Funktioniert Datenschutz im Unsichtbaren?

– Datenschutzgarantien, Transparenz und Intervenierbarkeit in versteckter Informationstechnik –

Marit Hansen

FIfFKon16 „in.visible systems“

26.11.2016, Berlin

forum <privatheit> selbstbestimmtes_leben_in_der_digitalen_welt

ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Roter Faden

- Datenschutz
  - Grundlage in Deutschland
  - Gewährleistungsziele
- Herausforderung „unsichtbar“
- Lösungsansätze: neu aufgestellt mit der Datenschutz-Grundverordnung?
- Fazit

Bild: Sjoerd Los

DATENSCHUTZ

Beim Datenschutz geht es primär um ~~Daten~~

Bild: Ashtyn Renee

Menschen mit ihren Rechten

Prüffragen bei der Gestaltung:

- Auswirkungen auf Menschen?
- Auswirkungen auf die Gesellschaft?

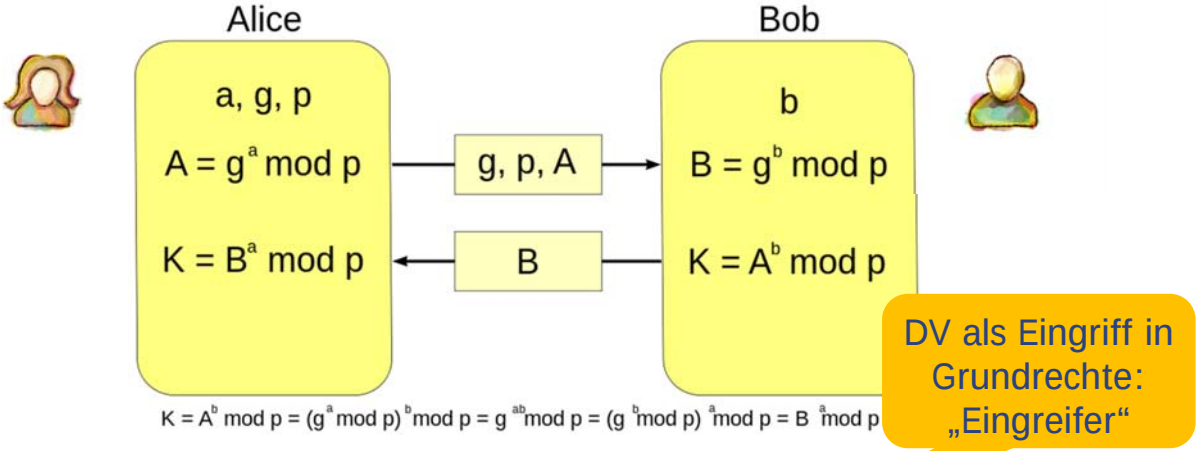
Datenschutz nötig:
Machtgefälle

Wichtig:
Perspektive der betroffenen Personen

Ansatzpunkt:
personen-bezogene Daten

Bild: Azureon2

Perspektive: Alice & Bob



DV als Eingriff in Grundrechte: „Eingreifer“

IT-Sicherheit: Der Angreifer ist Eve (oder Mallory).

Datenschutz: Der Angreifer ist Bob!
(Jedenfalls auch.)

Recht auf informationelle Selbstbestimmung

- Datenschutz-Grundrecht 1:
  „Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen“
- Jeder soll wissen können, wer was wann über ihn weiß.
- Anlass: Volkszählung
- Bundesverfassungsgericht: Urteil vom 15. Dezember 1983 (BVerfGE 65, 1)

IT-Grundrecht

- Datenschutz-Grundrecht 2:
  „Recht auf Gewährleistung der Vertraulichkeit und der Integrität informationstechnischer Systeme“
- Grundrecht auf digitale Intimsphäre;
  präventive staatliche Zugriffe nur bei tatsächlichen Anhaltspunkten einer konkreten Gefahr für ein überragend wichtiges Rechtsgut
- Anlass: Online-Durchsuchung
- Bundesverfassungsgericht: Urteil vom 27. Februar 2008 (1 BVR 37/07, 1 BVR 595/07)

Datenschutz-Grundsätze

Für personenbezogene Daten:

- Rechtsgrundlage, z.B. Gesetz oder Einwilligung
- Zweckbindung
- Erforderlichkeit
- Transparenz
- Betroffenenrechte
- Datensicherheit

Datenschutz >> Sicherheit personenbez. Daten

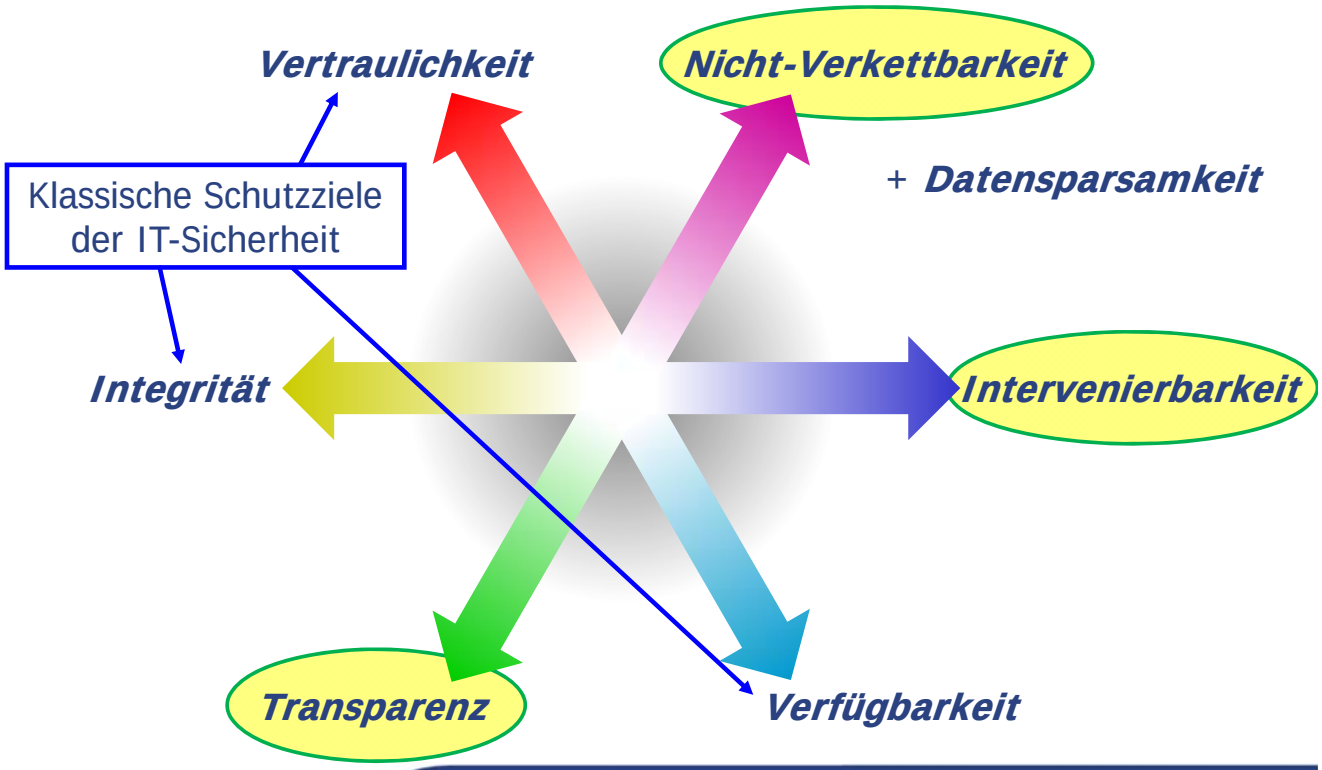


Bild: Daniel Lobo

HERAUSFORDERUNG „UNSICHTBAR“

Realität heute: dominierende Anbieter in allen Lebenslagen

In Teilen unsichtbar
(nicht wahrnehmbar/unbekannt):

- Verarbeitung wo und wann?
- Wie genau?
- Zugriffe durch welche Dritten?

PayPal

Google

Microsoft

Akamai

facebook

amazon

twitter

Realität heute: komplexe Arbeitsteilung

Zugriff auf eine (?) Webseite

Wem gehört die Webseite?

re:publica TEN

	BILD.DE	SPON	SZ
Requests	2339	2514	1886
Unique Hosts	195	184	172
3rd Party Hosts	182	172	160
Own Hosts (*)	13	12	12

(*) basiert auf augenscheinlich zum Verlag gehörenden Domains/Subdom

re:publica 2016 – Thorsten Schröder & Frank Rieger: Ad-Wars

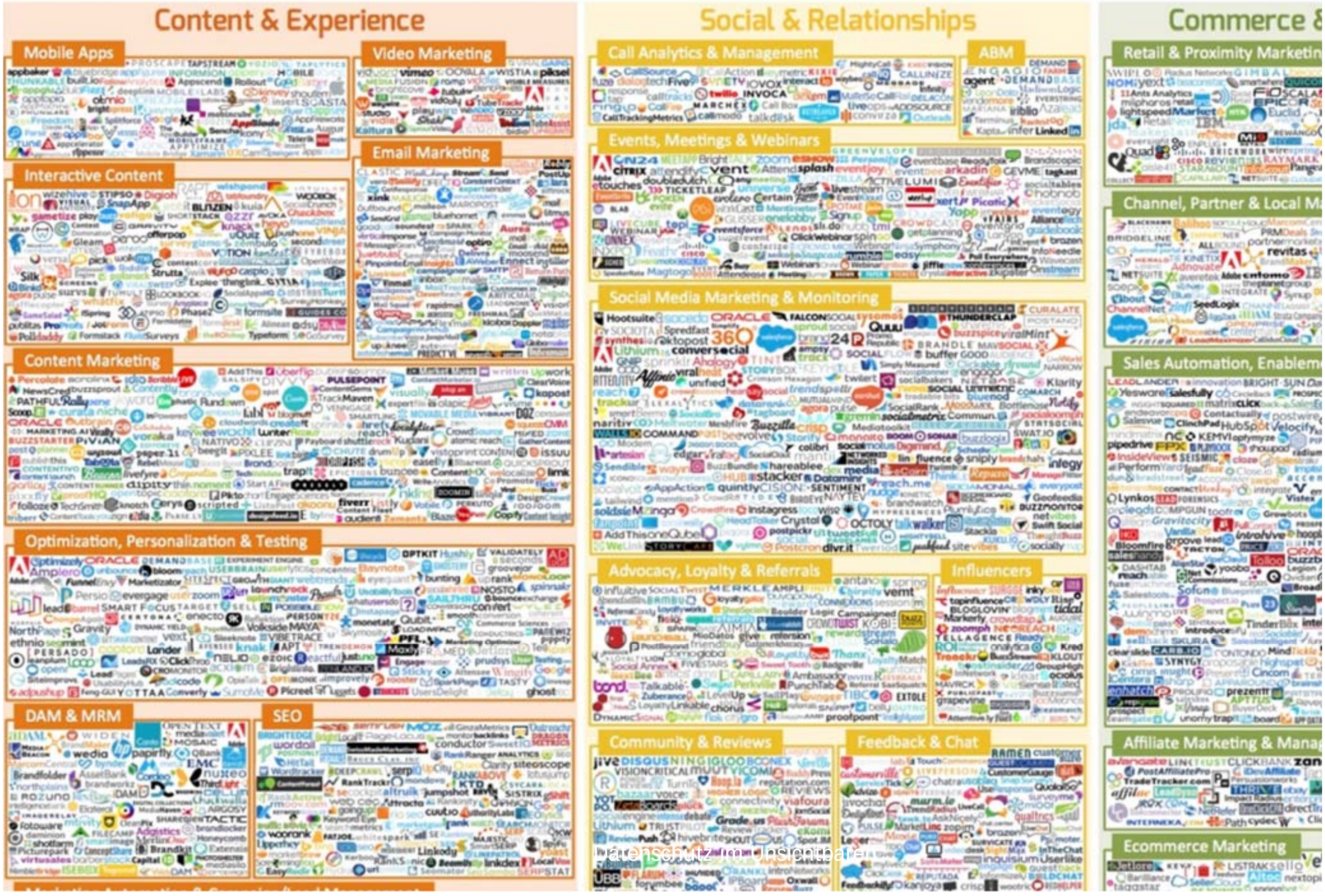
re:publica Abonnieren 11.008

Unsichtbare (unerwartete) massenhafte Einbindung von Dienstleistern:

- Sicherheit- und Datenschutzrisiken
- Transparenz?
- Nutzer-Intervention praktikabel?
- Verantwortung??

Realität heute: Marketing-Markt für (unsichtbare) Integration in Angebote

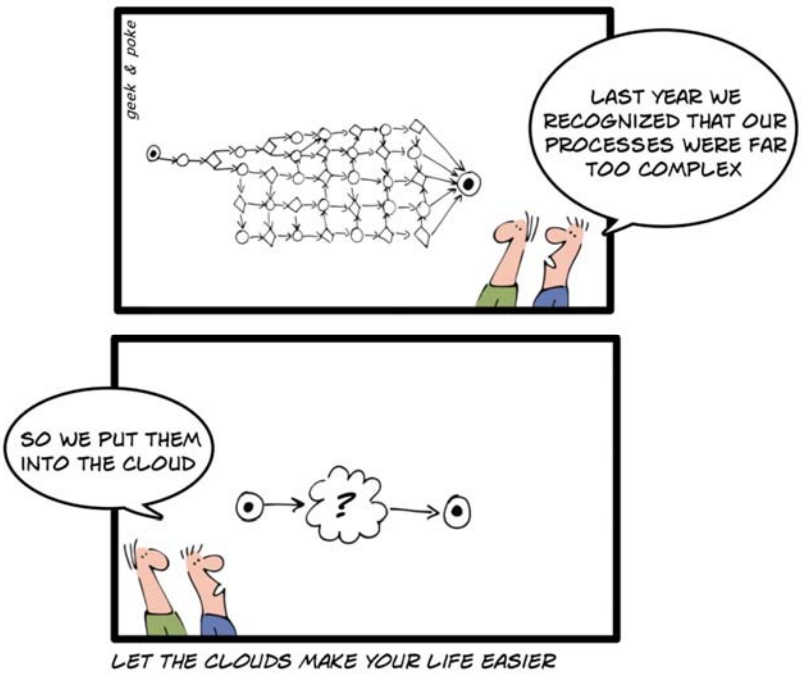
:.com Marketing Technology Landscape



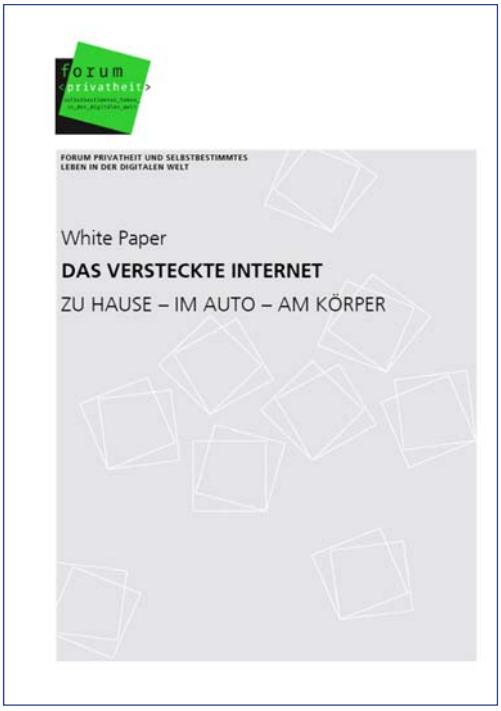
Realität heute: Cloud verbirgt Komplexität

Cloud als Default:

- Abhängigkeit von Dienstleistern
- Fremdbestimmbarkeit statt Eigenkontrolle
- Zugriffe durch welche Dritten?



Realität heute: „verstecktes Internet“

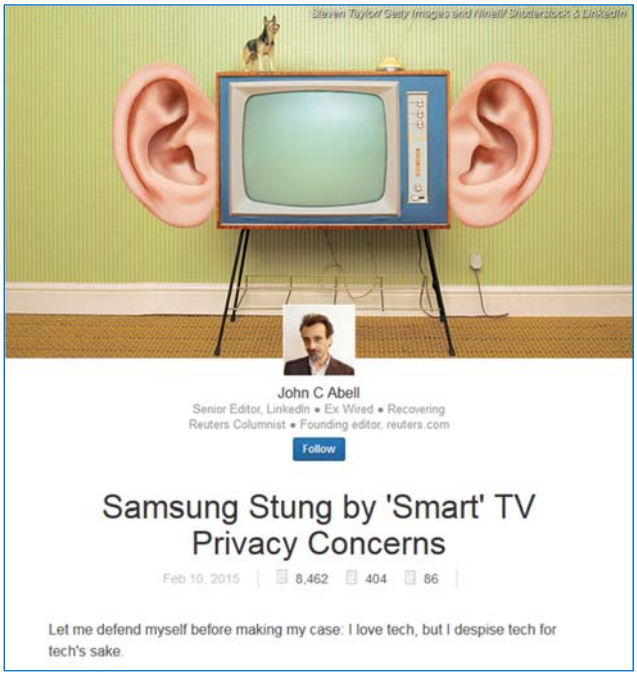


https://www.forum-privatheit.de/forum-privatheit-de/aktuelles/aktuelles_dokumente/White-Paper-2-Final_17.07.15-Druckversion.pdf

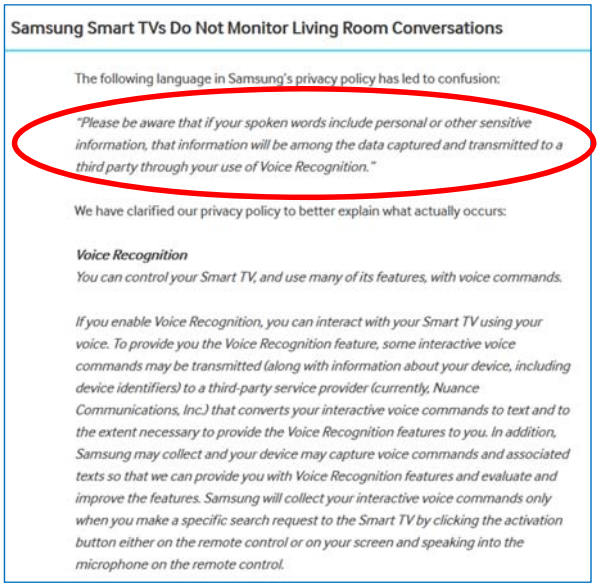
DANA 1/2015

https://pixabay.com/

Beispiel: Samsung + Drittanbieter „Nichts Privates sagen“



https://www.linkedin.com/pulse/when-good-tech-goes-bad-smart-tv-edition-john-c-abell



http://global.samsungtomorrow.com/samsung-smart-tvs-do-not-monitor-living-room-conversations/

Smart Home: nicht alles für jeden unsichtbar

Bild: CODE_n

„Betreiber“:
- Haushaltsvorstand
- Vermieter
- Arbeitgeber

Nicht ganz neu: vgl. TK-Anlage und Einzelverbindungsnachweis

§ 99 Abs. 1 TKG:

„[...] Bei Anschlüssen im Haushalt ist die Mitteilung nur zulässig, wenn der Teilnehmer in Textform erklärt hat, dass er alle zum Haushalt gehörenden Mitbenutzer des Anschlusses darüber informiert hat und künftige Mitbenutzer unverzüglich darüber informieren wird, dass ihm die Verkehrsdaten zur Erteilung des Nachweises bekannt gegeben werden.

Bei Anschlüssen in Betrieben und Behörden ist die Mitteilung nur zulässig, wenn der Teilnehmer in Textform erklärt hat, dass die Mitarbeiter informiert worden sind und künftige Mitarbeiter unverzüglich informiert werden und dass der Betriebsrat oder die Personalvertretung entsprechend den gesetzlichen Vorschriften beteiligt worden ist oder eine solche Beteiligung nicht erforderlich ist. [...]“

Nicht ganz neu: vgl. WhatsApp-Nutzungsbedingungen

„Adressbuch. Du stellst uns regelmäßig die Telefonnummern von WhatsApp-Nutzern und deinen sonstigen Kontakten in deinem Mobiltelefon-Adressbuch zur Verfügung. Du bestätigst, dass du autorisiert bist, uns solche Telefonnummern zur Verfügung zu stellen, damit wir unsere Dienste anbieten können.“

WhatsApp

https://www.whatsapp.com/legal/?l=de#terms-of-service

Nicht nur Datenabfluss kritisch, auch Fernbeeinflussung

Terrified driver almost crashes car when loan company hit 'kill switch' for missing repayments

Mirror

18:11, 26 SEP 2014 | UPDATED 18:35, 26 SEP 2014 | BY CHRISTOPHER BUCKTIN

Heartless creditors LOCKED T. Candice Smith's steering wheel and stopped her engine as she drove down a busy Las Vegas highway

Scared: T. Candice Smith

A terrified driver nearly crashed her car when it suddenly shut down on a motorway - only to find her LOAN COMPANY had used a remote kill switch after she missed a payment.

T. Candice Smith was driving with her friend down a three-lane Las Vegas interstate when her steering wheel began to lock up.

The car's engine then stopped causing the vehicle to come to a stop.

„used a remote kill switch after she missed a payment”

http://www.mirror.co.uk/news/technology-science/terrified-driver-crashes-car-loan-4325955

Nicht nur Datenabfluss kritisch, auch Fernbeeinflussung

The Register®
Biting the hand that feeds IT

Business ▸ Government

I want to remotely disable Londoners' cars, says Met's top cop

Psst, chief. You've probably not heard of backdoors – this is a seriously bad idea

A Met Police helmet. Pic: Shutterstock

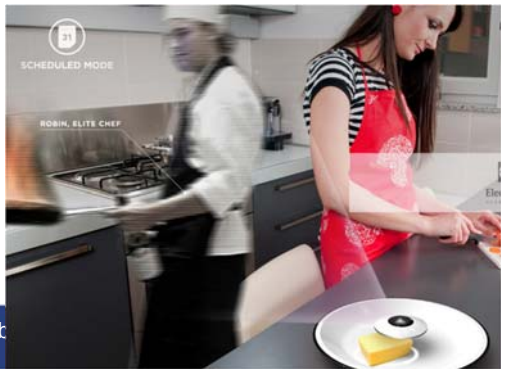
22 Sep 2016 at 15:04, Gareth Corfield

Metropolitan Police commissioner Sir Bernard Hogan-Howe wants the capital's cops to be able to remotely disable people's cars, he told the London Assembly's police and crime committee today.

http://www.theregister.co.uk/2016/09/22/met_police_commissioner_i_want_remotely_kill_car_electronics/

„remotely disable people's cars"

Smart Home: HCI neu denken – auch für Datenschutz?



CC BY NC Bilder: Electrolux Design Lab

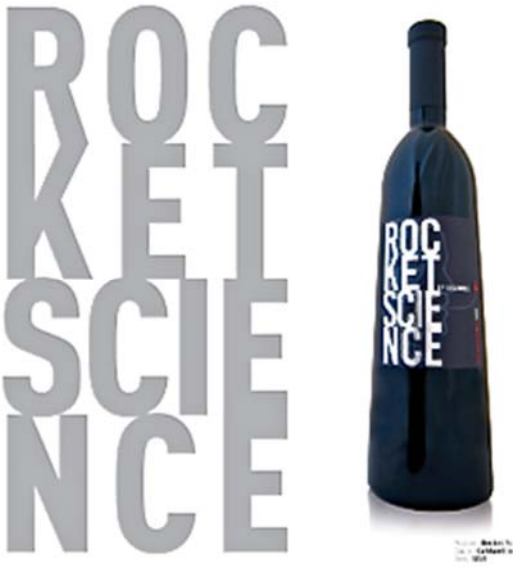
Pflicht zur Verringerung der Komplexität? – „historisch gewachsen“

Bild: Rohit Mattoo

It‘s no rocket science. Is it?

Anmerkung: Komplexitätsminimierung in Rocket Science angestrebt

Bild: Steve Jurvetson



Fortschritt hat andere Prioritäten

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE SCIENCE BOOTNOTES FORUMS

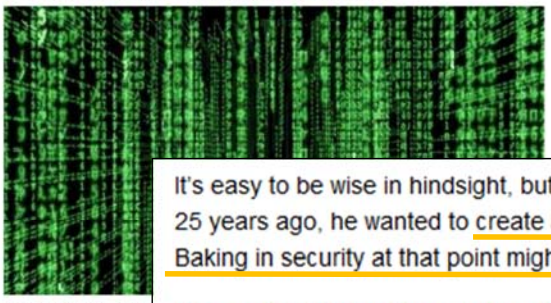
Security

Sir Tim Berners-Lee defends decision not to bake security into www

'The idea that privacy is dead is hopelessly sad'

More like this

Tim Berners-Lee



8 Oct 2014 at 12:24, John L

IP Expo Sir Tim Berners-Lee
wide web.

It's easy to be wise in hindsig
25 years ago, he wanted to
Baking in security at that po

"[*The web*] might not have ta
this morning.

Sir Tim's views are in contras
regretted not building in sec
current push towards always
more to do with timing and priorities than principles.

During a keynote presentation at the infrastructure conference, Sir Tim discussed a vision for the web where users are more in control of managing their privacy.

"The idea that privacy is dead is hopelessly sad," Sir Tim Berners-Lee said. "We have to build systems that allow for privacy."

It's easy to be wise in hindsight, but Sir Tim explained that at the point he invented the world wide web 25 years ago, he wanted to create a platform that developers would find familiar and easy to use. Baking in security at that point might have worked against that goal, he said.

"[*The web*] might not have taken off if it had been too difficult," he told an audience at IPExpo Europe this morning.

Sir Tim's views are in contrast with those of another internet pioneer, Vint Cerf, who recently said he regretted not building in security to basic internet protocols. Berners-Lee strongly supported the current push towards always-on crypto (https) for websites now underway, so his differing views are more to do with timing and priorities than principles.

„timing and priorities" – Sicherheit (und DS) als nachrangig eingestuft

http://www.theregister.co.uk/2014/10/08/sir_tim_bernerslee_defends_decision_not_to_bake_security_into_www/

Verständnis durch Reverse Engineering?

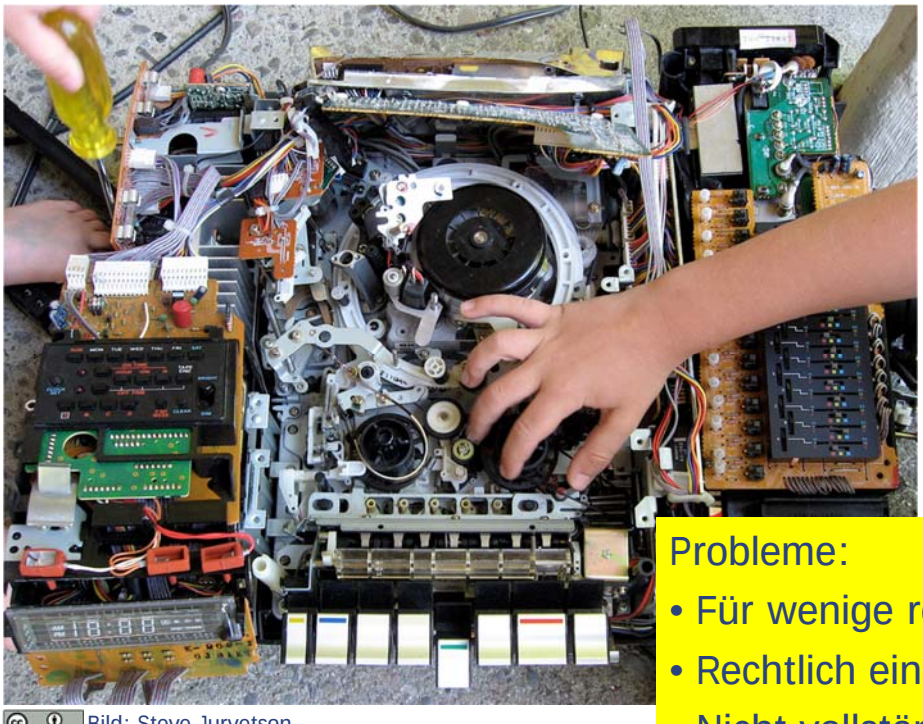


Bild: Steve Jurvetson

Probleme:

- Für wenige realistisch
- Rechtlich eingeschränkt
- Nicht vollständig verstehbar (Bsp. „gezinkte Primzahlen")

Algorithmen-Kontrolle

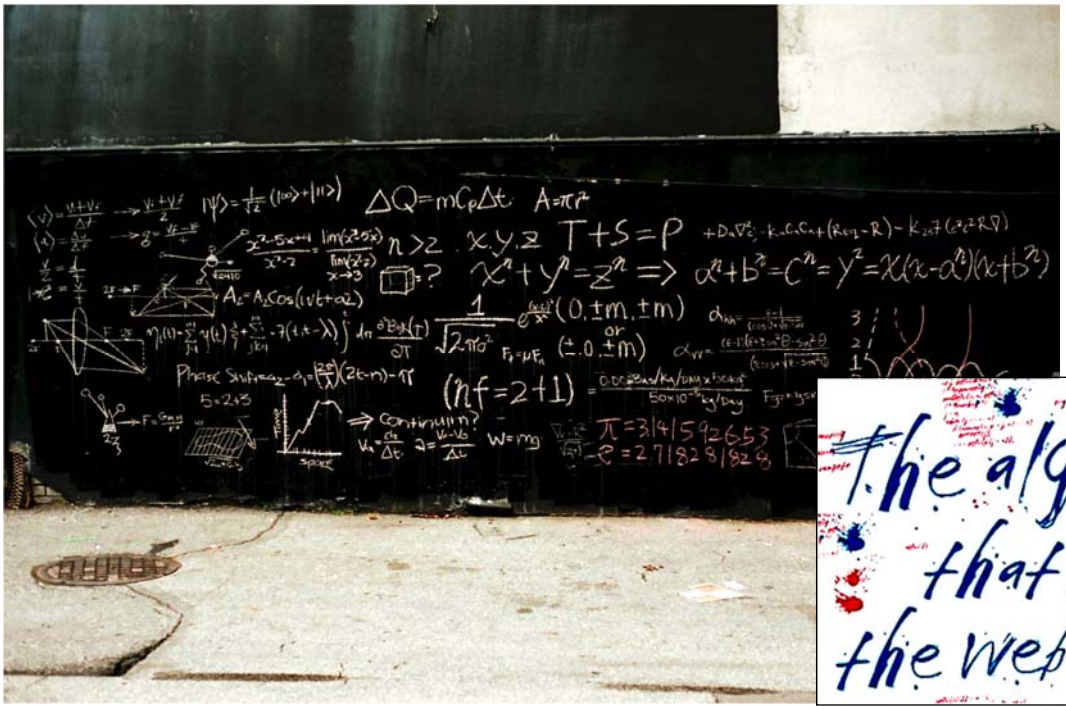


Bild: Byron Barrett

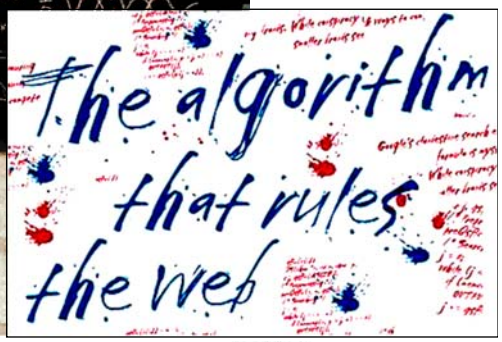


Bild: ApolitikNow

„Kaste von Experten“: Algorithmiker

Mayer-Schönberger: Die Gesellschaft muss politisch sicherstellen und in Gesetzen festlegen: In der Verwaltungs- und Strafgerichtsbarkeit dürfen solche Prognosen nicht verwendet werden, um über Schuld oder Unschuld zu entscheiden. Für andere wichtige Entscheidungen, also ob ein Kredit gewährt wird oder eine Operation stattfindet, muss der Algorithmus, der Risikovorhersagen berechnet, von einem Experten einsehbar sein. Die Faktoren, die in die Berechnung der Prognose einfließen, müssen transparent sein, und es muss Regeln geben, wie der Betroffene das Ergebnis widerlegen kann.

ZEIT: Woher sollen die von Ihnen geforderten Experten kommen?

Mayer-Schönberger: Wir glauben, dass sich eine eigene Kaste von Experten entwickeln wird, die Algorithmiker.

ZEIT: Wie Wirtschaftsprüfer für die Bilanz?

Mayer-Schönberger: Genau, sie müssen das Wissen über das Design von Algorithmen haben und sich dann einen spezifischen Algorithmus ansehen.

ZEIT: Sie fordern also eine Art Algorithmus-TÜV.

Mayer-Schönberger: Genau.

Bild: CyberHades

„Open Source“ reicht nicht

http://www.zeit.de/2013/09/Internet-Tuev-Viktor-Mayer-Schoenberger-Big-Data/

HEILSBRINGER DATENSCHUTZ-GRUNDVERORDNUNG?

Prinzipien der Europäischen Datenschutz-Grundverordnung

- Marktortprinzip (Art. 3 – d.h. auch für außereuropäische Player mit DV in der EU)
- Signifikante Sanktionen (Art. 83, 84)

Ziel: Schutz der Rechte und Freiheiten natürlicher Personen

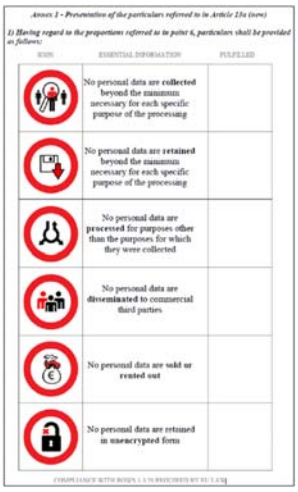
- Insbesondere:
  - Adäquater Umgang mit Risiken (Art. 24, 25, 32, 35, 36)
  - Datenschutz durch Technikgestaltung (Art. 25; Sicherheit: Art. 32)
  - Datenschutz durch datenschutzfreundliche Voreinstellungen (Art. 25)
  - Transparenz für die betroffenen Personen (Art. 5, 12-15, 19, 22, 30, 33)
  - Intervenierbarkeit für die betroffenen Personen (Art. 5, 7, 8, 16-18, 20, 21)
  - Verantwortung des für die Verarbeitung Verantwortlichen (Art. 6 II, 24)
- Adressat: Datenverarbeiter
  (Betreiber, Auftragnehmer, u.U. auch Privatpersonen; nicht unmittelbar Hersteller)

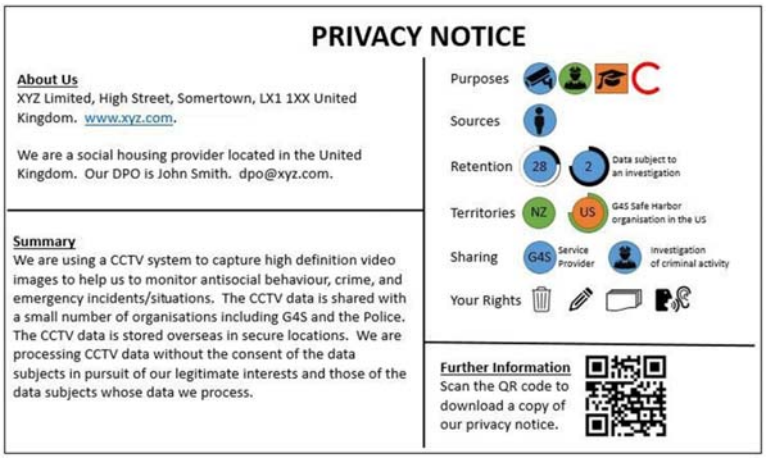
Transparenz: Verständlichkeit der Datenverarbeitung

- Eigentlich Grundsatz der fairen und transparenten Datenverarbeitung in DS-GVO
- Aber Ausnahmen möglich: im Ermessen des Verantwortlichen keine Information der betroffenen Personen, wenn „die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde“ (Art. 14 Abs. 5 lit. b DS-GVO)
  - Big Data?
  - Ubiquitous Computing?
- Und wenn Information: wie?

Vorschläge für mehr Transparenz

- Klare und einfache Sprache
- „Layered Policies“: Aufbau in mehreren Ebenen
- Standardisierte Bildsymbole (Art. 12 Abs. 7 DS-GVO)
- Maschinenlesbar

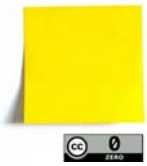




Quelle: http://www.dataprotectionpeople.com/5918-2/ (Januar 2016)

Vorschläge für Unterstützung der Selbstbestimmung

- Datensparsamkeit und Privacy by Design als Grundprinzip
  [stark unter Beschuss von Politik und Wirtschaft, Gegenbegriffe: Datenreichtum, Datensouveränität]
- Binden der akzeptierten Verarbeitungsregeln an die Daten (z.B. Sticky Policies) [Seiteneffekte beachten!]



- Assistenten Technik/Menschen/Organisationen
  [Vertrauensmodell!]
- Adäquate HCI

Bild: Andy Newsam

Datenschutz „by Design“ & „by Default“

- Anforderung aus Art. 25 EU-Datenschutz-Grundverordnung
- Richtet sich primär an: Datenverarbeiter (auch im Auftrag) + (nur indirekt!) Hersteller von IT-Systemen
- Ziel: Gestaltung von Systemen + Diensten
  von Anfang an über den gesamten Lebenszyklus
  a) datensparsam
  b) mit möglichst datenschutzfreundlichen Voreinstellungen

Datenschutz „by Default“ in der DS-GVO: Art. 25

Ohnehin schon im Erforderlichkeitsprinzip (Artikel 5)

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

Bsp.: Social Networks

Datenschutz „by Design“ & „by Default“ gemäß Erwägungsgrund 78 DS-GVO

- Nachweis durch interne Strategien & t+o Maßnahmen, u.a.
  - Datenminimierung
  - Schnellstmögliche Pseudonymisierung
  - Transparenz in Bezug auf Funktionen+Verarbeitung
  - Ermöglichung der Überwachung der Verarbeitung durch die betroffenen Personen
  - Ermöglichung für Sicherheitsfunktionen „on top“ durch Verantwortlichen

(78) Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun. Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte auch bei öffentlichen Ausschreibungen Rechnung getragen werden.

- Ermutigung für Hersteller
- Berücksichtigung in öffentlichen Ausschreibungen

Zusätzlich zu Datenschutz: Verbraucherschutz

Anforderung an eine gültige Einwilligung nach Datenschutzrecht:

- bewusst,
- informiert und
- freiwillig.

Wie viel den betroffenen Personen zumuten?

Eine AGB-Vertragsklausel kann eingeschränkt gültig oder unwirksam sein, weil

- die AGB-Bestimmung unklar ist,
- die AGB-Bestimmung überraschend ist oder
- die AGB-Bestimmung den Kunden unangemessen benachteiligt.

Bilder: Daniel Lobo

Bild: SIDwms

FAZIT

Fazit 1/2

- Informationelle Selbstbestimmung:
  - Schon immer mehr Ziel als Realität
  - Bei versteckter Informationstechnik Einzelfall-Selbstbestimmung nicht möglich
  - Feingranulare Abfragen oder Konfigurationen: zeitintensiv und anspruchsvoll, für die meisten unzumutbar
  - Vergleich Organspende / Patientenverfügung

- Aber Garantien durch eingebauten Datenschutz möglich
  - Privacy by design & by default
  - „by default“: nur Startpunkt – und dann?
  - „One size fits all“ in vielen Bereichen nicht realistisch

Fazit 2/2

- Realität der heutigen Informationstechnik und Informationsgesellschaft dermaßen weit weg vom Datenschutz-Optimum
  ... und sogar vom Akzeptablen

- Lösungen müssen sichtbarer werden
  - Für Hersteller, Betreiber, Nutzer und Datenschutzbehörden
  - Über die Community-Grenzen hinaus
  - Diskussion von Seiteneffekten & Technikfolgen nötig
  - Call for help!

- Datenschützer müssen sichtbarer werden

Vielen Dank für die Aufmerksamkeit!

Marit Hansen
https://www.datenschutzzentrum.de/

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein