowohl einen Account bei Yahoo als auch eine Kundenkarte des Einzelhändlers.

https://www.zeit.de/wirtschaft/2011-01/werbung-internet/seite-2

heise.de

heise online

Verband: Umsatz mit Online-Werbung knackt 4-Milliarden-Marke

10.03.2021 18:52 Uhr

Torsten Kleinz

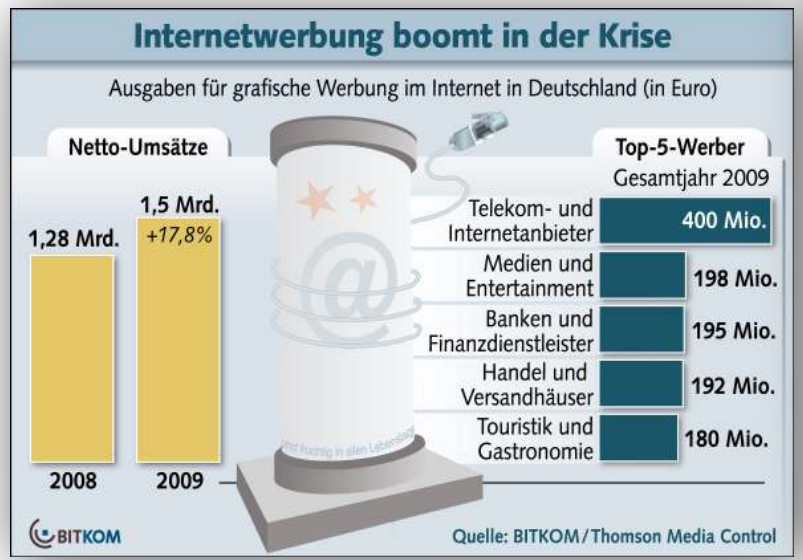
Online wie offline: Werbung allerorten.
(Bild: ieronymos / Shutterstock.com)

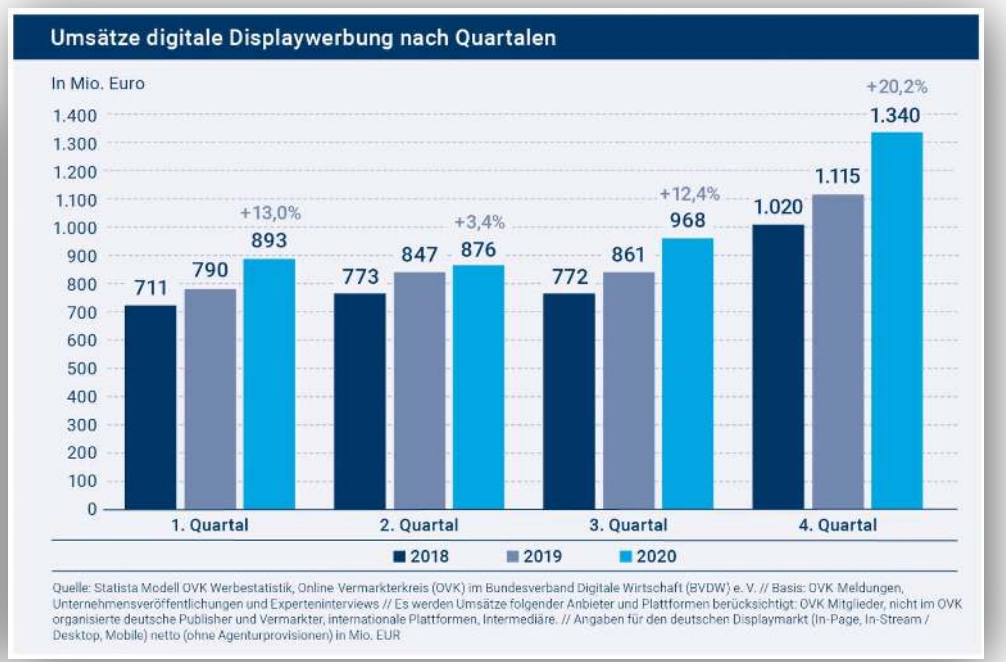
Die deutschen Online-Vermarkter können stark gestiegene Nutzungszahlen inzwischen wieder in Werbeerlöse ummünzen. Statt Mallorca-Reisen werden Webcams beworben.

Die Krise der Online-Werbebranche war nur sehr kurz: Nach eher kurzfristigen Wachstumsrückgängen im vergangenen Jahr rechnet der Online-Vermarkterkreis (OVK) im Bundesverband Digitale Wirtschaft (BVDW) mit einem deutlichen Umsatzplus für digitale Display-Werbung von 12,9 Prozent auf 4,08 Milliarden für das Jahr 2020. Damit übersteigt das Wachstum sogar das der Vorjahre.

https://www.heise.de/-5077251

Mit Werbung wird Geld verdient!





Wirtschaftskrise im Jahr 2009

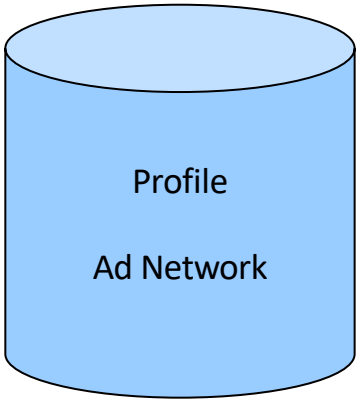
aus: https://www.heise.de/-5077251

Third-Party Cookies

GET http://adnet.example.net/banner1.gif
Cookie: guid=8867563
Referer: http://www.bookshop.example

GET http://adnet.example.net/banner2.gif
Cookie: guid=8867563
Referer: http://www.healthinfo.example

GET http://adnet.example.net/banner3.gif
Cookie: guid=8867563
Referer: http://www.lifeinsurance.example



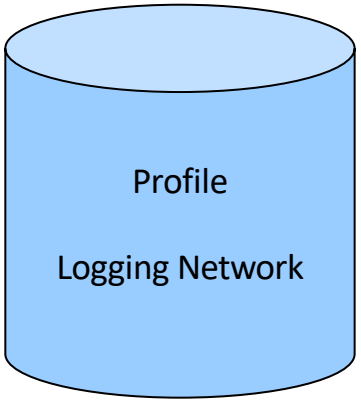
Protection: Delete cookies

Mobile logging networks

App 1: SN-Device, start, stop, …
82031M6UV2F, 2012-12-19T16:39:57, 2012-12-19T16:45:33

App 2: SN-Device, start, stop, address book, …
82031M6UV2F, 2012-12-20T12:19:11, 2012-12-20T12:25:01, data

App 3: SN-Device, start, stop, location info, …
82031M6UV2F, 2012-12-20T12:21:23, 2012-12-20T12:21:55, data



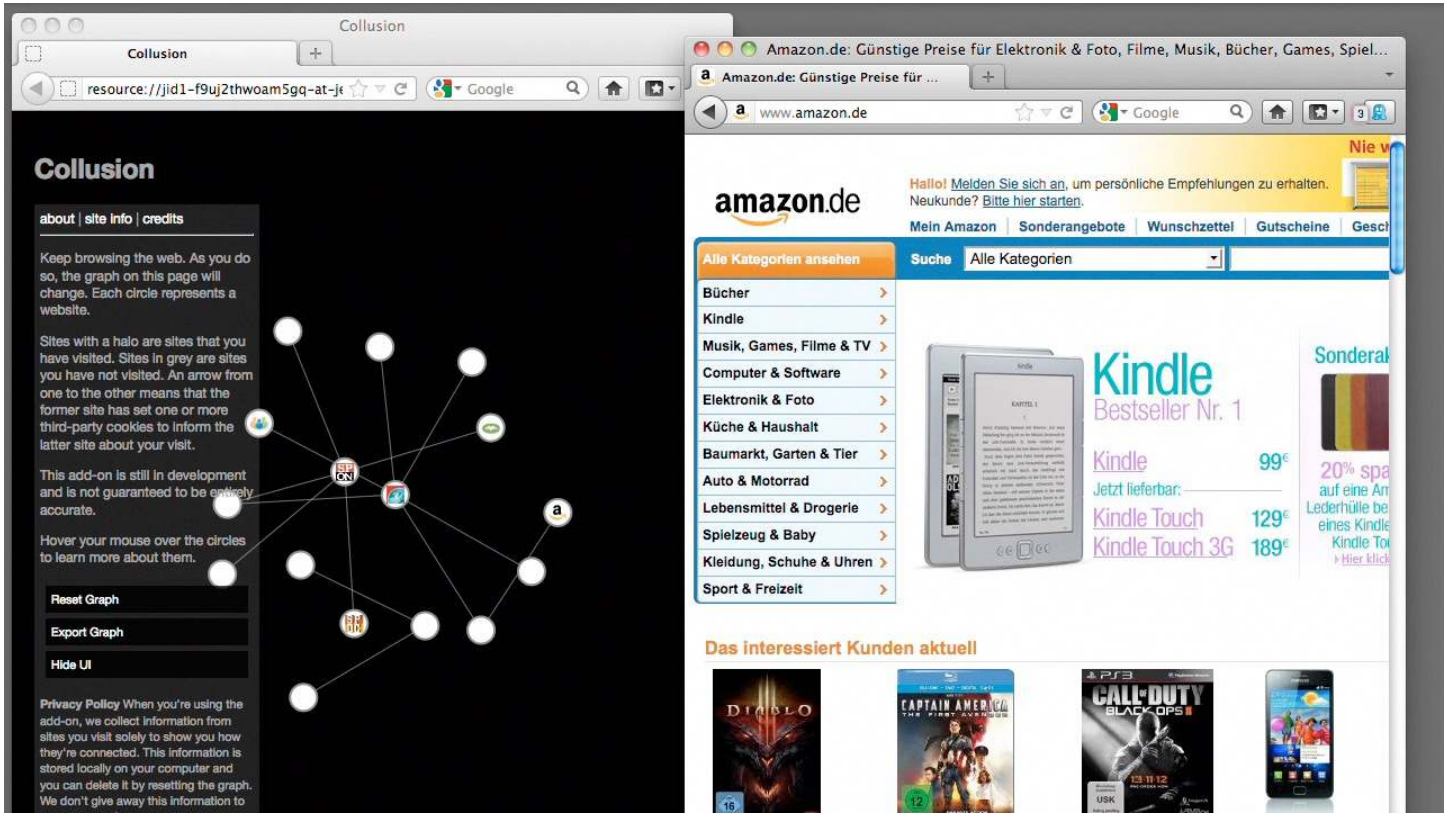
How to protect?

Ghostery – Visualisation of tracking

Lightbeam (Collusion) – Visualisation of tracking

Left: Dependency graph

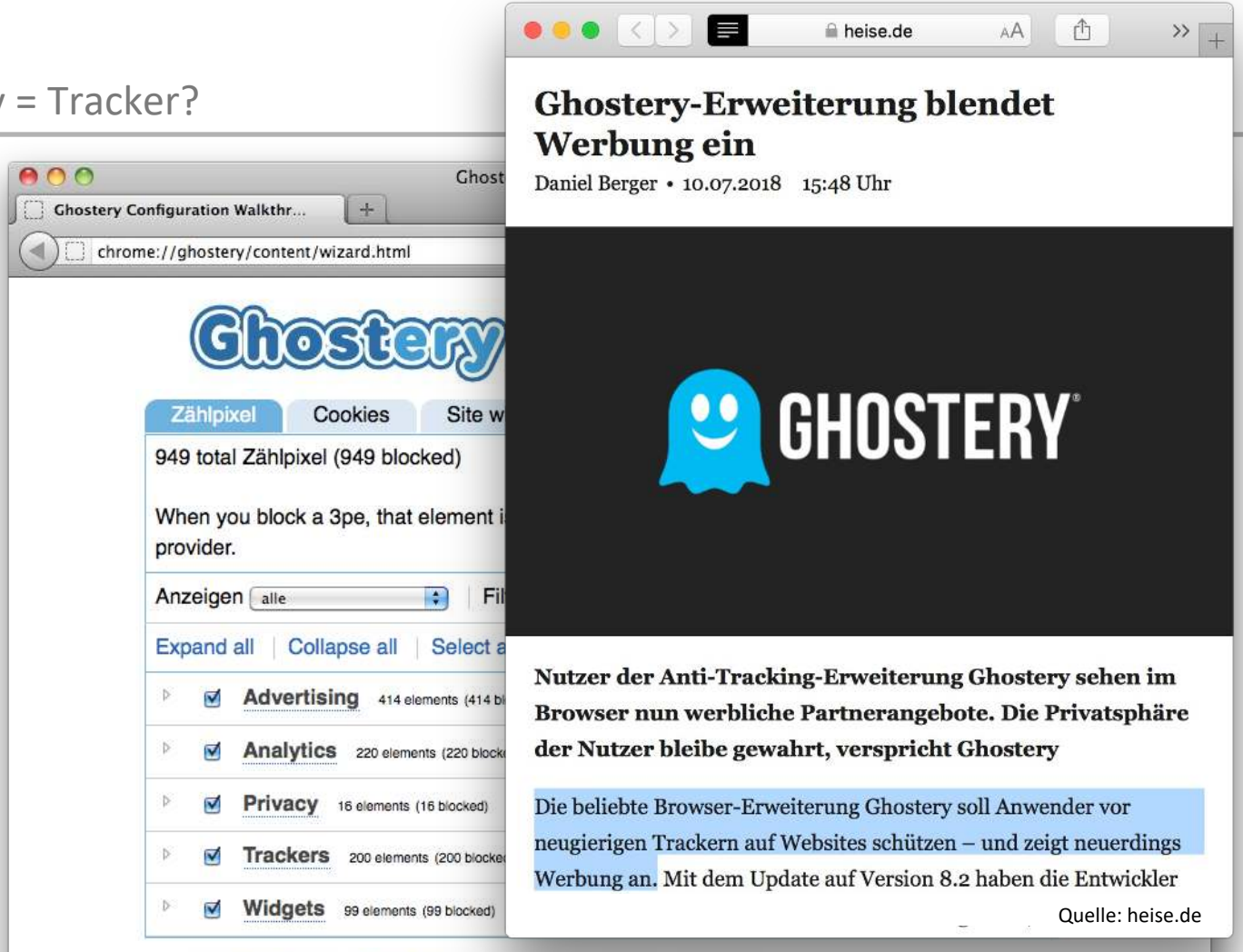
Right: Browser window



Ghostery = Tracker?

https://mashable.com/2013/06/17/ad-blocker-helps-ad-industry/

Ghostery = Tracker?



Quelle: heise.de

- Tracking with a »Browser Fingerprint« (without cookies)

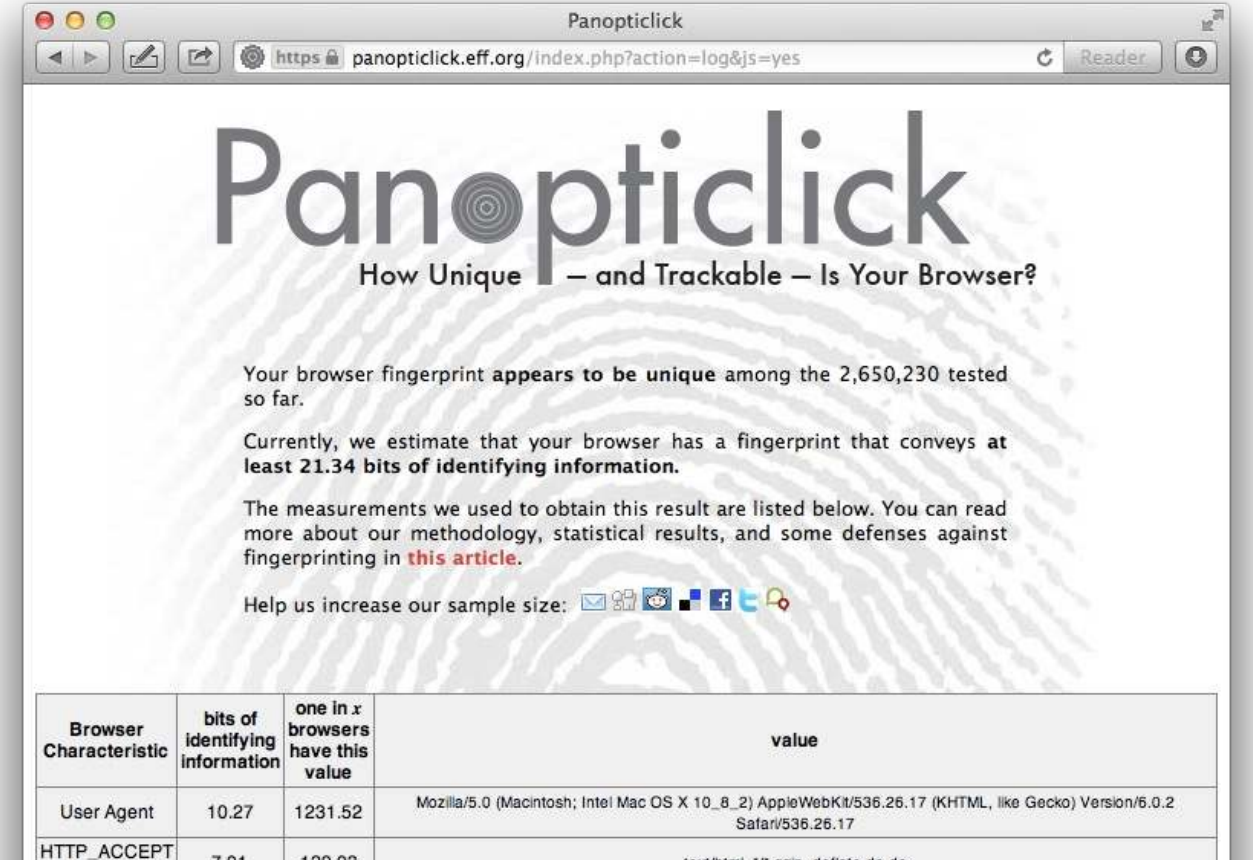
- Tracking data and entropy:
  - User Agent: ca. 10 Bit
  - HTTP_ACCEPT Headers: ca. 7 Bit
  - Browser Plugin Details: ca. 20 Bit
  - Time Zone: ca. 2,5 Bit
  - Screen Size and Color Depth: ca. 5 Bit
  - System Fonts: >=21 Bit
  - Are Cookies Enabled? ca. 0,4 Bit
  - Limited supercookie test? ca. 1 Bit

- https://panopticlick.eff.org

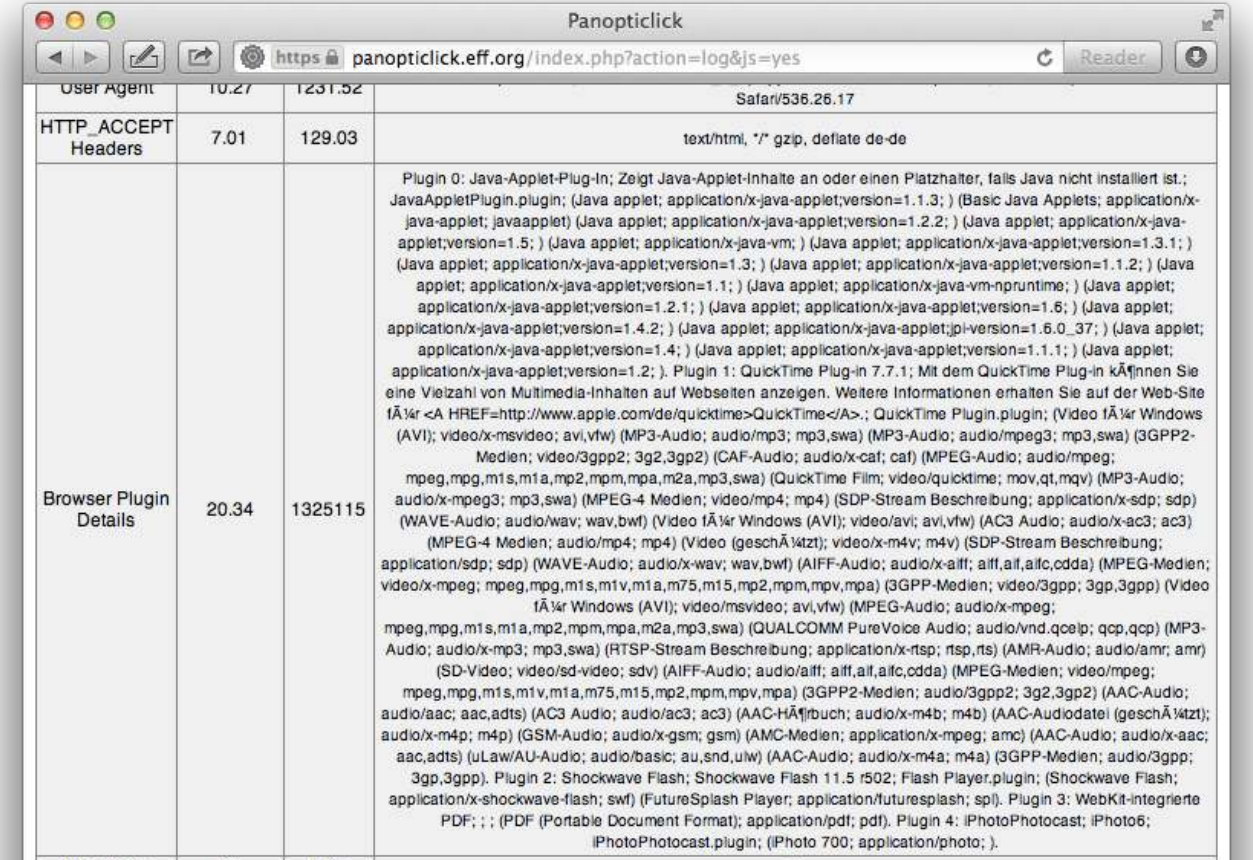
Panopticlick

Eckersley, 2010

Eckersley, 2010



Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
User Agent	10.27	1231.52	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_2) AppleWebKit/536.26.17 (KHTML, like Gecko) Version/6.0.2 Safari/536.26.17
HTTP_ACCEPT	7.01	129.03	



User Agent	10.27	1231.52	Safari/536.26.17
HTTP_ACCEPT Headers	7.01	129.03	text/html, */* gzip, deflate de-de
Browser Plugin Details	20.34	1325115	Plugin 0: Java-Applet-Plug-In; Zeigt Java-Applet-Inhalte an oder einen Platzhalter, falls Java nicht installiert ist.; JavaAppletPlugin.plugin; (Java applet; application/x-java-applet;version=1.1.3;) (Basic Java Applets; application/x-java-applet; javaapplet) (Java applet; application/x-java-applet;version=1.2.2;) (Java applet; application/x-java-applet;version=1.5;) (Java applet; application/x-java-vm;) (Java applet; application/x-java-applet;version=1.3.1;) (Java applet; application/x-java-applet;version=1.3;) (Java applet; application/x-java-applet;version=1.1.2;) (Java applet; application/x-java-applet;version=1.1;) (Java applet; application/x-java-vm-npruntime;) (Java applet; application/x-java-applet;version=1.2.1;) (Java applet; application/x-java-applet;version=1.6;) (Java applet; application/x-java-applet;version=1.4.2;) (Java applet; application/x-java-applet;jpi-version=1.6.0_37;) (Java applet; application/x-java-applet;version=1.4;) (Java applet; application/x-java-applet;version=1.1.1;) (Java applet; application/x-java-applet;version=1.2;). Plugin 1: QuickTime Plug-in 7.7.1; Mit dem QuickTime Plug-in kÃ¶nnen Sie eine Vielzahl von Multimedia-Inhalten auf Webseiten anzeigen. Weitere Informationen erhalten Sie auf der Web-Site fÃ¼r <A HREF=http://www.apple.com/de/quicktime>QuickTime</A>.; QuickTime Plugin.plugin; (Video fÃ¼r Windows (AVI); video/x-msvideo; avi,vfw) (MP3-Audio; audio/mp3; mp3,swa) (MP3-Audio; audio/mpeg3; mp3,swa) (3GPP2-Medien; video/3gpp2; 3g2,3gp2) (CAF-Audio; audio/x-caf; caf) (MPEG-Audio; audio/mpeg; mpeg,mpg,m1s,m1a,mp2,mpm,mpa,m2a,mp3,swa) (QuickTime Film; video/quicktime; mov,qt,mqv) (MP3-Audio; audio/x-mpeg3; mp3,swa) (MPEG-4 Medien; video/mp4; mp4) (SDP-Stream Beschreibung; application/x-sdp; sdp) (WAVE-Audio; audio/wav; wav,bwf) (Video fÃ¼r Windows (AVI); video/avi; avi,vfw) (AC3 Audio; audio/x-ac3; ac3) (MPEG-4 Medien; audio/mp4; mp4) (Video (geschÃ¼tzt); video/x-m4v; m4v) (SDP-Stream Beschreibung; application/sdp; sdp) (WAVE-Audio; audio/x-wav; wav,bwf) (AIFF-Audio; audio/x-aiff; aiff,aif,aifc,cdda) (MPEG-Medien; video/x-mpeg; mpeg,mpg,m1s,m1v,m1a,m75,m15,mp2,mpm,mpv,mpa) (3GPP-Medien; video/3gpp; 3gp,3gpp) (Video fÃ¼r Windows (AVI); video/msvideo; avi,vfw) (MPEG-Audio; audio/x-mpeg; mpeg,mpg,m1s,m1a,mp2,mpm,mpa,m2a,mp3,swa) (QUALCOMM PureVoice Audio; audio/vnd.qcelp; qcp,qcp) (MP3-Audio; audio/x-mp3; mp3,swa) (RTSP-Stream Beschreibung; application/x-rtsp; rtsp,rts) (AMR-Audio; audio/amr; amr) (SD-Video; video/sd-video; sdv) (AIFF-Audio; audio/aiff; aiff,aif,aifc,cdda) (MPEG-Medien; video/mpeg; mpeg,mpg,m1s,m1v,m1a,m75,m15,mp2,mpm,mpv,mpa) (3GPP2-Medien; audio/3gpp2; 3g2,3gp2) (AAC-Audio; audio/aac; aac,adts) (AC3 Audio; audio/ac3; ac3) (AAC-HÃ¶rbuch; audio/x-m4b; m4b) (AAC-Audiodatei (geschÃ¼tzt); audio/x-m4p; m4p) (GSM-Audio; audio/x-gsm; gsm) (AMC-Medien; application/x-mpeg; amc) (AAC-Audio; audio/x-aac; aac,adts) (uLaw/AU-Audio; audio/basic; au,snd,ulw) (AAC-Audio; audio/x-m4a; m4a) (3GPP-Medien; audio/3gpp; 3gp,3gpp). Plugin 2: Shockwave Flash; Shockwave Flash 11.5 r502; Flash Player.plugin; (Shockwave Flash; application/x-shockwave-flash; swf) (FutureSplash Player; application/futuresplash; spl). Plugin 3: WebKit-integrierte PDF; ; ; (PDF (Portable Document Format); application/pdf; pdf). Plugin 4: iPhotoPhotocast; iPhoto6; iPhotoPhotocast.plugin; (iPhoto 700; application/photo;).

Beispiel für Anwendung von Browser Fingerprint

- Laterpay: Bezahldienstanbieter für Micropayments

- Zitat aus den AGBs für Nutzer von Laterpay: (ca. 2016)

  »Was macht LaterPay, um Ihr Internet-fähiges Endgerät zu identifizieren?

  LaterPay verwendet unterschiedliche Verfahren um sicherzustellen, dass der Bezahlinhalteanbieter dem richtigen Endgerät ermöglicht, von dem Vertrauensvorschuss zu profitieren und Inhalte zu konsumieren, bevor eine Registrierung erfolgt.

  Hierfür werden wahlweise Browser Fingerprint und die IP-Adresse, Daten des Bezahlinhalteanbieters, Protokolleigenschaften sowie Cookies verwendet.«

  https://www.laterpay.net/terms/

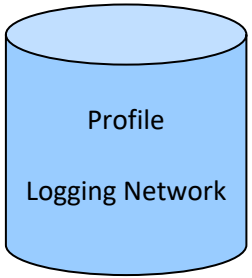
Device Fingerprinting

- Unique? App
  - Shows possible device identifiers
  - Developed at University of Erlangen

App 1: SN-Device, start, stop, …
82031M6UV2F, 2012-12-19T16:39:57

App 2: SN-Device, start, stop, address book, …
82031M6UV2F, 2012-12-20T12:19:11, data

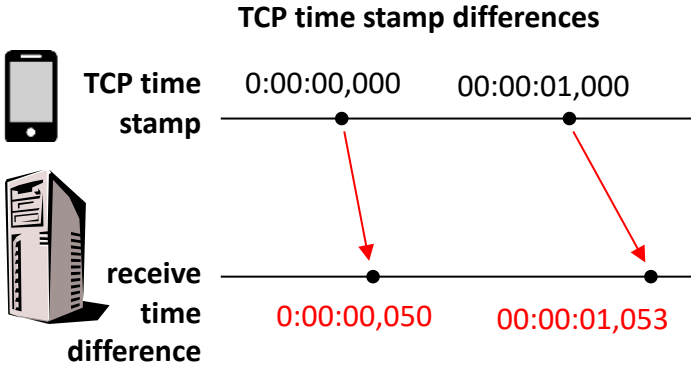
App 3: SN-Device, start, stop, location info, …
82031M6UV2F, 2012-12-20T12:21:23, data

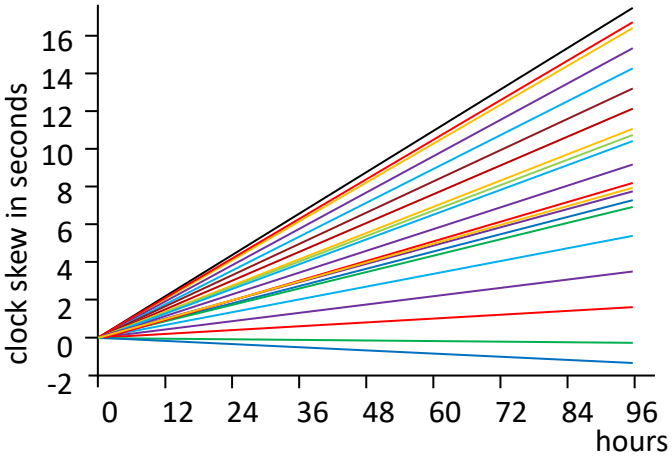


http://www.iphone-ticker.de/oh-mein-gott-so-eindeutig-laesst-jedes-iphone-zuordnen-66244/

Timing differences for mobile device identification

- Long term observation of deterministic and device specific internal clock skew of mobile devices

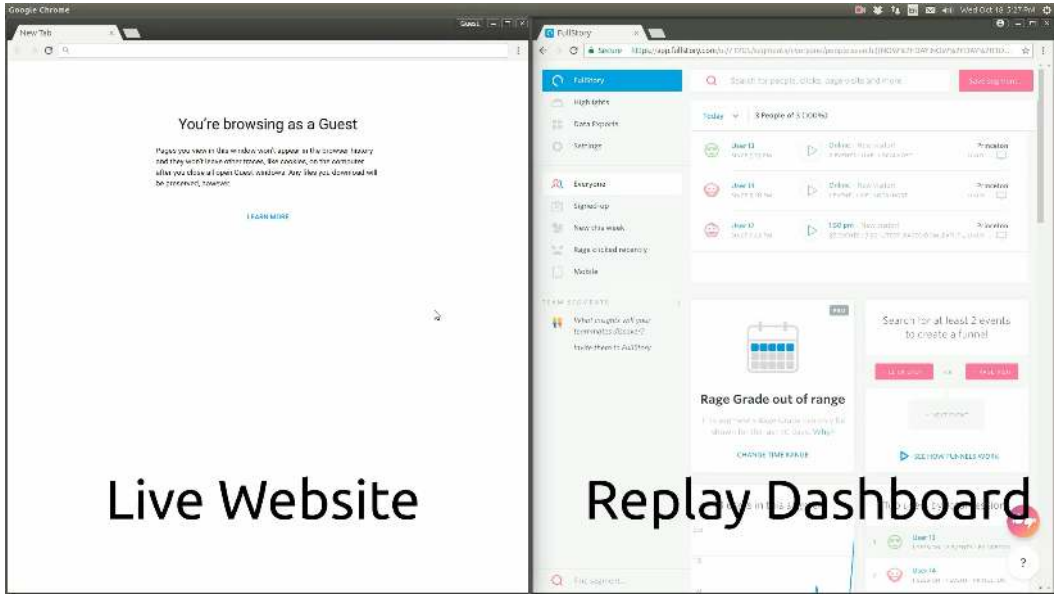




- Protection ideas
  - modification of TCP standard
  - add noise (time jitter) to TCP time stamp

Tadayoshi Kohno, Remote physical device fingerprinting, 2005 and c't 11 (2014) 160-161

- Tracking by use of JavaScript functionallity allows full recording of a browser session (within a browser window)
  - Mouse movements
  - All typing events – also before submitting a web form

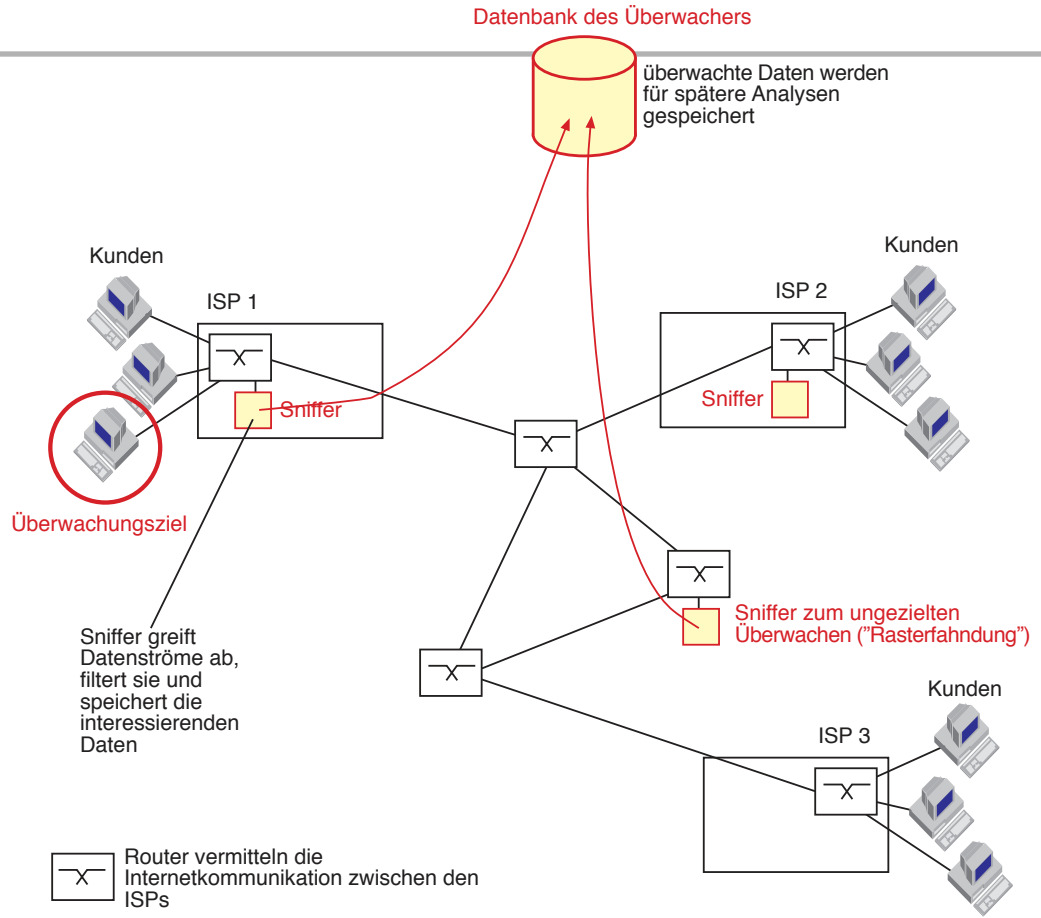


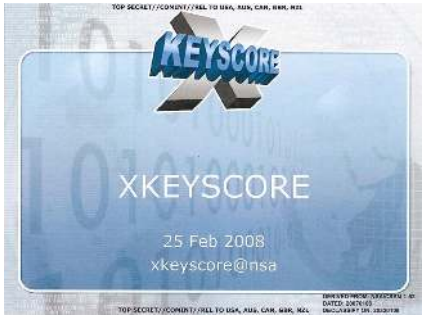
Source: https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/

Zur Verantwortung von Informatiker*innen

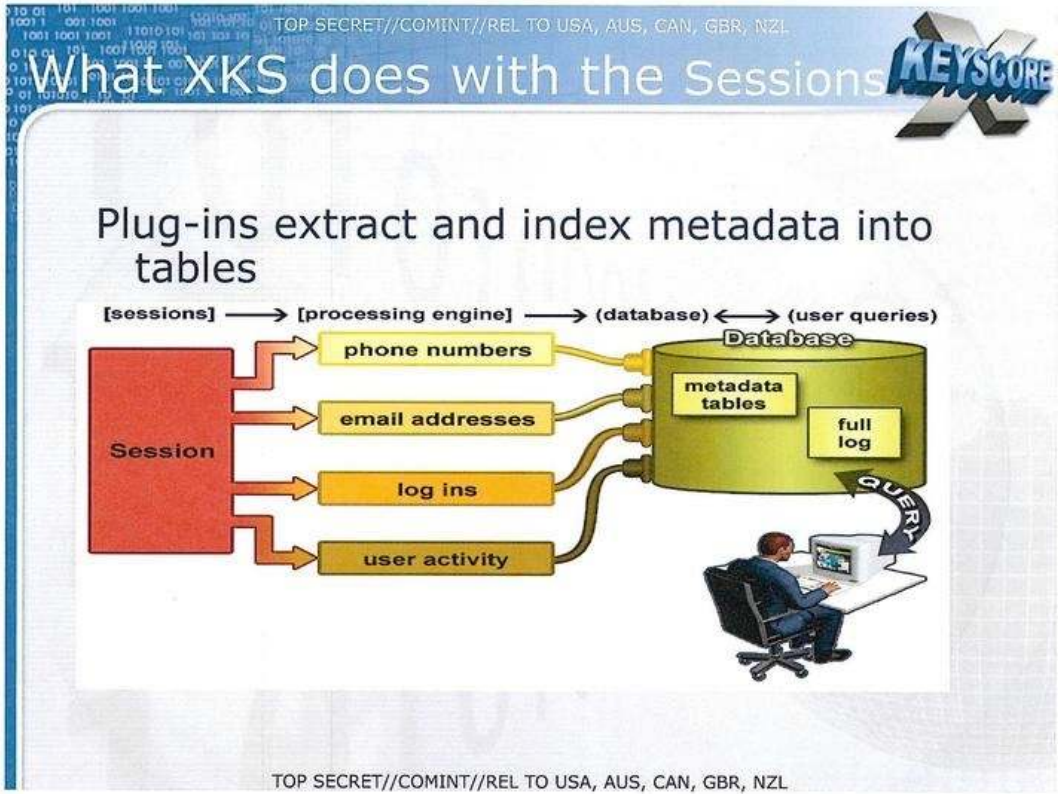
- Wo die Kategorien »Gut und Böse« weiterhelfen
  - Ethische Aspekte
- Wir bezahlen mit unseren Daten
  - Spannungsfeld von Online-Marketing und Datenschutz
- Ich habe doch nichts zu verbergen
  - Innere Sicherheit und Überwachung
- Drohnenkrieg
  - Militärischer Einsatz von Informationstechnologie

Carnivore

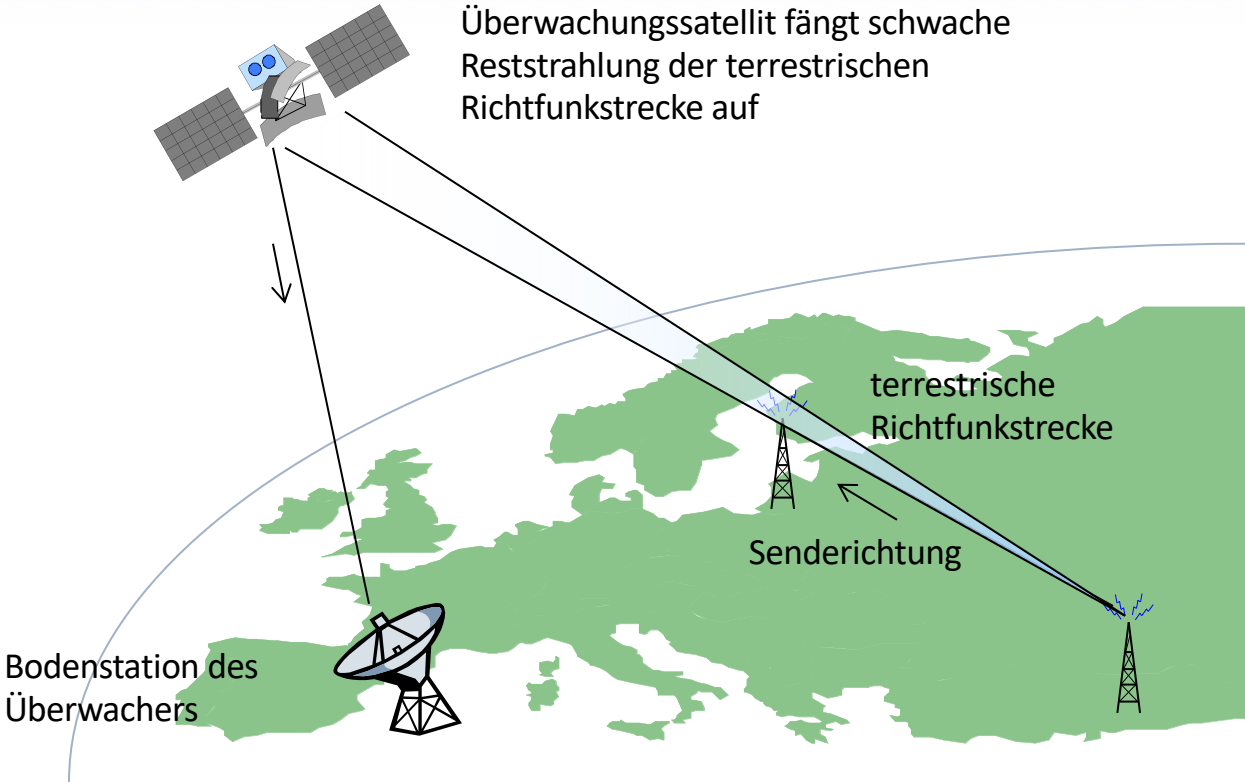

Datenbank des Überwachers
überwachte Daten werden für spätere Analysen gespeichert
Kunden
ISP 1
Sniffer
Überwachungsziel
Sniffer greift Datenströme ab, filtert sie und speichert die interessierenden Daten
Kunden
ISP 2
Sniffer
Sniffer zum ungezielten Überwachen ("Rasterfahndung")
Kunden
ISP 3
Router vermitteln die Internetkommunikation zwischen den ISPs



Quelle: Wikimedia



ECHELON


Überwachungssatellit fängt schwache Reststrahlung der terrestrischen Richtfunkstrecke auf
terrestrische Richtfunkstrecke
Senderichtung
Bodenstation des Überwachers

ECHELON

- Das EU-Parlament über das globale Überwachungssystem ECHELON:

  - »... daß nunmehr kein Zweifel mehr daran bestehen kann, daß das System nicht zum Abhören militärischer, sondern zumindest privater und wirtschaftlicher Kommunikation dient, ...«

  - »... ihre Bürger und Unternehmen über die Möglichkeit zu informieren, daß ihre international übermittelten Nachrichten unter bestimmten Umständen abgefangen werden; besteht darauf, daß diese Information begleitet wird von praktischer Hilfe bei der Entwicklung und Umsetzung umfassender Schutzmaßnahmen, auch was die Sicherheit der Informationstechnik anbelangt; ...«

Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)). EU Parlament, Nichtständiger Ausschuss über das Abhörsystem Echelon, Sitzungsdokument A5-0264/2001, Teil 1, 11. Juli 2001.

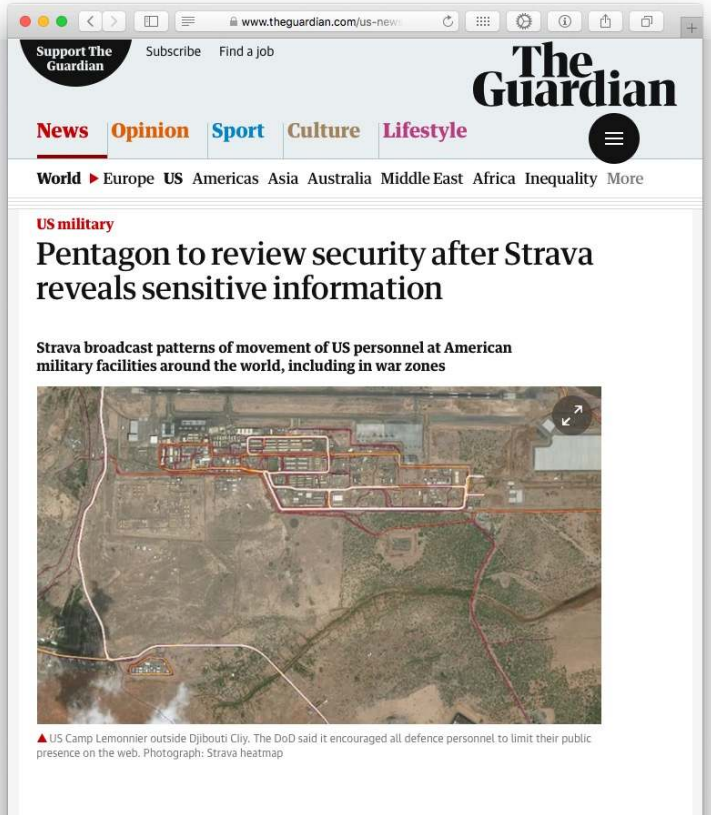
ECHELON

- Überwachungsstation in Bad Aibling

Source: http://ig.cs.tu-berlin.de/w2000/ir1/referate2/b-1a/

Soziale Netze und Datenschutz – Der Fall »Strava Heatmap«

- Fitness-Tracker Website veröffentlicht beliebte Laufstrecken
- Soldaten des US-Militärs offiziell ausgestattet mit Fitness-Tracker
- Öffentliche »Heatmap« enthüllt ungewollt geheime US-Bases im Ausland



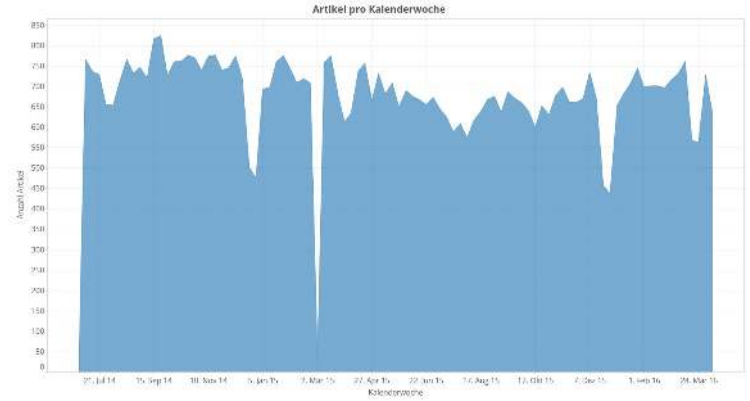
Sources:
https://twitter.com/Nrg8000/status/957318498102865920
https://www.theguardian.com/us-news/2018/jan/29/pentagon-strava-fitness-security-us-military

https://www.dkriesel.com/spiegelmining

- Reverse Engineering von über 70.000 Spiegel-Online-Artikeln (2016)
- Verteilung von veröffentlichten Artikeln der Rubriken über das Jahr
- Kombination von Merkmalen: Textlänge und Zeit
  - längste Artikel wochentags zwischen 5 und 6 Uhr wochentags
  - längste Artikel am Wochenende zwischen 7 und 9 Uhr
- Auch Arbeits-, Urlaubs und Redaktionsgewohnheiten waren aus den Daten analysierbar.

SpiegelMining. Auch Spiegelredakteure feiern Weihnachten. Eine Analyse von 70.000 SpiegelOnline-Artikeln

Seit Mitte 2014 habe ich mehr als 70.000 Artikel von SpiegelOnline systematisch gespeichert. Jeden Tag kommen im Schnitt 100 dazu. Diese Artikelmasse werden wir in der nächsten Zeit auswerten und erforschen. Was herauskommt, ist eine tiefgreifende Analyse des Publikationsverhaltens des vielleicht größten Meinungsmachers Deutschlands.



https://www.dkriesel.com/blog/2016/0725_spiegelmining_analyse_70000_spiegelonline_artikel

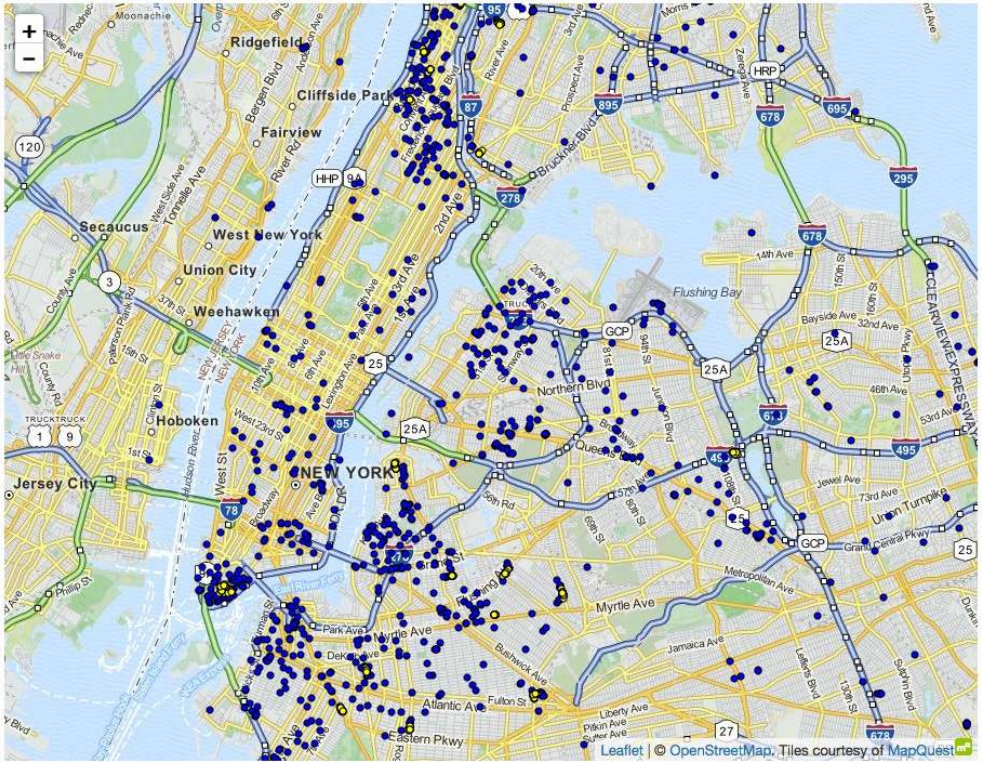
Pseudonymisierte Daten…

…können Persönlichkeitsrechte verletzen.

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

Daten öffentlich abrufbar unter:

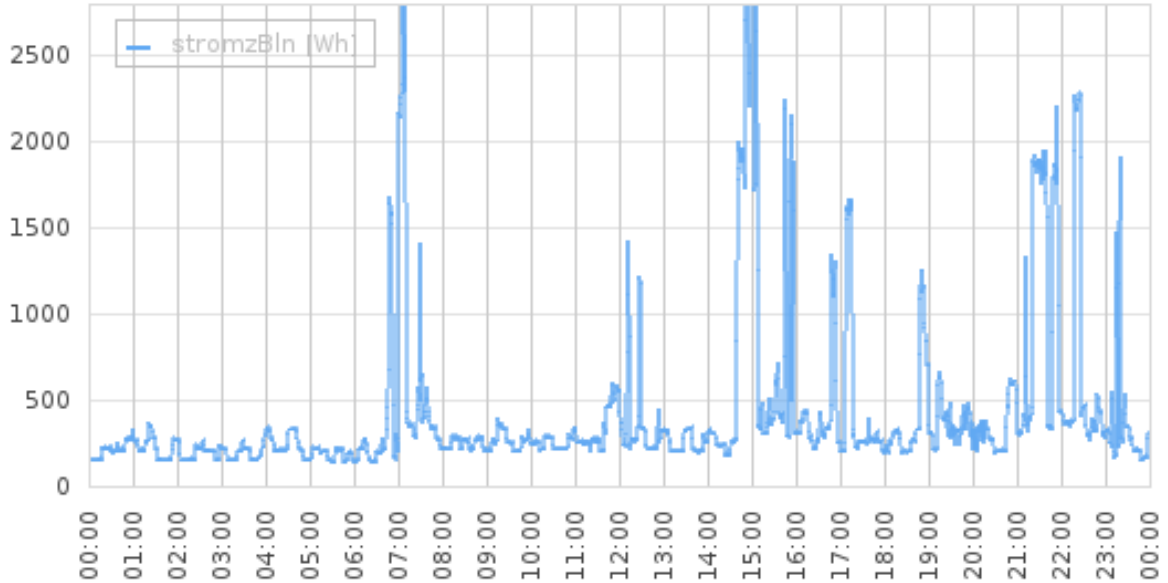
http://www.andresmh.com/nyctaxitrips/



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 (2014)

Stromverbrauch verrät Infos über persönliche Lebensverhältnisse



Bundestrojaner, Stuxnet, Flame

- Darf sich der Staat auch solcher Angriffsmethoden bedienen,
  - die zwar dem Schutz des Staates und seiner Bürger dienen, jedoch die Integrität und Vertrauenswürdigkeit von IT-Systemen untergraben und schlimmstenfalls auch gegen ihn selbst verwendet werden können?

- Antwort: »Neues Computergrundrecht«
  - Bundesverfassungsgericht im Februar 2008:
    - Grundrecht auf »Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme«
    - Erlaubte Einschränkungen:
      - Gefährdung von Leib, Leben und Freiheit einer Person
      - Gefährdung der Grundlagen des Staates
      - Gefährdung der Grundlagen der Existenz der Menschen

Darf sich der Staat auch solcher Angriffsmethoden bedienen?

- Implementierungen
  - politisch motivierte staatliche Angriffe mit oder auf IT-Systeme anderer Staaten (Cyberwarfare)
    - Stuxnet, (Duqu,) Flame
  - Gesetzlich erlaubte Telekommunikationsüberwachung und Beweissicherung (Online Durchsuchung) direkt auf dem PC eines Verdächtigen
    - Staatstrojaner / Bundestrojaner

Stuxnet: Angriffsszenario Industrieanlage

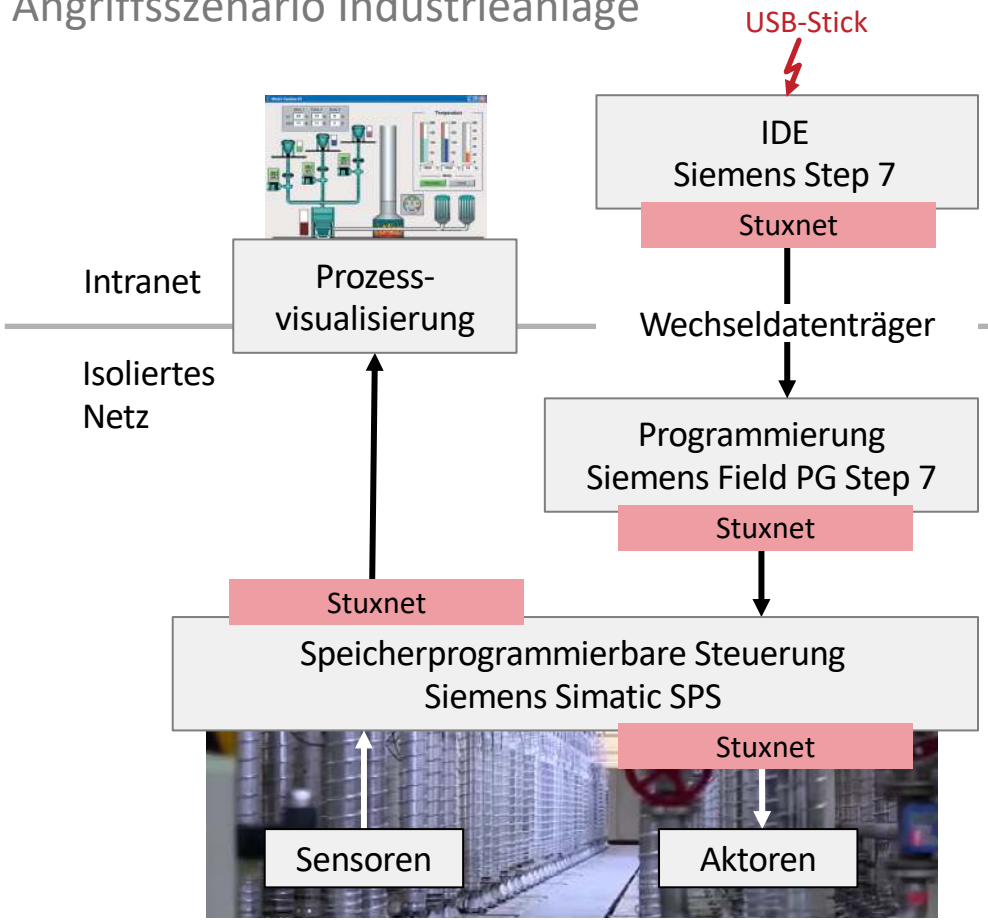
- Internetwurm, der mit dem Ziel entwickelt wurde, die innerbetrieblichen Abläufe eines speziellen Typs von Industrieanlagen empfindlich zu stören
  - Entdeckung im Juli 2010
  - Ziel: Unbemerkte Änderung von Programmteilen in speicherprogrammierbaren Steuerungen (SPS)
  - Verwendet vier Zeroday-Exploits zur Verbreitung und Rechteausweitung
  - Selbstzerstörung (nur Windows-Komponente) nach 35 Tagen

- Urheber: USA und Israel
  - Anordnung von 2006 von US-Präsident Gerorge W. Bush
  - in 2010 bestätigt durch Präsident Obama

  Quelle: New York Times: Obama Order Sped Up Wave Of Cyberattacks Against Iran. June 1, 2012, page A1

Bild von Natanz (Majid Saeedi/Getty Images)

Stuxnet, 2010:
Angriffsszenario Industrieanlage



Treiber mit gestohlenen Zertifikaten (Realtek, JMicron) signiert

Manipulation Step-7-IO-Treiber und -Projektdateien

Vermutlich genaue Kenntnis der Anlagen vorhanden gewesen

Stuxnet überprüft Konfiguration der SPS und befällt nur bestimmte Systeme

Transitives trojanisches Pferd, da zunächst die IDE befallen wird, um anschließend die SPS zu manipulieren.

Mechanische Zerstörung (Drehzahlmanipulation) der Zentrifugen

Spionagesoftware:
Pegasus (NSO Group) und Predator

https://www.sueddeutsche.de/politik/pegasus-spionage-bka-trojaner-1.5403678 (9.2021)
https://www.dw.com/de/pegasus-spionage-skandal-ohne-ende/a-62476414 (7.2022)
https://www.deutschlandfunkkultur.de/watergate-in-griechenland-100.html (10.2022)

Das BKA habe eine legale Version erworben, erklärt die Vizechefin der Behörde

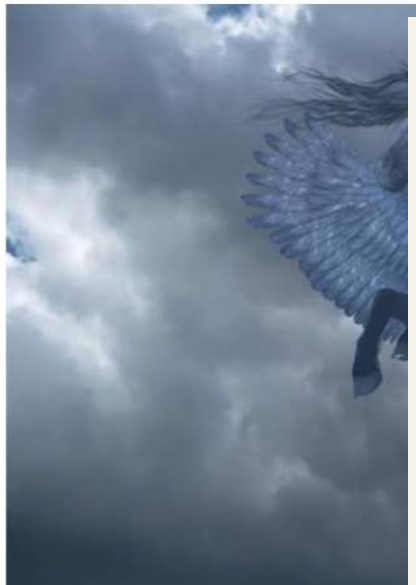
Das BKA habe allerdings nicht die Standardversion der Software erworben, erklärte Vizebehördenchefin Link im Bundestag. Denn "Pegasus" könne viel mehr, als das deutsche Gesetz erlaube. Das herkömmliche Programm unterscheide normalerweise nicht zwischen Quellen-Telekommunikationsüberwachung, also dem Mitlesen von Chats, und Online-Durchsuchung, also dem Ausspähen von gespeicherten Dateien auf einem Smartphone. Zudem sei nicht ausreichend nachvollziehbar, was die Software eigentlich so mache auf einem Zielgerät.

Die israelische Herstellerfirma habe allerdings auf Wunsch des BKA eine technische Anpassung vorgenommen und eine Software entwickelt, die verfassungskonform eingesetzt werden könne, sagte Link. Dieser maßgeschneiderte Trojaner sei durch das BKA umfangreich überprüft worden. Man habe sich dabei auch mit dem Bundesamt für die Sicherheit in der Informationstechnik (BSI) abgestimmt. Es seien außerdem Sicherheitsvorkehrungen getroffen worden, so würden die überwachten Telefonnummern durch Hashwerte verschleiert, sodass die Herstellerfirma die Zielpersonen nicht identifizieren könne. Darüber hinaus habe man sich von NSO vertraglich zusichern lassen, dass keine Daten an die Firma abfließen, sondern an das BKA.

MENSCHENRECHTE UND DATENSCHUTZ

Pegasus: Spionage-Skandal ohne Ende

Kein Smartphone ist sicher, wenn es mit der Spähsoftware Pegasus infiziert wird. In Thailand sollen Demokratie-Aktivisten damit ausspioniert worden sein. Zu den deutschen Kunden gehören womöglich das BKA und der BND.



Spionagesoftware namens Predator

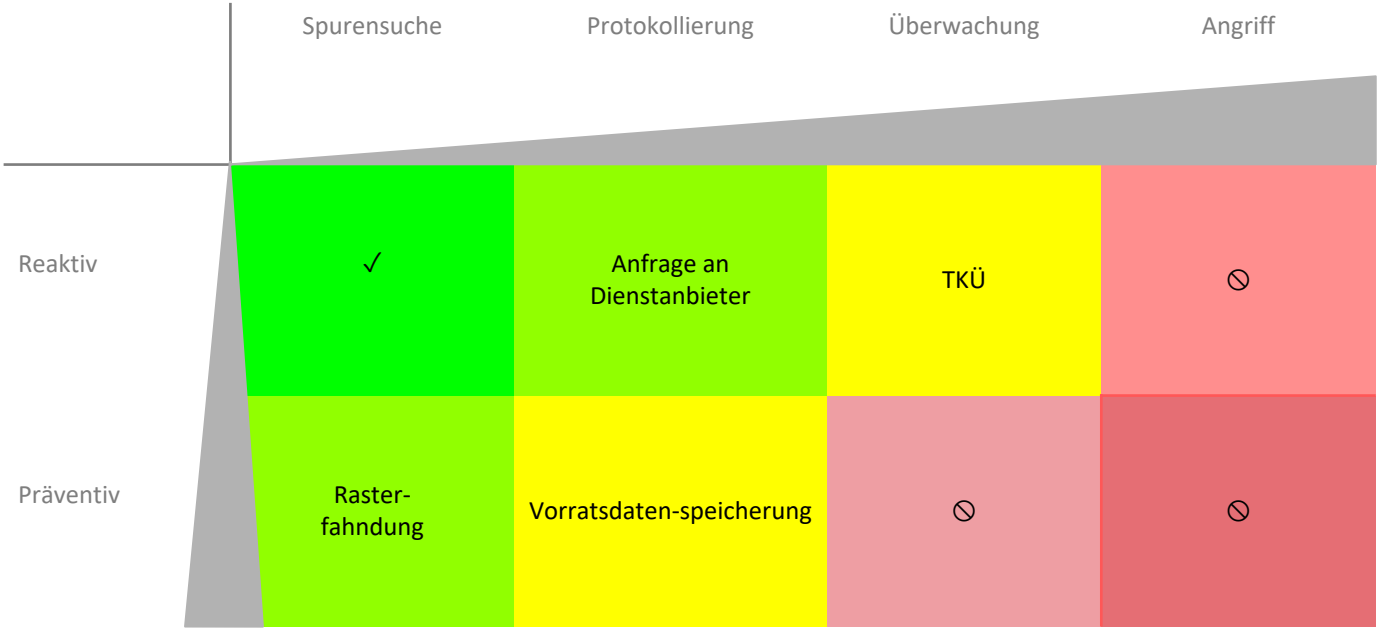
Im Juli 2021 untersuchen Bill Marczak und seine Kollegen das Handy eines Menschenrechtsaktivisten aus Saudi-Arabien und entdecken dort neben Pegasus noch eine zweite neue Spionagesoftware.

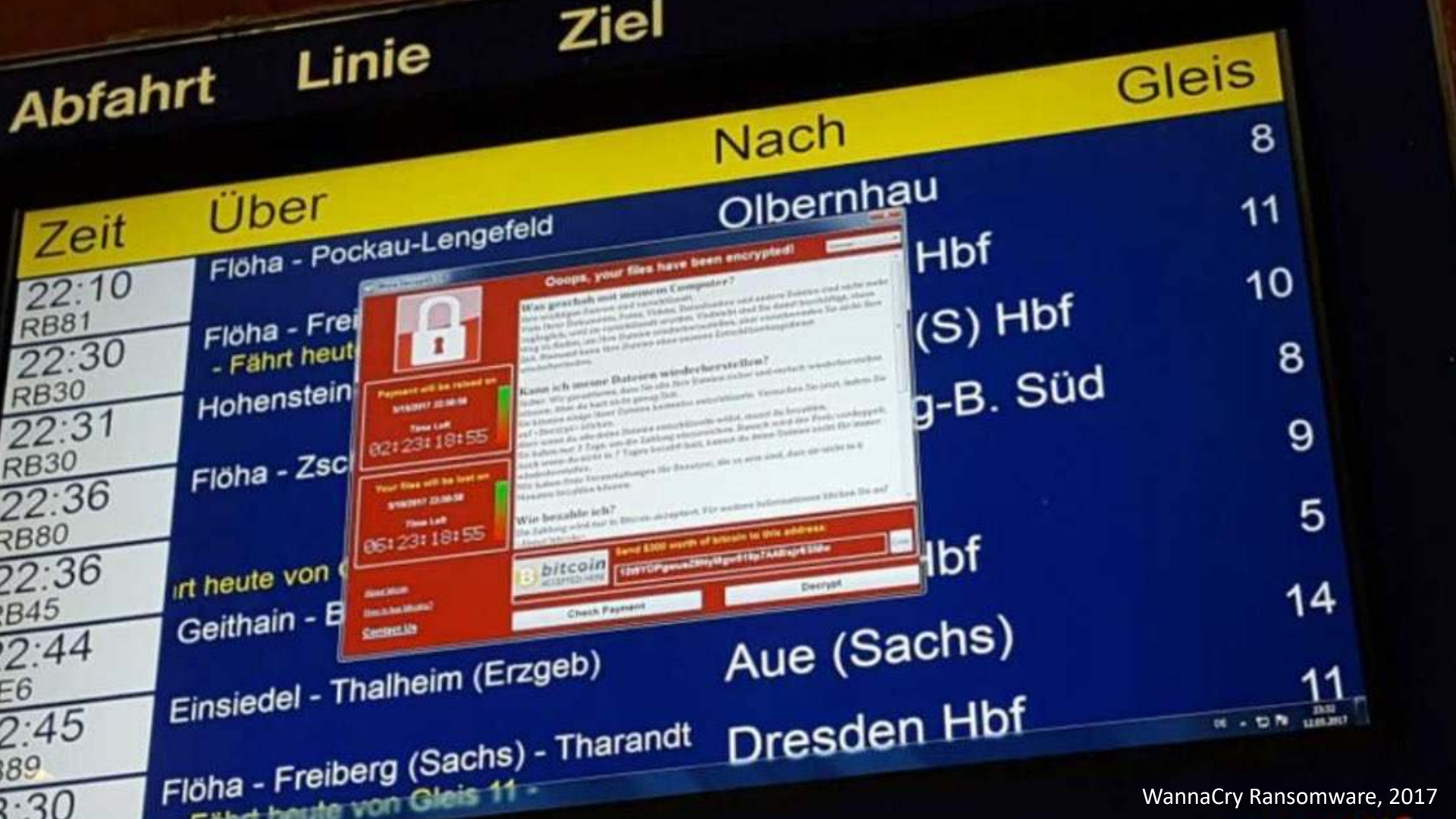
"Die Spyware trug mehrmals den Namen Predator im Software-Code, was uns sehr interessiert hat", so Marczak. Sie beginnen mit der Untersuchung, finden einen infizierten Link auf dem Handy. Klickt man da drauf, installiert sich Predator automatisch und das Mobiltelefon selbst wird zur modernen Wanze.

& Die Spionagesoftware schneidet nicht nur Telefongespräche mit, sondern alles, was in der Umgebung des Telefons passiert. Sie macht Screenshots, greift Passwörter ab und kann auch Chats in vermeintlich sicheren Kurznachrichtendiensten wie Whatsapp, Telegram und Signal mitlesen.

Eingriffstiefe in die Freiheit

- Darf sich der Staat solcher Angriffsmethoden bedienen?





WannaCry Ransomware, 2017

Zur Verantwortung des Informatikers

- Wo die Kategorien »Gut und Böse« weiterhelfen
  - Ethische Aspekte
- Wir bezahlen mit unseren Daten
  - Spannungsfeld von Online-Marketing und Datenschutz
- Ich habe doch nichts zu verbergen
  - Innere Sicherheit und Überwachung
- Drohnenkrieg
  - Militärischer Einsatz von Informationstechnologie

Militärischer Einsatz von Informationstechnologie

Aufklärungsdrohne Heron 1 und deren Steuerung

Bilder: www.bundeswehr.de

- Spannungsfeld:
  - Fern-Aufklärung mittels Informationstechnik √
  - Fern-Tötung mittels Informationstechnik ?

Aus dem Beweisbeschluss SV-14 vom 7. Juli 2016 des 1. Untersuchungsausschusses der 18. Wahlperiode des Deutschen Bundestages:

«… Ist unter Berücksichtigung der festgestellten Bedingungen eine Telefonnummer – beziehungsweise eine IMEI- oder IMSI-Identifizierung – als einziges technisches Datum mittelbar oder unmittelbar ausreichend, um eine Fernlenkwaffe mit hinreichender Treffergenauigkeit für eine gezielte Tötung einsetzen zu können? …»

Geleakte Fassung unter https://tinyurl.com/gtv552j

Bild: https://upload.wikimedia.org/wikipedia/commons/3/33/MQ-9_Reaper_-_090609-F-0000M-777.JPG

IMSI-Catcher in Drohne simuliert Mobilfunkzelle

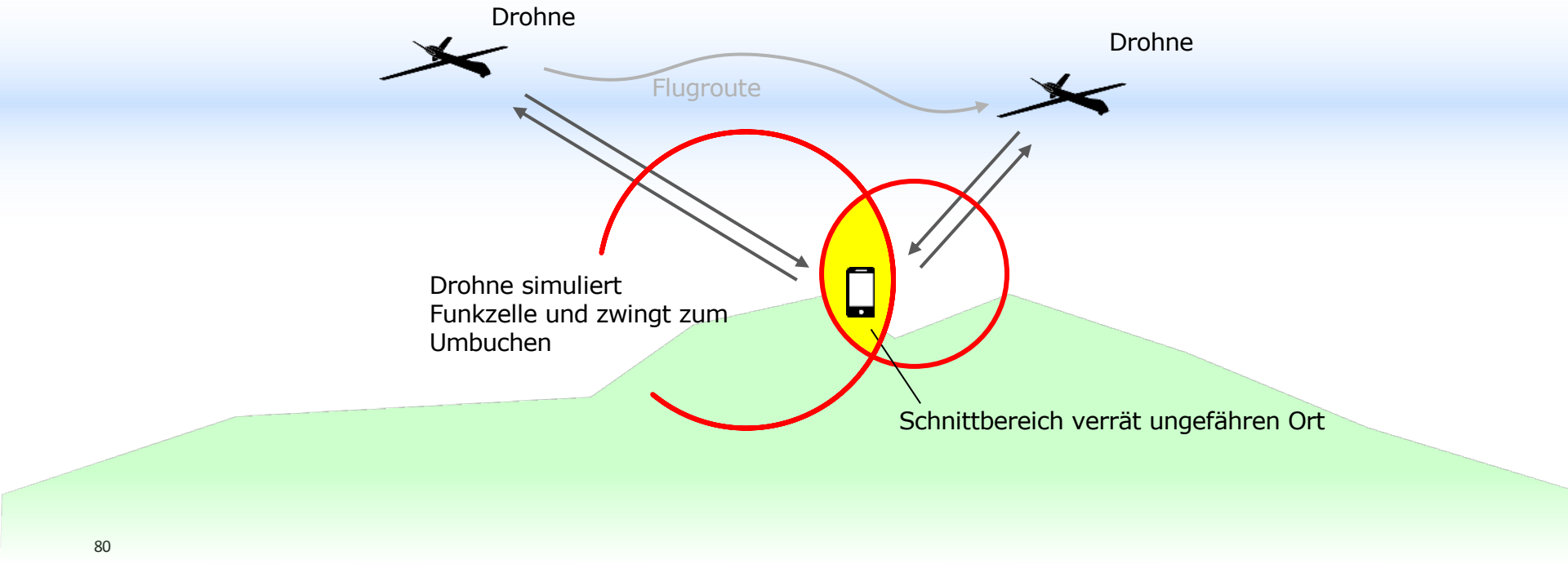
MFG wählt sich in die Funkzelle ein und es werden IMSI/TMSI und IMEI übertragen

Drohne bestimmt Empfangsrichtung der Funkwellen

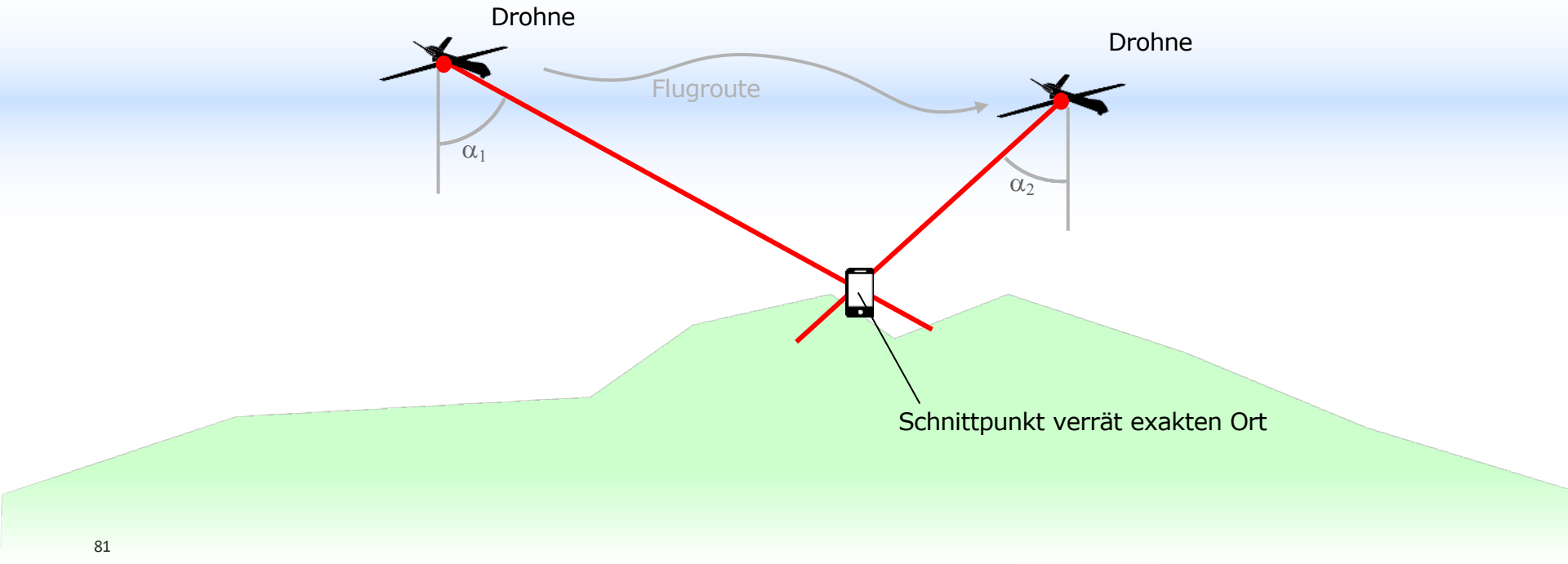
Positionsermittlung als Schnittpunkt der Erdoberfläche mit der Empfangsrichtung

Bild: https://upload.wikimedia.org/wikipedia/commons/3/33/MQ-9_Reaper_-_090609-F-0000M-777.JPG

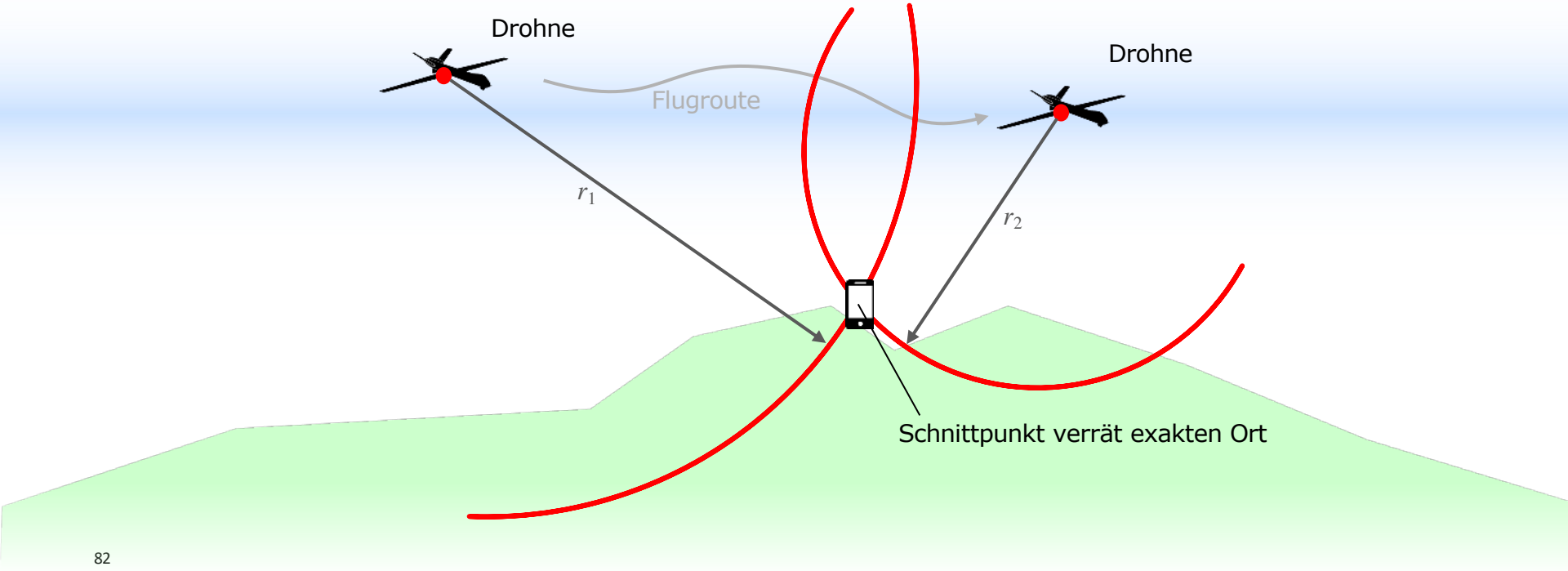
IMSI-Catcher in Drohne simuliert Mobilfunkzelle



Drohne bestimmt Empfangsrichtung der Funkwellen



Drohne bestimmt Empfangsrichtung der Funkwellen



Zur Verantwortung des Informatikers

- Wo die Kategorien »Gut und Böse« weiterhelfen
  - Ethische Aspekte
- Wir bezahlen mit unseren Daten
  - Spannungsfeld von Online-Marketing und Datenschutz
- Ich habe doch nichts zu verbergen
  - Innere Sicherheit und Überwachung
- Drohnenkrieg
  - Militärischer Einsatz von Informationstechnologie

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