Privacy and data protection by design – cross-over of multiple disciplines

Marit Hansen
Privacy and Information Commissioner
Schleswig-Holstein, Germany

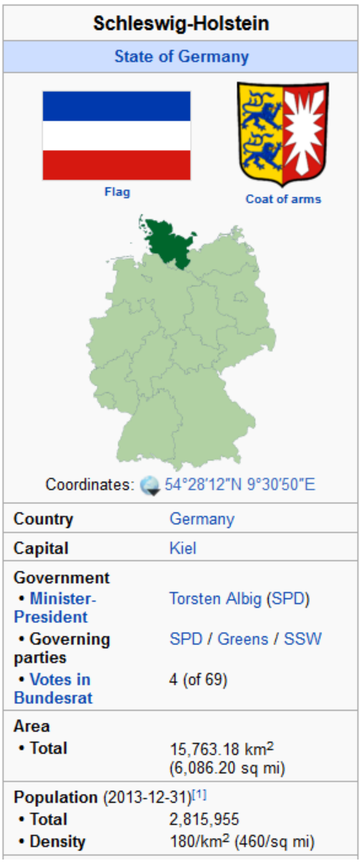
marit.hansen@datenschutzzentrum.de

Annual Privacy Forum 2015
Luxembourg, 7 October, 2015

ipen
forum privatheit selbstbestimmtes_leben_in_der_digitalen_welt
ABC4TRUST
FutureID
ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Setting of ULD

- Data Protection Authority (DPA) for both the public and private sector
- Also responsible for freedom of information



Schleswig-Holstein

State of Germany

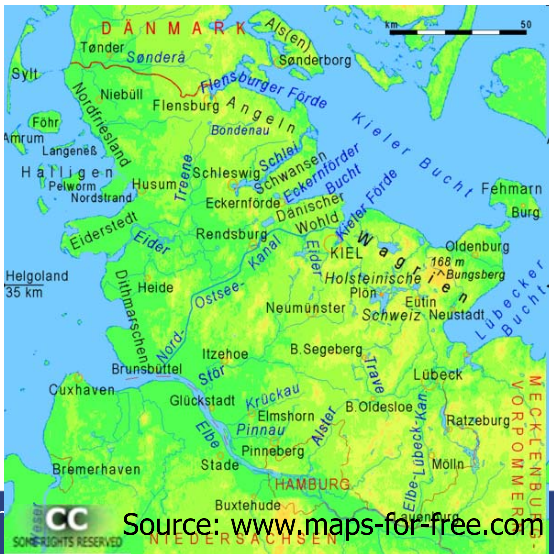
Flag

Coat of arms

Coordinates: 54°28′12″N 9°30′50″E

Country	Germany
Capital	Kiel
Government	
• Minister-President	Torsten Albig (SPD)
• Governing parties	SPD / Greens / SSW
• Votes in Bundesrat	4 (of 69)
Area	
• Total	15,763.18 km^2 (6,086.20 sq mi)
Population (2013-12-31)[1]	
• Total	2,815,955
• Density	180/km^2 (460/sq mi)

Source: en.wikipedia.org/ wiki/Schleswig-Holstein



Source: www.maps-for-free.com

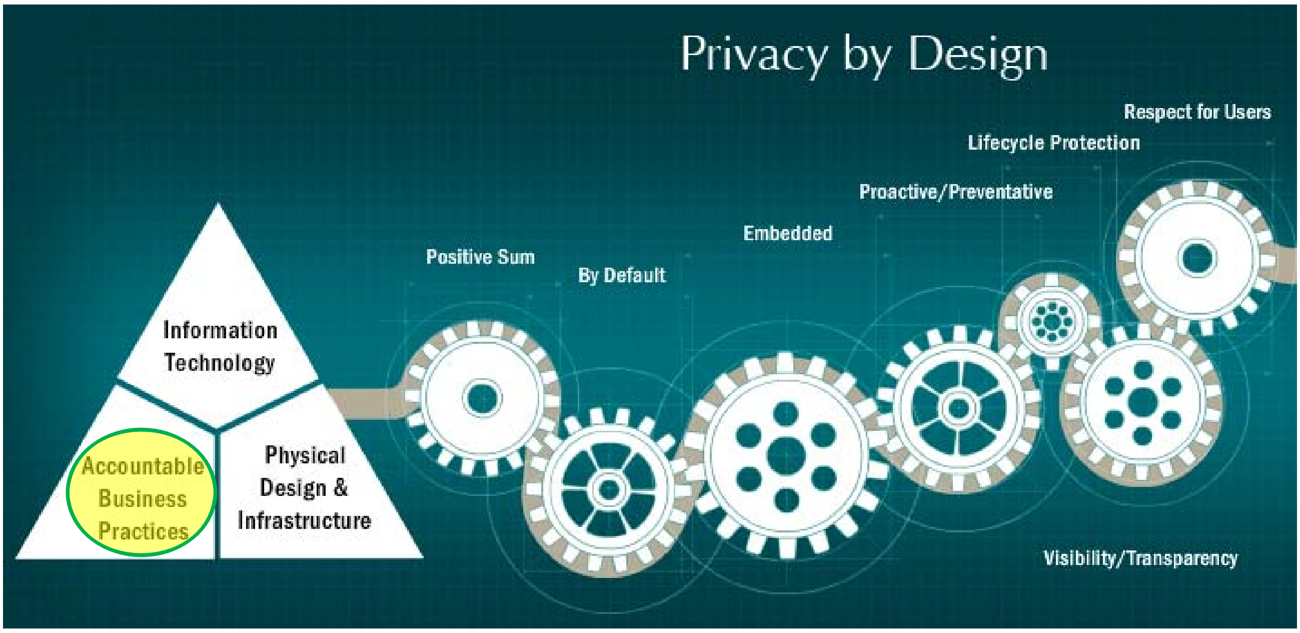
Overview

1. Privacy and Data Protection by Design
2. A motivated approach of all relevant disciplines
3. Beware of obstacles
4. Conclusion

1. Privacy and Data Protection by Design

Source: Colin Kinner

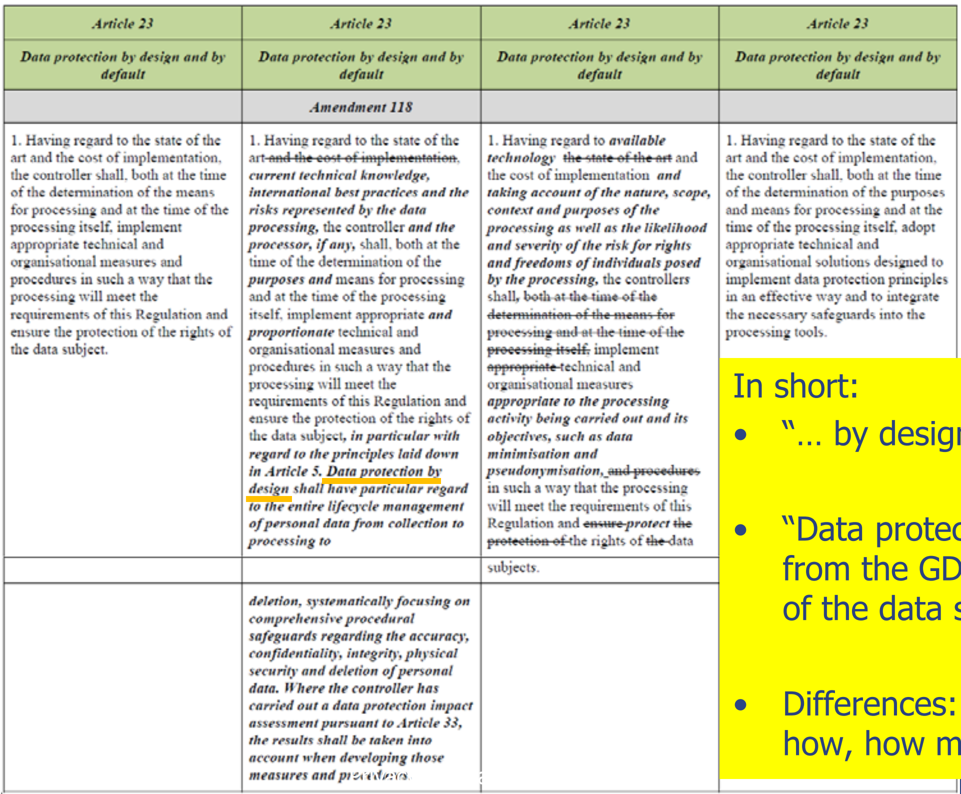
Cavoukian's Privacy by Design



http://privacybydesign.ca/

Privacy & data protection by design – cross-over of disciplines

General Data Protection Regulation (GDPR) Art. 23 (1) – Discussion

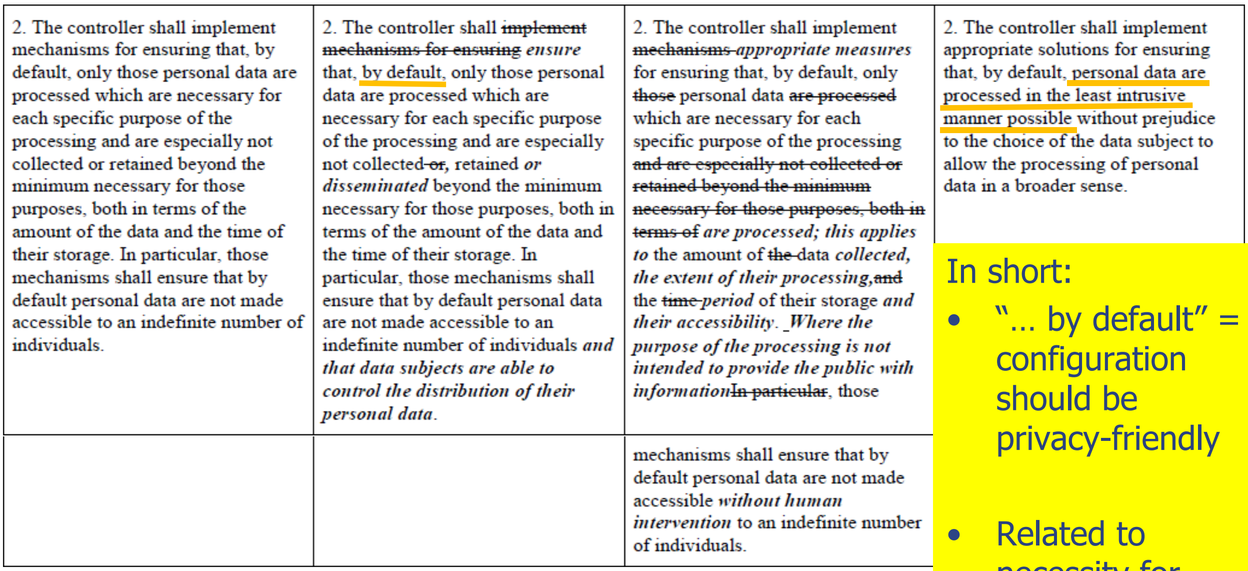


Article 23	*Article 23*	*Article 23*	*Article 23*
Data protection by design and by default	***Data protection by design and by default***	***Data protection by design and by default***	***Data protection by design and by default***
	Amendment 118		
1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.	1. Having regard to the state of the art ~~and the cost of implementation~~, ***current technical knowledge, international best practices and the risks represented by the data processing,*** the controller ***and the processor, if any,*** shall, both at the time of the determination of the ***purposes and*** means for processing and at the time of the processing itself, implement appropriate ***and proportionate*** technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, ***in particular with regard to the principles laid down in Article 5. Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to***	1. Having regard to ***available technology*** ~~the state of the art~~ and the cost of implementation ***and taking account of the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for rights and freedoms of individuals posed by the processing,*** the controllers shall, ~~both at the time of the determination of the means for processing and at the time of the processing itself,~~ implement ~~appropriate~~ technical and organisational measures ***appropriate to the processing activity being carried out and its objectives, such as data minimisation and pseudonymisation,*** ~~and procedures~~ in such a way that the processing will meet the requirements of this Regulation and ~~ensure~~ ***protect*** ~~the protection of~~ the rights of ~~the~~ data	1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the purposes and means for processing and at the time of the processing itself, adopt appropriate technical and organisational solutions designed to implement data protection principles in an effective way and to integrate the necessary safeguards into the processing tools.
		subjects.	
	deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data. Where the controller has carried out a data protection impact assessment pursuant to Article 33, the results shall be taken into account when developing those measures and procedures		

In short:

- "… by design" = built-in
- "Data protection" = reqs from the GDPR, esp. rights of the data subject
- Differences: who, when, how, how much?

General Data Protection Regulation (GDPR)
Art. 23 (2) – Discussion

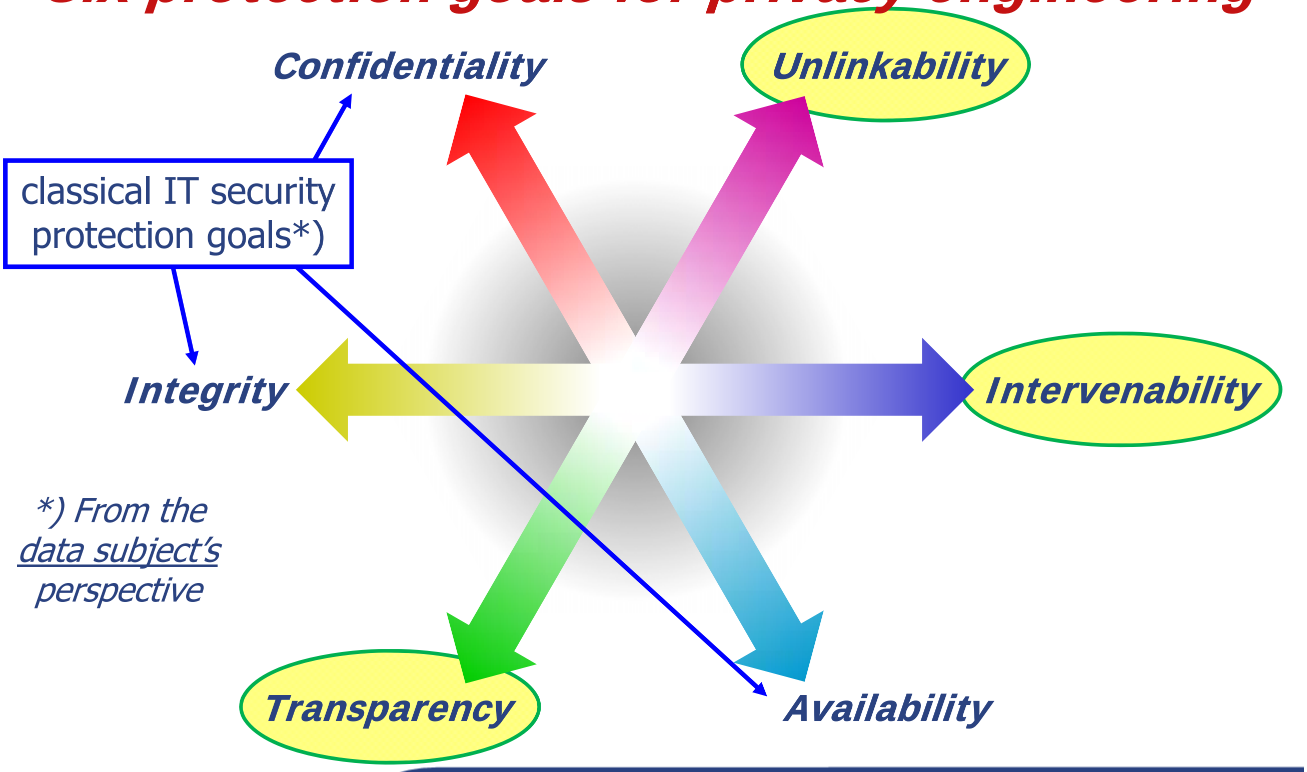


European Commission	1st reading position of the European Parliament	General Approach of the Council	EDPS recommendations
2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.	2. The controller shall ~~implement mechanisms for ensuring~~ *ensure* that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected ~~or~~, retained *or disseminated* beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals *and that data subjects are able to control the distribution of their personal data*.	2. The controller shall implement ~~mechanisms~~ *appropriate measures* for ensuring that, by default, only ~~those~~ personal data ~~are processed~~ which are necessary for each specific purpose of the processing ~~and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of~~ *are processed; this applies to* the amount of ~~the~~ data *collected, the extent of their processing*,~~and~~ the ~~time~~ *period* of their storage *and their accessibility. _Where the purpose of the processing is not intended to provide the public with information*~~In particular~~, those	2. The controller shall implement appropriate solutions for ensuring that, by default, personal data are processed in the least intrusive manner possible without prejudice to the choice of the data subject to allow the processing of personal data in a broader sense.
		mechanisms shall ensure that by default personal data are not made accessible *without human intervention* to an indefinite number of individuals.	

In short:

- "… by default" = configuration should be privacy-friendly
- Related to necessity for purpose

Six protection goals for privacy engineering



Confidentiality

Unlinkability

classical IT security protection goals*)

Integrity

Intervenability

Transparency

Availability

*) From the <u>data subject's</u> perspective

Protection Goals for Privacy Engineering

Confidentiality
Unlinkability
Integrity
Intervenability
Transparency
Availability

Protection goal "unlinkability"

The protection goal of

Unlinkability

is defined as the property that
privacy-relevant data cannot be linked
across domains that are constituted by
a common purpose and context.

Reference: Hansen/Jensen/Rost: Protection Goals for Privacy Engineering, Proc. 1st International Workshop on Privacy Engineering, IEEE, 2015

Protection Goals for Privacy Engineering

Confidentiality
Unlinkability
Integrity
Intervenability
Transparency
Availability

Protection goal "transparency"

The protection goal of

Transparency

is defined as the property that
all privacy-relevant data processing
– including the legal, technical,
and organisational setting –
can be understood and reconstructed at any time.

Reference: Hansen/Jensen/Rost: Protection Goals for Privacy Engineering, Proc. 1st International Workshop on Privacy Engineering, IEEE, 2015

Protection goal "intervenability"

Protection Goals for Privacy Engineering

Confidentiality
Unlinkability
Integrity
Intervenability
Transparency
Availability

The protection goal of

Intervenability

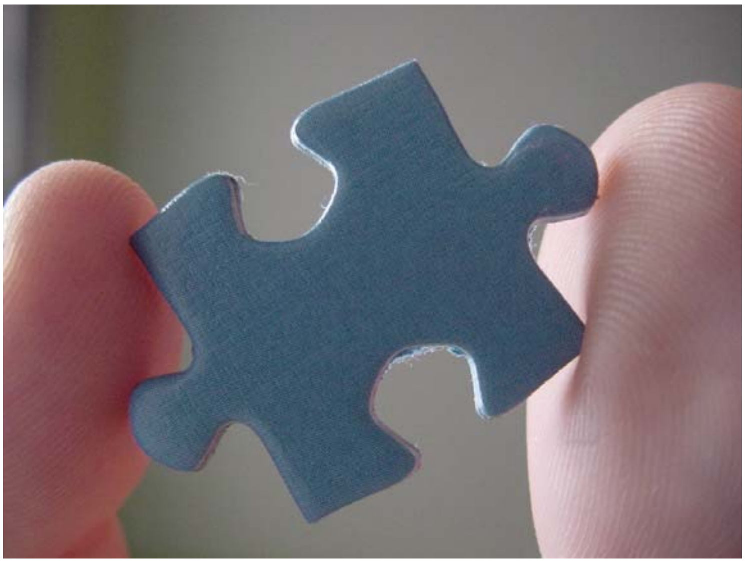
is defined as the property that intervention is possible concerning all ongoing or planned privacy-relevant data processing.

Reference: Hansen/Jensen/Rost: Protection Goals for Privacy Engineering, Proc. 1st International Workshop on Privacy Engineering, IEEE, 2015

Protection goals need multiple disciplines – in particular intervenability

- Intervenability is not prominent in privacy engineering literature
- Reasons for that:
  - Hard to formalise and to measure
  - Compared with data minimisation research far less proposed techniques and technologies
  - Can often not be solved within the IT system alone
  - Needs a running system with clear responsibilities (operator, users) – not on prototype level
  - Not one fixed solution, but process-oriented, taking into account the full lifecycle of system evolution

2. A motivated approach of all relevant disciplines – the ideal scenario



Source: Olga Berrios

Puzzle metaphor

Privacy by Design

- Means involvement of all relevant stakeholders for putting together the puzzle
- Including representatives from
  - The application context
  - Technology / computer science / soft-/hardware engineering
  - (Data protection) law
  - Business studies
  - Psychology
  - Social sciences
  - Ethics …

Source: rama_miguel

Puzzle metaphor

Source: Olga Berrios

- Think of a puzzle
- The colours represent various disciplines
- The pieces are the methods/tools/ instruments for Privacy by Design

Multiple disciplines necessary

Source: Ken Teegardin

- Law: lawfulness
- Technology: engineering
- Economy:
  - Organisational processes
  - Business models
- Psychology++: user interaction, organisational culture
- Ethics & social / political sciences …

How it could work

Effects for data subjects?
Effects for society?

Lawfulness?

Source: Kevin Dooley

- Starting point: task to implement
- ⇨ Purpose
- Which information is necessary?
- How to gather & process the necessary data?
- Protection level “normal” / “high” / “very high”? *Risks?*
- Consider the protection goals; perspective: data subject
- Choice of measures from “PbD repository”
- Evaluate ⇗

Nice idea: “PbD repository”

Source: Olga Berrios

But not that easy:

- Dependencies and interrelations
- Side effects
- Usually no naïve plug & play possible

Current status:

- Some attempts
- Not well sorted
- Not well understood

Especially lack of cross-disciplinary understanding!

How to integrate privacy modules

🅭 🅯 Source: Horia Varlan

the same idea of

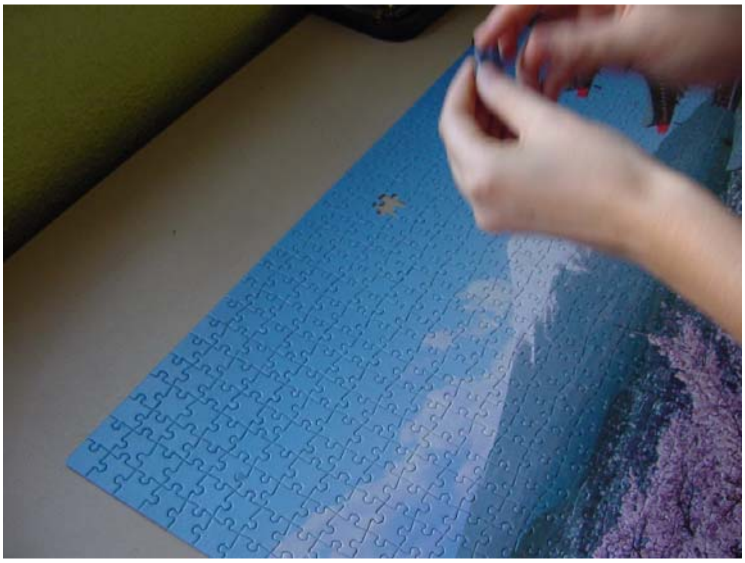
Legacy systems that are not designed with privacy in mind

- Technology, e.g. architectures, infrastructures
- Business processes
- Law …

Building in privacy may be difficult / impossible!

Whose task?

If everything works out



🅭 🅯 Source: Olga Berrios

However, the puzzle comparison is flawed:

- Several solutions, several pictures
- Not using all pieces
- You may not notice quickly if something goes wrong

"Understanding is an illusion"

AUTO ALLIANCE
DRIVING INNOVATION®

Data minimisation:
"… necessary for legitimate business purposes …"

Source: Horia Varlan

Obstacles:

- Different vocabulary
  - Even hijacked vocab
- Inherent logic of each discipline
  - Binary or fuzzy?
  - Solution-oriented?
- Still learning from non-understanding is possible

Data Protection by Design is about ~~data~~

Source: Ashtyn Renee

human beings with their rights

3. Beware of obstacles – the careless dark? real-life scenario

Source: The U.S. Army

Challenge 1: Storage by default

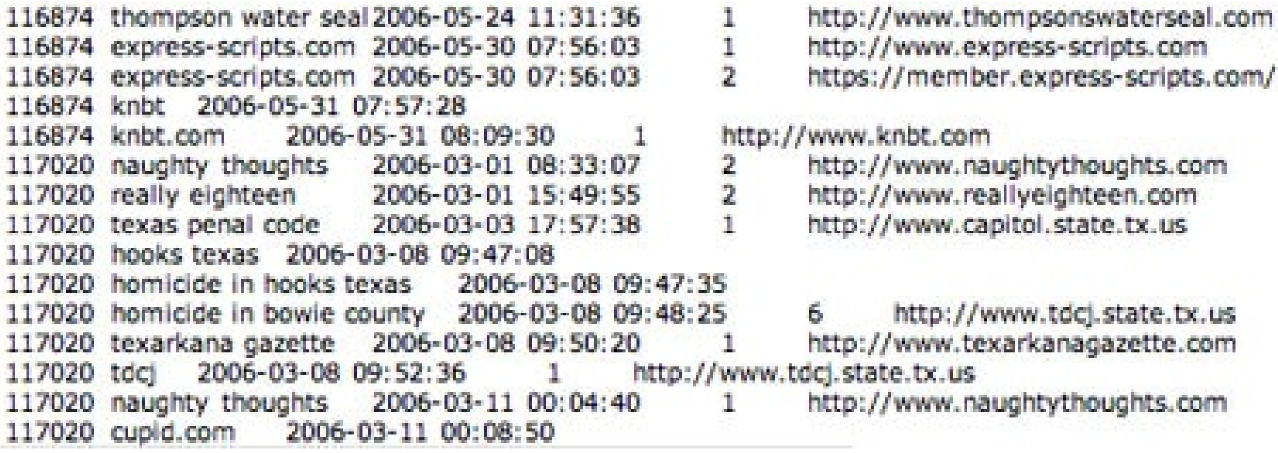
- **Statements often heard:**
  - "For functionality tests or debugging, we need data, much data."
  - "You never know when you are going to need it."

- **Problem:** if erasure, often no real erasure
- **Problem:** logfiles+temporary files are often not taken into account – even in privacy assessment

Challenge 2a: Linkability by default

- **Principle in IT:**
  - Keep accurate data
  - Avoidance of redundancies in databases
  - Naïve approach: central world-wide database of all subjects/objects + access control / different views
- **Problem:** difficult for desired separation of powers (and separation of purposes) ⇒ risk
- **Problem:** real life

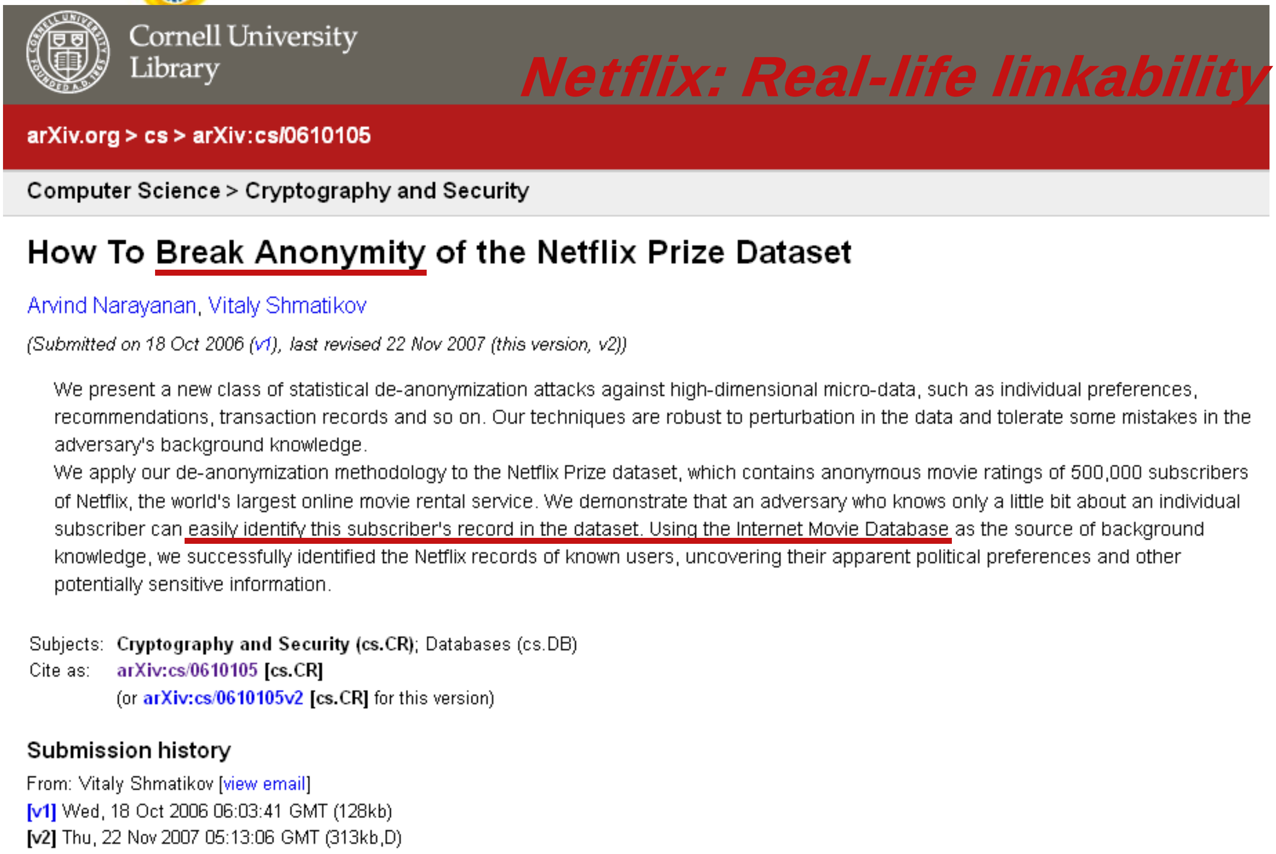
Example: 2006: AOL publishes ~~anonymised~~ pseudonymised search engine requests of 3 months



```
116874  thompson water seal 2006-05-24 11:31:36      1      http://www.thompsonswaterseal.com
116874  express-scripts.com  2006-05-30 07:56:03      1      http://www.express-scripts.com
116874  express-scripts.com  2006-05-30 07:56:03      2      https://member.express-scripts.com/
116874  knbt    2006-05-31 07:57:28
116874  knbt.com      2006-05-31 08:09:30      1      http://www.knbt.com
117020  naughty thoughts     2006-03-01 08:33:07      2      http://www.naughtythoughts.com
117020  really eighteen      2006-03-01 15:49:55      2      http://www.reallyeighteen.com
117020  texas penal code     2006-03-03 17:57:38      1      http://www.capitol.state.tx.us
117020  hooks texas   2006-03-08 09:47:08
117020  homicide in hooks texas     2006-03-08 09:47:35
117020  homicide in bowie county    2006-03-08 09:48:25      6      http://www.tdcj.state.tx.us
117020  texarkana gazette    2006-03-08 09:50:20      1      http://www.texarkanagazette.com
117020  tdcj    2006-03-08 09:52:36      1      http://www.tdcj.state.tx.us
117020  naughty thoughts     2006-03-11 00:04:40      1      http://www.naughtythoughts.com
117020  cupid.com     2006-03-11 00:08:50
```

Quelle: http://www.lunchoverip.com/2006/08/being_user_4417.html

Netflix: Real-life linkability



arXiv.org > cs > arXiv:cs/0610105

Computer Science > Cryptography and Security

How To Break Anonymity of the Netflix Prize Dataset

Arvind Narayanan, Vitaly Shmatikov

(Submitted on 18 Oct 2006 (v1), last revised 22 Nov 2007 (this version, v2))

We present a new class of statistical de-anonymization attacks against high-dimensional micro-data, such as individual preferences, recommendations, transaction records and so on. Our techniques are robust to perturbation in the data and tolerate some mistakes in the adversary's background knowledge.

We apply our de-anonymization methodology to the Netflix Prize dataset, which contains anonymous movie ratings of 500,000 subscribers of Netflix, the world's largest online movie rental service. We demonstrate that an adversary who knows only a little bit about an individual subscriber can easily identify this subscriber's record in the dataset. Using the Internet Movie Database as the source of background knowledge, we successfully identified the Netflix records of known users, uncovering their apparent political preferences and other potentially sensitive information.

Subjects:	**Cryptography and Security (cs.CR)**; Databases (cs.DB)
Cite as:	arXiv:cs/0610105 [cs.CR]
	(or arXiv:cs/0610105v2 [cs.CR] for this version)

Submission history

From: Vitaly Shmatikov [view email]

[v1] Wed, 18 Oct 2006 06:03:41 GMT (128kb)

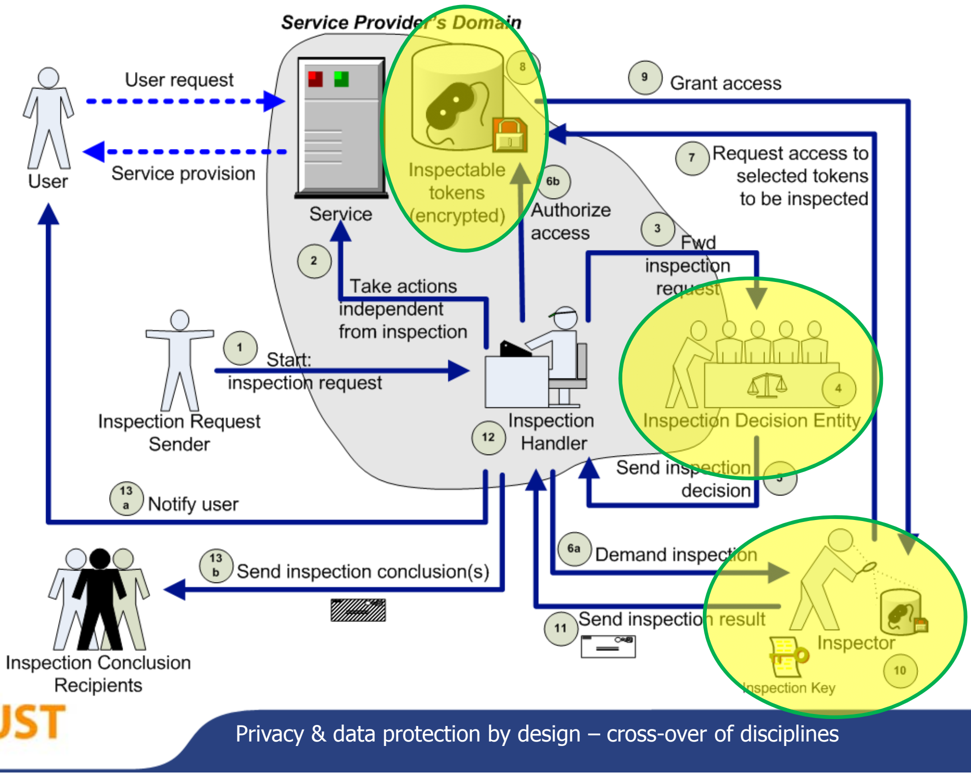
[v2] Thu, 22 Nov 2007 05:13:06 GMT (313kb,D)

Challenge 2b: Unlinkability is difficult

- **Problem:** unlinkability often means more effort, more complexity
- **Problem:** unlinkability by involving additional parties raises questions on the responsibility / liability / accountability for the data processing
  - Joint controllership?
  - Contractual relations?
  - Who is to be addressed …
    - … by users?
    - … by supervisory authorities?
    - … by police / law enforcement?

Solvable!
But at best answers to be provided together with the privacy technology.

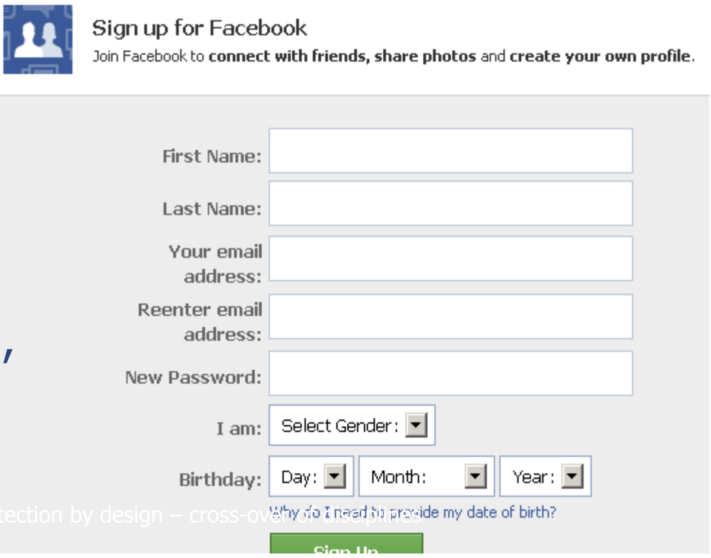
Example Privacy-ABCs: process for exceptionally revealing identity information needing multiple parties


Service Provider's Domain
User
User request
Service provision
Service
Inspectable tokens (encrypted)
8
9 Grant access
7 Request access to selected tokens to be inspected
6b Authorize access
3 Fwd inspection request
2 Take actions independent from inspection
1 Start: inspection request
Inspection Request Sender
12 Inspection Handler
Inspection Decision Entity
4
5 Send inspection decision
13a Notify user
13b Send inspection conclusion(s)
6a Demand inspection
11 Send inspection result
Inspector
10
Inspection Key
Inspection Conclusion Recipients

ABC4TRUST

Challenge 3: Real identity information by default

- **Tradition:**
  Real name – long-established tradition in many cultures: "Whoever doesn't say his/her name, is suspicious"
- **Psychology / business:** form of address in customer contact
- **Problem:** Even if pseudonyms are accepted, database design with first name / last name


Sign up for Facebook

Join Facebook to **connect with friends, share photos** and **create your own profile.**

First Name:

Last Name:

Your email address:

Reenter email address:

New Password:

I am: Select Gender:

Birthday: Day: Month: Year:

Why do I need to provide my date of birth?

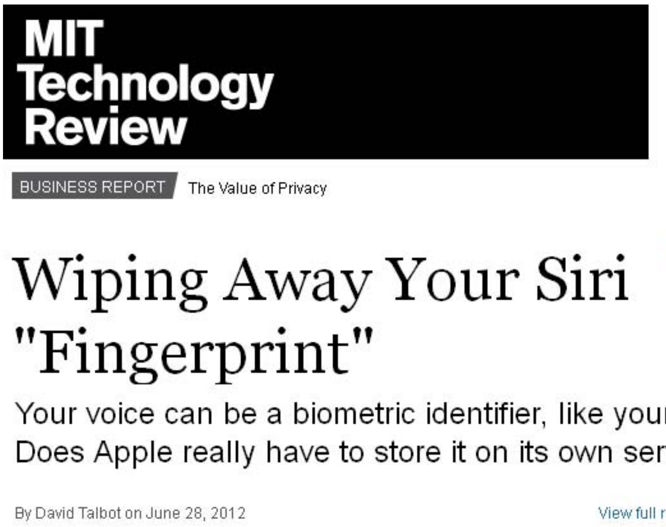
Challenge 3: Real identity information by default

- **Real identity:**
  also in biometrics-related applications

- E.g. in social networks:
  - Photos of oneself or others
  - (Today predominantly self-claimed) height, weight, mood …

- E.g. in speech assistance systems:
  - Voice

Siri: iPhone speech assistance in the iCloud



MIT Technology Review

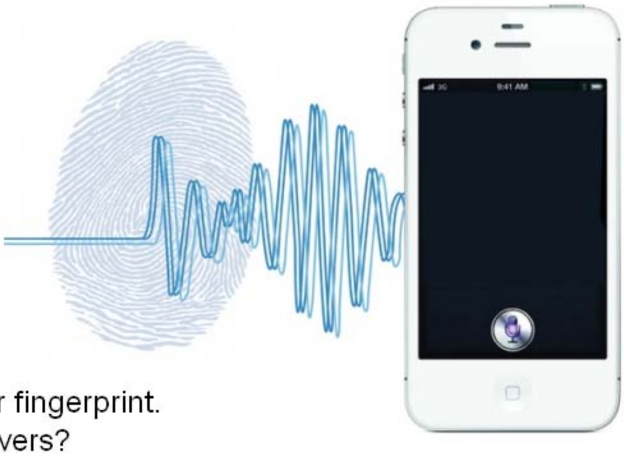
BUSINESS REPORT The Value of Privacy

Wiping Away Your Siri "Fingerprint"

Your voice can be a biometric identifier, like your fingerprint. Does Apple really have to store it on its own servers?

By David Talbot on June 28, 2012

View full report ➜ Download ⬇



http://www.technologyreview.com/news/428053/wiping-away-your-siri-fingerprint/

Voice biometrics in the iCloud

"Trudy Muller, an Apple spokeswoman, confirmed that voice recordings are stored when users ask a spoken question like 'What's the weather now?'

'This data is only used for Siri's operation and to help Siri improve its understanding and recognition,' she said.

Muller added that the company takes privacy 'very seriously,' noting that questions and responses that Siri sends over the Internet are encrypted, and that recordings of your voice are not linked to other information Apple has generated about you.

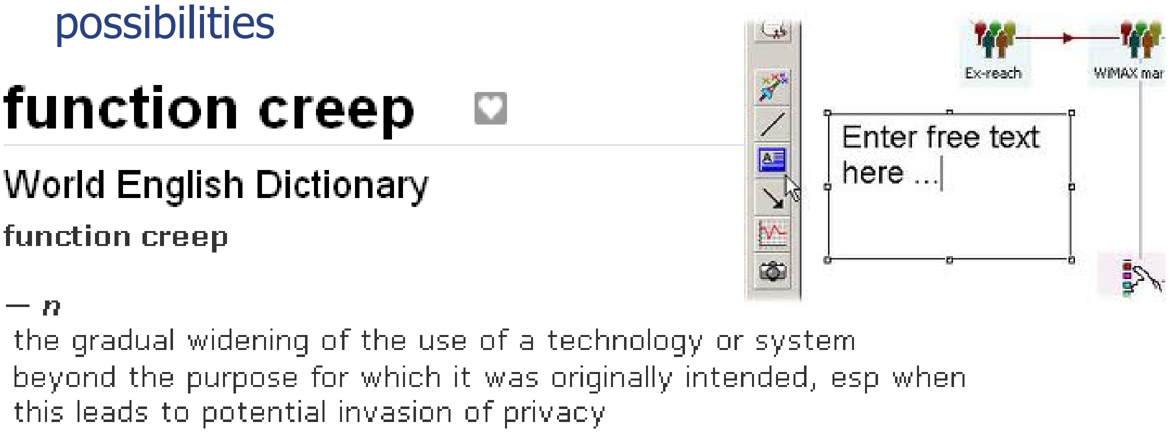
(Siri does upload your contact list, location, and list of stored songs, though, to help it respond to your requests.)"

http://www.technologyreview.com/news/428053/wiping-away-your-siri-fingerprint/

Challenge 4: Function creep as feature

- **Principle in IT:**
  - Re-use of applications (multi-purpose)
  - Naïve approach: digitising everything, context-spanning identifiers, interoperability, openness for new usage possibilities

Example: Big Data!



function creep

World English Dictionary

function creep

— *n*

the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, esp when this leads to potential invasion of privacy

Enter free text here ...

Challenge 5: Fuzzy or incomplete information by default

- **Perspective of lawyers:**
  - Don’t be too exact if not necessary
  - Don’t know too much (otherwise: mala fide)
- **Perspective of economists:**
  - Don’t tell too much without extra benefit
- **Sometimes perspective of IT:**
  - Documentation is boring

- **Problem:** Sloppy system descriptions, unclear responsibilities
- **Problem:** Sloppy privacy policies

Examples: Unclear responsibilities

- **Usual excuse when data breaches occur:**
  “not our responsibility”,
  e.g. psychiatric data on the Internet (Nov. 2011):
  cascading service providers, no or only oral contracts, one-(wo)man software developing company, accounts have never be changed over 10 years

⇒ Who is to be fined?

- **Online investigation software** used by the police (2011): “We have only rented the software. We don’t know how it works (we are not supposed to know). We have never processed any data.”

Example: Sloppy privacy policies

"We may collect and process the following data about you:

…

Details of your visits to our site including, but not limited to, traffic data, location data, weblogs and other communication data, whether this is required for our own billing purposes or otherwise and the resources that you access; …"

Example: Sloppy privacy policies

"Collection and Use of Non-Personal Information

We also collect non-personal information – data in a form that does not permit direct association with any specific individual. We may collect, use, transfer, and disclose non-personal information for any purpose. The following are some examples of non-personal information that we collect and how we may use it:

We may collect information such as occupation, language, zip code, area code, unique device identifier, location, and the time zone where an Apple product is used so that we can better understand customer behavior and improve our products, services, and advertising.

…"

Challenge 6: Consent

- **Legal requirements for consent:**
  - Freely given
  - Informed
  - Explicit
  - Specific, not coupled with other usages
  - Withdrawable with effect for the future

Misplaced Confidences: Privacy and the Control Paradox

Laura Brandimarte[1], Alessandro Acquisti[1] and George Loewenstein[2]

Brandimarte / Acquisti / Loewenstein
researching the illusion of control

- **Problem:** many insufficient implementations, often: tricking the user into giving consent (e.g. pre-checked ☒)

⇒ Invalid consent cannot be legal basis for data processing

⇒ Unlawful data processing

Example: Shrink-wrap or click-wrap “consent”

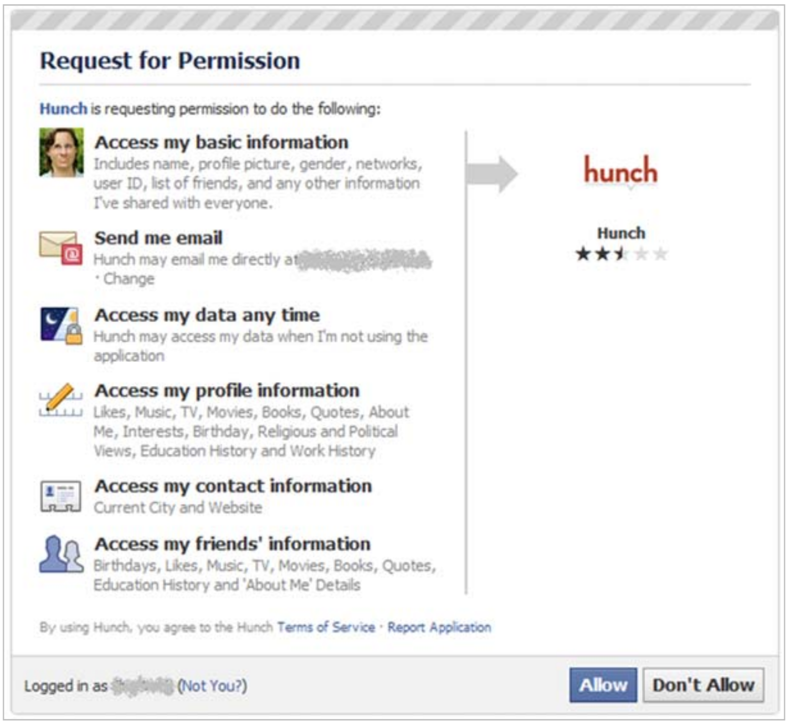
“**Your Consent**
By using this site, you agree with the terms of this Privacy Policy. Whenever you submit information via this site, you consent to the collection, use, and disclosure of that information in accordance with this Privacy Policy.“

http://www.eurebooks.eu/privacy/

“By using this site you agree to the terms and conditions below. Icemakers reserves all rights to changes without notice.”

http://www.icemakers.se/content/legal.aspx

Example: "Take it or leave it" apps



Request for Permission

Hunch is requesting permission to do the following:

Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone.

Send me email
Hunch may email me directly at [redacted] · Change

Access my data any time
Hunch may access my data when I'm not using the application

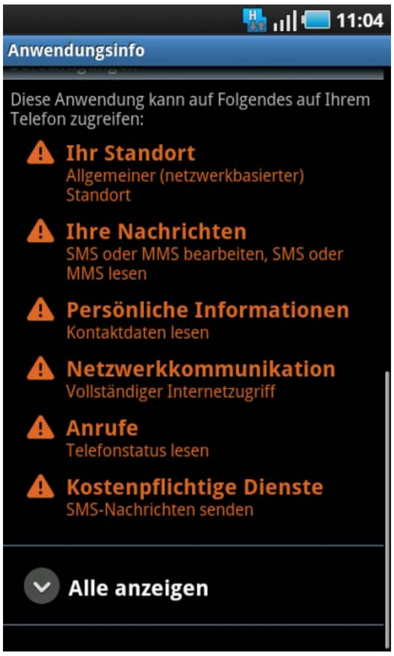
Access my profile information
Likes, Music, TV, Movies, Books, Quotes, About Me, Interests, Birthday, Religious and Political Views, Education History and Work History

Access my contact information
Current City and Website

Access my friends' information
Birthdays, Likes, Music, TV, Movies, Books, Quotes, Education History and 'About Me' Details

By using Hunch, you agree to the Hunch Terms of Service · Report Application

Logged in as [redacted] (Not You?)



Anwendungsinfo

Diese Anwendung kann auf Folgendes auf Ihrem Telefon zugreifen:

Ihr Standort
Allgemeiner (netzwerkbasierter) Standort

Ihre Nachrichten
SMS oder MMS bearbeiten, SMS oder MMS lesen

Persönliche Informationen
Kontaktdaten lesen

Netzwerkkommunikation
Vollständiger Internetzugriff

Anrufe
Telefonstatus lesen

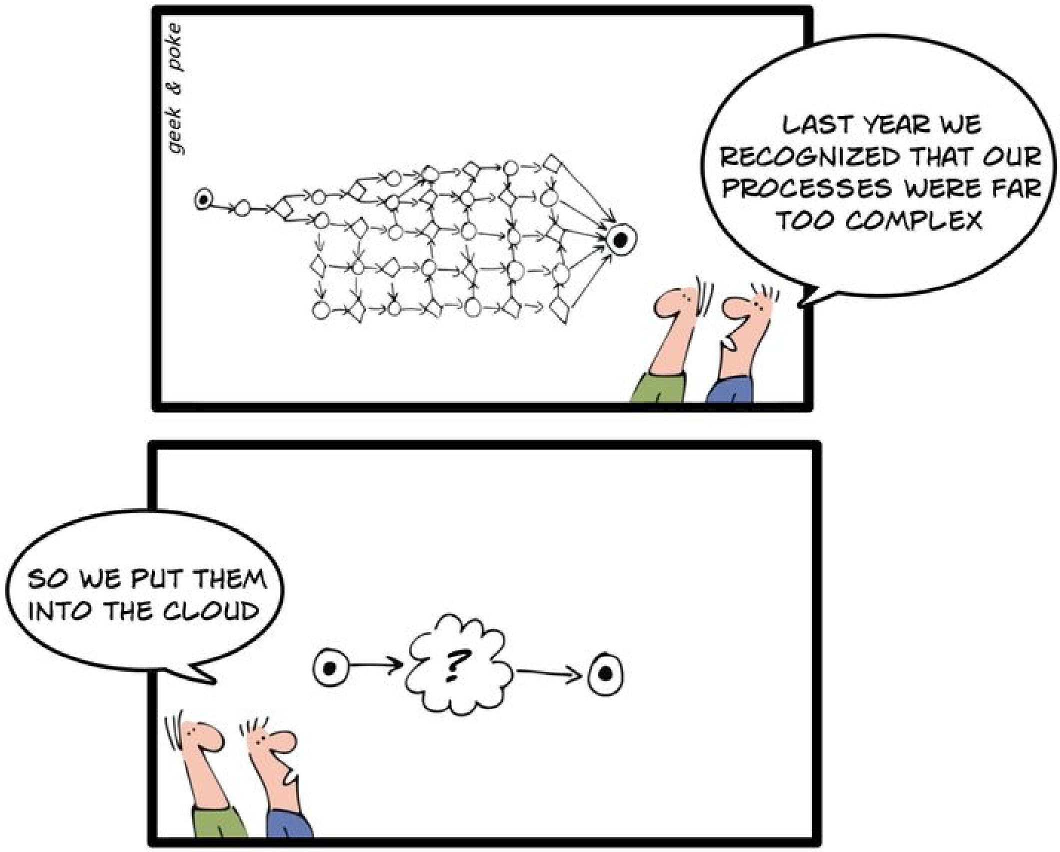
Kostenpflichtige Dienste
SMS-Nachrichten senden

Challenge 7: Integration of 3rd parties & "Location doesn't matter"

- **Service providers offer:** take-over of all annoying complexity
- **Technology offers:** dissociation from location
  - Dynamic routing
  - Dynamic assignment of resources in cloud computing (elasticity of ICT systems)
- **Problem:** Location definitely matters
  in law …
  … and in risk assessment

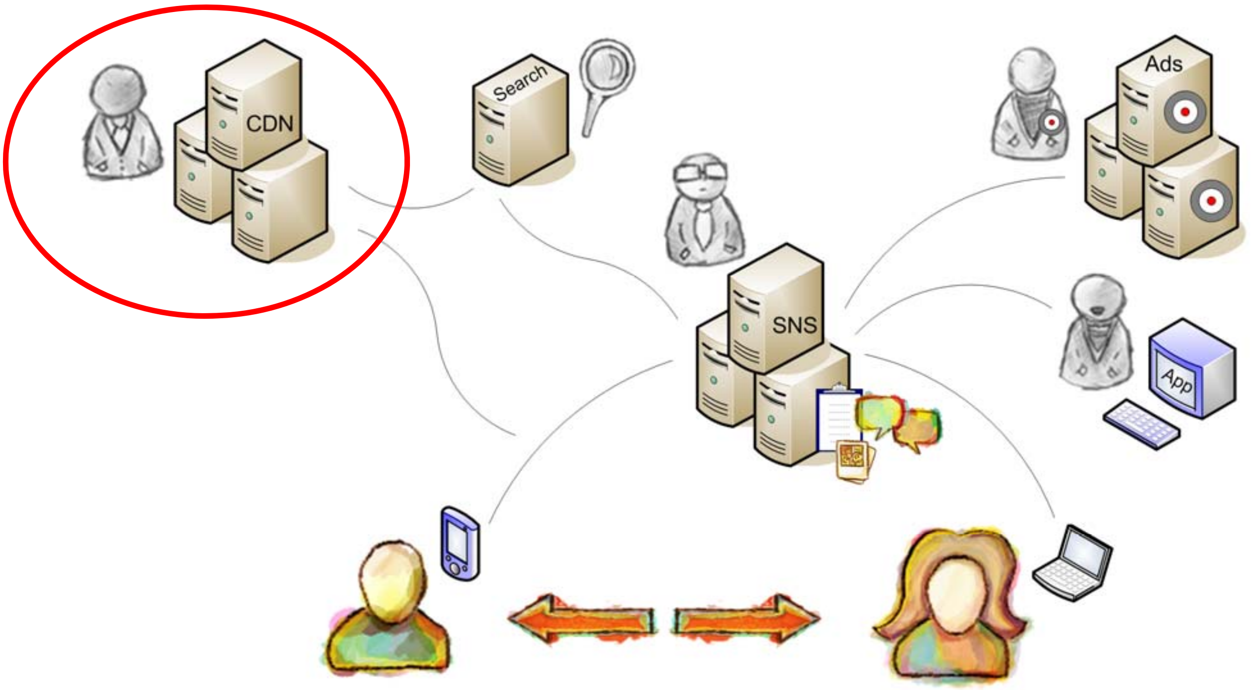
We self-certify compliance with:

U.S.•EU
SAFEHARBOR
U.S. DEPARTMENT OF COMMERCE


geek & poke
LAST YEAR WE RECOGNIZED THAT OUR PROCESSES WERE FAR TOO COMPLEX
SO WE PUT THEM INTO THE CLOUD
?

LET THE CLOUDS MAKE YOUR LIFE EASIER

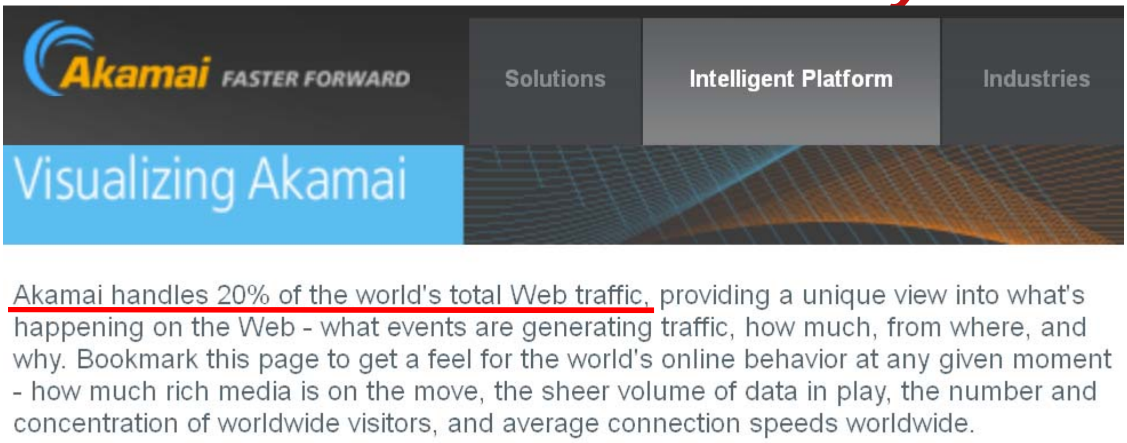
Example: Integrating 3rd party services



Example: Integrating 3rd party services – Content Delivery Networks

- Content Delivery Networks are being used to cache data.
- There are a few big ones such as Akamai, being employed by organisations such as
  - Facebook
  - Apple
  - German TV channels
  - Office of the Federal Chancellor of Germany
  - …

Example: Integrating 3rd party services – Content Delivery Networks



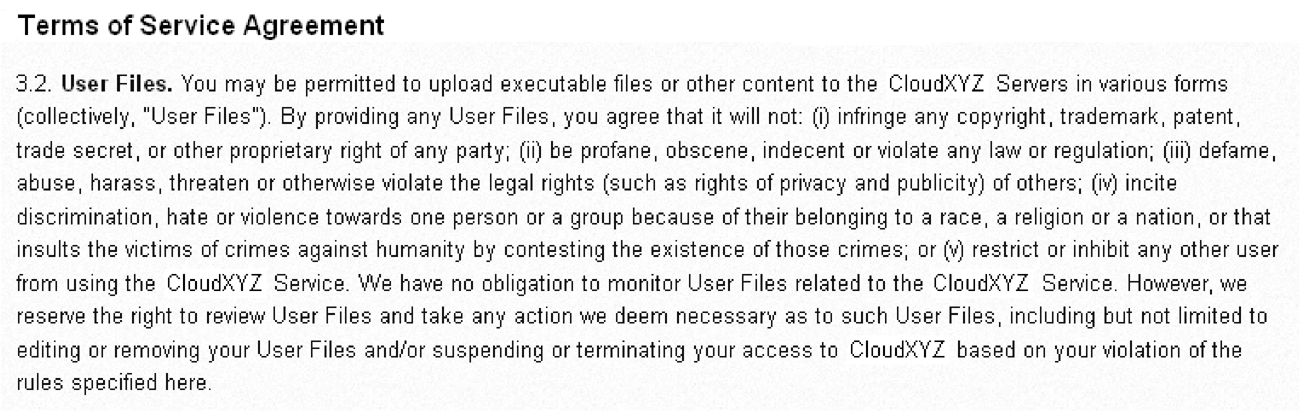
Akamai handles 20% of the world's total Web traffic, providing a unique view into what's happening on the Web - what events are generating traffic, how much, from where, and why. Bookmark this page to get a feel for the world's online behavior at any given moment - how much rich media is on the move, the sheer volume of data in play, the number and concentration of worldwide visitors, and average connection speeds worldwide.

- CDNs (similar: big centralised SNS, search engines, SPAM filters, …) collect, link and analyse masses of personal data
- Is the German Chancellor responsible for potential linkage (by choosing the service and causing the transfer of usage data)?

Risks of (remote) services: Unknown reading / changing access

- **Problem:** Access by governmental authorities, often without informing the data subjects
- **Problem:** "Indecency check": Filtering/deleting/blocking of content, possible account termination
- **Problem:** How to enforce the user's rights in a foreign jurisdiction?

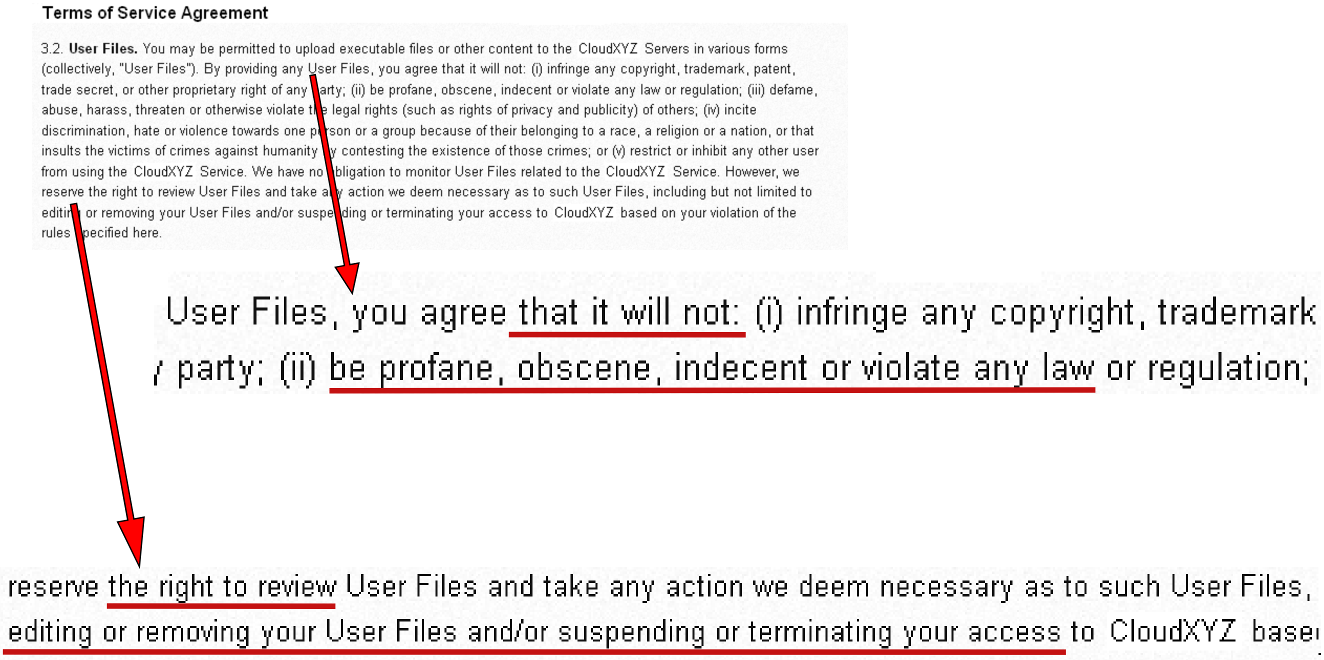
Example: Terms and Conditions of a remote cloud



Terms of Service Agreement

3.2. **User Files.** You may be permitted to upload executable files or other content to the CloudXYZ Servers in various forms (collectively, "User Files"). By providing any User Files, you agree that it will not: (i) infringe any copyright, trademark, patent, trade secret, or other proprietary right of any party; (ii) be profane, obscene, indecent or violate any law or regulation; (iii) defame, abuse, harass, threaten or otherwise violate the legal rights (such as rights of privacy and publicity) of others; (iv) incite discrimination, hate or violence towards one person or a group because of their belonging to a race, a religion or a nation, or that insults the victims of crimes against humanity by contesting the existence of those crimes; or (v) restrict or inhibit any other user from using the CloudXYZ Service. We have no obligation to monitor User Files related to the CloudXYZ Service. However, we reserve the right to review User Files and take any action we deem necessary as to such User Files, including but not limited to editing or removing your User Files and/or suspending or terminating your access to CloudXYZ based on your violation of the rules specified here.

Example: Terms and Conditions of a remote cloud



Terms of Service Agreement

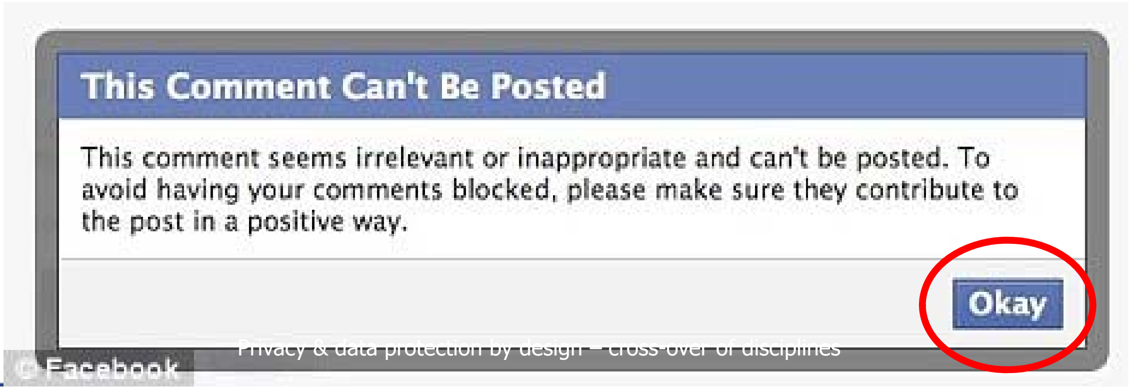
3.2. **User Files.** You may be permitted to upload executable files or other content to the CloudXYZ Servers in various forms (collectively, "User Files"). By providing any User Files, you agree that it will not: (i) infringe any copyright, trademark, patent, trade secret, or other proprietary right of any party; (ii) be profane, obscene, indecent or violate any law or regulation; (iii) defame, abuse, harass, threaten or otherwise violate the legal rights (such as rights of privacy and publicity) of others; (iv) incite discrimination, hate or violence towards one person or a group because of their belonging to a race, a religion or a nation, or that insults the victims of crimes against humanity by contesting the existence of those crimes; or (v) restrict or inhibit any other user from using the CloudXYZ Service. We have no obligation to monitor User Files related to the CloudXYZ Service. However, we reserve the right to review User Files and take any action we deem necessary as to such User Files, including but not limited to editing or removing your User Files and/or suspending or terminating your access to CloudXYZ based on your violation of the rules specified here.

User Files, you agree that it will not: (i) infringe any copyright, trademark
party; (ii) be profane, obscene, indecent or violate any law or regulation;

reserve the right to review User Files and take any action we deem necessary as to such User Files,
editing or removing your User Files and/or suspending or terminating your access to CloudXYZ base

Mistake 8: Little support of intervention

- **Problem:** Little user control (e.g. on profiling)
- **Problem:** Data subject's rights (access, rectification, erasure) not well implemented
- **Problem:** Lock-in for many services

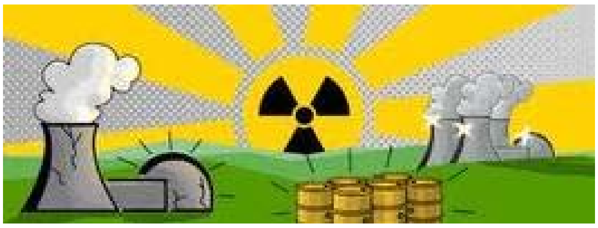


This Comment Can't Be Posted

This comment seems irrelevant or inappropriate and can't be posted. To avoid having your comments blocked, please make sure they contribute to the post in a positive way.

Challenge 9: No lifecycle assessment

- **Statements often heard:**
  - "Let's start!"
  - Be early on the market
  - Create precedents, devil-may-care



- **Problem:** Know the start, but not more – no exit strategy
- **Problem:** "Quick & dirty" may survive
- **Problem:** Long-term thinking and planning is difficult – with few incentives

Challenge 10: Changing assumptions / surplus functionality

- **Problem:** No documented assumptions, no guaranteed conditions
- **Problem:** No established change management

- How to deal with changes?

- **Examples:**
  - Statistics from cancer registry with some fuzziness in linkage – how to establish a feedback process?
  - Privacy tools – what about the business model? Privacy-friendly payment system? Payment via targeted ads?
  - Obligations from law enforcement / homeland security?

Risks if challenges are not met

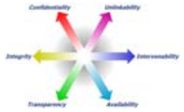
Source: Rob Pongsajapan

- Bits and pieces, but no coherent, comprehensive approach
- Data protection by design only "on paper" to prevent fines?
- Technological progress, but often:
  - Too few incentives
  - Laws are not supporting or even impeding PbD

Overview

1. Privacy and Data Protection by Design
2. A motivated approach of all relevant disciplines
3. Beware of obstacles
4. Conclusion

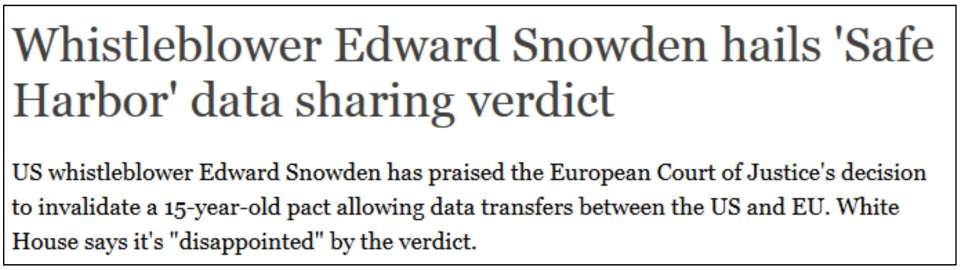
4. Conclusion



- Cross-over of disciplines
  - Is sometimes difficult and time-consuming (but the most efficient way?)
  - Reasonable for research (even if not valued in the respective disciplines’ metrics)
  - To some extent necessary for workable solutions!
- The whole is more than the sum of its parts.
- Need for catching up: Big companies & secret services have been using the multidisciplinary approach for a long time – with other objectives in mind.

One discipline I haven’t mentioned: ~~sports~~ journalism

News from
6 Oct, 2015



Whistleblower Edward Snowden hails 'Safe Harbor' data sharing verdict

US whistleblower Edward Snowden has praised the European Court of Justice's decision to invalidate a 15-year-old pact allowing data transfers between the US and EU. White House says it's "disappointed" by the verdict.

http://www.dw.com/en/whistleblower-edward-snowden-hails-safe-harbor-data-sharing-verdict/a-18765062

Sascha Lobo

Reto Klar

Die Bewertungen dieses Urteils kamen s
meisten Fachleute brauchen würden, die
Urteilsbegründung zu analysieren: "Sens
"starkes Signal" (Justizminister), "Welt v
Diese Einschätzungen mögen richtig sei
überraschendes Kopfballtor einer Manns
Schlimmer noch, das ganze Datenschutz
Abhang statt. Bei stürmischem Wind. Mi
einem zweiten aus Granit.

“… they are celebrating a surprising headed goal of a team that is 16:1 adrift. Even worse, the privacy tournament takes place on a hillside. In stormy weather. With a ball made from straw. And another one made from granite.”

http://www.spiegel.de/netzwelt/web/safe-harbor-zeigt-probleme-werden-nur-verschoben-lobo-kolumne-a-1056594.html

4. Conclusion

Confidentiality
Unlinkability
Integrity
Intervenability
Transparency
Availability

- Cross-over of disciplines
  - Is sometimes difficult and time-consuming (but the most efficient way?)
  - Reasonable for research (even if not valued in the respective disciplines' metrics)
  - To some extent necessary for workable solutions!
- The whole is more than the sum of its parts.
- Need for catching up: Big companies & secret services have been using the multidisciplinary approach for a long time – with other objectives in mind.
- Publicity & media coverage can be a game changer.

Thank you for your attention!

Marit Hansen
marit.hansen@datenschutzzentrum.de

ipen

forum <privatheit> selbstbestimmtes_leben_in_der_digitalen_welt

ABC4TRUST

FutureID

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein