

---

# Top Mistakes in System Design from a Privacy Perspective

Marit Hansen

January 29, 2013

privtech12, Göteborg



Unabhängiges Landeszentrum für  
Datenschutz Schleswig-Holstein

## *Overview*

- The legal perspective of privacy and data protection
- Top mistakes in system design from a privacy perspective
- Conclusion

# Setting of ULD in Schleswig-Holstein

- 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

<b>Country</b>	Germany
<b>Capital</b>	Kiel
<b>Government</b>	
• <b>Minister-President</b>	Torsten Albig (SPD)
• <b>Governing parties</b>	SPD / Greens / SSW
• <b>Votes in Bundesrat</b>	4 (of 69)
<b>Area</b>	
• <b>Total</b>	15,763.18 km <sup>2</sup> (6,086.20 sq mi)
<b>Population</b> (2011-12-31) <sup>[1]</sup>	
• <b>Total</b>	2,837,641
• <b>Density</b>	180 / km <sup>2</sup> (470 / sq mi)

Source: [en.wikipedia.org/wiki/Schleswig-Holstein](http://en.wikipedia.org/wiki/Schleswig-Holstein)



Source: [www.maps-for-free.com](http://www.maps-for-free.com)

## *Complex system of data protection commissioners in Germany*

- **1 Federal DP Commissioner**
  - for **public sector** on the federal level;  
legal basis: Federal DP Act (BDSG)
  
- **16+ DP Commissioners for 16 States**
  - for **public sector** on the State level;  
legal basis: 16 State DP Acts
  - for **private sector**, i.e., companies  
located in the State;  
legal basis: **Federal DP Act**
  
- **Own DP Commissioners for  
churches and broadcasting corporations**



## *Good news: Harmonisation on the EU level*

European data protection directives:

- Data Protection Directive 95/46/EC
- e-Privacy Directive 2009/136/EC

... to be implemented by the Member States in national law



## *7 rules of European data protection law*

1. Lawfulness

Processing of personal data is lawful only if a statutory provision permits it or if the data subject has consented.

2. Consent

3. Purpose Binding

Consent means: informed consent and freely given.

4. Necessity and Data Minimisation

5. Transparency and Data Subject's Rights

6. Data Security

Personal data obtained for one purpose must not be processed for other purposes.

7. Audit and Control

## *7 rules of European data protection law*

1. Lawfulness

2. Consent

3. Purpose Binding

4. Necessity and Data Minimisation

5. Transparency and Data Subject's Rights

6. Data Security

7. Audit and Control

Only personal data necessary for the respective purpose may be processed.

Personal data must be erased as soon as they are not needed anymore.

## *7 rules of European data protection law*

1. Lawfulness

2. Consent

3. Purpose Binding

4. Necessity and Data Minimization

5. Transparency and Data Subject's Rights

6. Data Security

7. Audit and Control

Collection and use of personal data has to be transparent for data subjects.

Data subjects have rights to access and rectification as well as (constrained) on blocking and erasure of their personal data.



## *7 rules of European data protection law*

1. Lawfulness

2. Consent

3. Purpose Binding

4. Necessity and Data Minimisation

5. Transparency and Data Subject's Rights

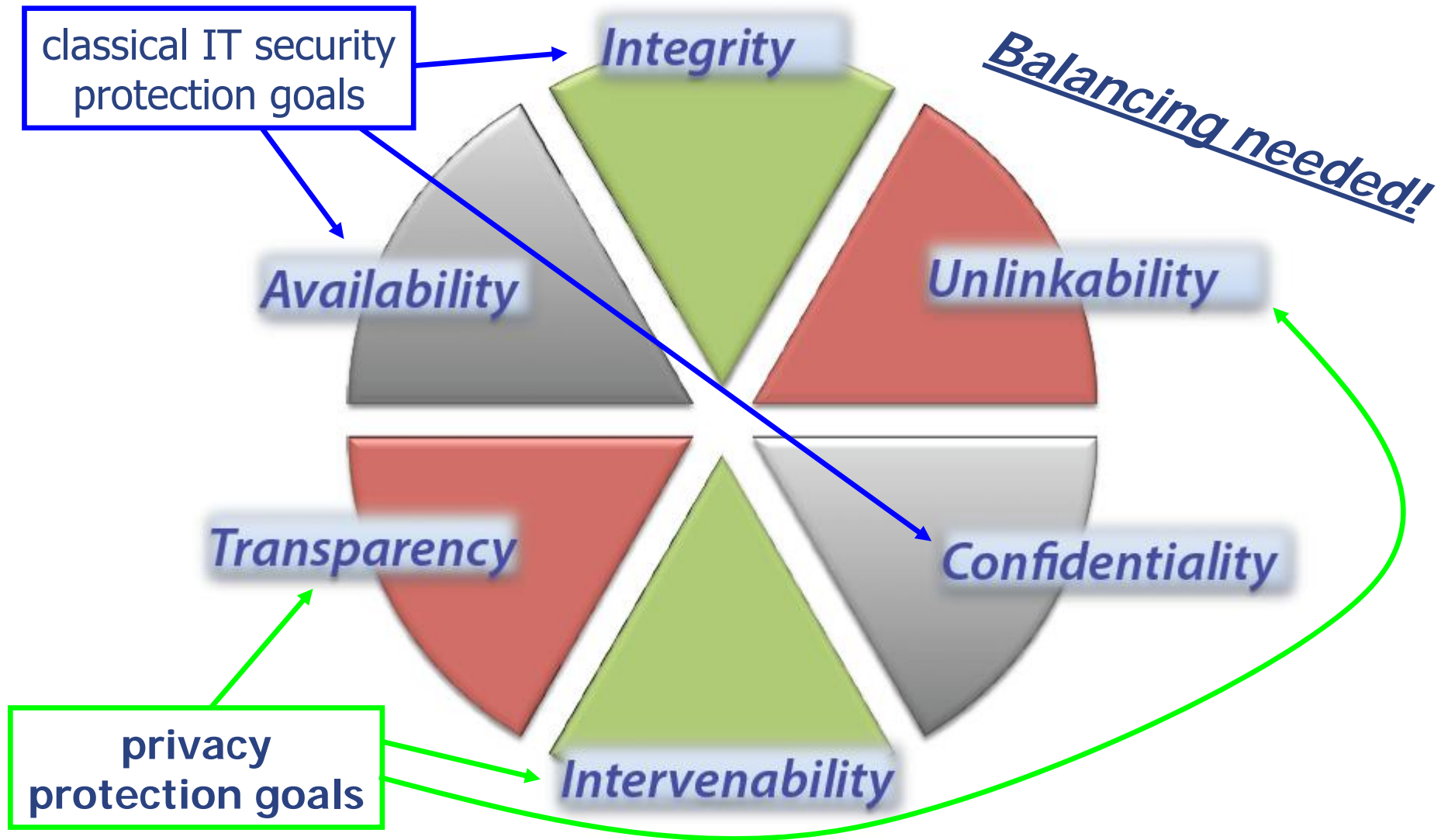
6. Data Security

7. Audit and Control

Unauthorised access to personal data must be prevented by technical and organisational safeguards.

Need for internal and external auditing/controlling of the data processing

## *Extended Set of Protection Goals*



## *Relation of CIA-UTI and 7 rules of European data protection law*

1. Lawfulness

2. Consent

Transparency

Intervenability

3. Purpose Binding

Unlinkability

4. Necessity and Data Minimisation

Unlinkability

5. Transparency and Data Subject's Rights

Transparency

Intervenability

6. Data Security

Confidentiality

Integrity

Availability

7. Audit and Control

Transparency

Intervenability

Integrity

## *Overview*

- The legal perspective of privacy and data protection
- Top mistakes in system design from a privacy perspective
- Conclusion



## *Mistake 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

## *Mistake 2: Linkability by default*

- **Principle in IT:**
  - 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)  $\Rightarrow$  risk
- **Problem:** unlinkability often means more effort, more complexity
- **Problem:** real life

*Example: 2006: AOL publishes anonymised 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	cupld.com	2006-03-11	00:08:50		

Quelle: [http://www.lunchoverip.com/2006/08/being\\_user\\_4417.html](http://www.lunchoverip.com/2006/08/being_user_4417.html)

## *Number 4417749*

school supplies for Iraq children

the best season to visit Italy

safest place to live      termites

mature living

tea for good health

hand tremors      nicotine effects on the body      dry mouth      bipolar

numb fingers      60 single men      dog that urinates on everything

Mrs Arnold said she was shocked that her search queries had been recorded and released to the public by AOL.

"My goodness, it's my whole personal life," she said.

"I had no idea somebody was looking over my shoulder."





## 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)

## *Netflix: Real-life linkability*

Here's what the dynamic duo have to say about one person whose data they outed:

*"First, we can immediately find his political orientation based on his strong opinions about "Power and Terror: Noam Chomsky in Our Times" and "Fahrenheit 9/11." Strong guesses about his religious views can be made based on his ratings on "Jesus of Nazareth" and "The Gospel of John". He did not like "Super Size Me" at all; perhaps this implies something about his physical size? Both items that we found with predominantly gay themes, "Bent" and "Queer as folk" were rated one star out of five. He is a cultish follower of "Mystery Science Theater 3000". This is far from all we found about this one person, but having made our point, we will spare the reader further lurid details. "*

So Netflix may have inadvertently revealed the political affiliation, sexual orientation, BMI and God-knows-what else of 500,00 of their subscribers. Way to go!

## *Mistake 3: Real identity by default*

- **Tradition:**

**Real name** – long-established tradition in many cultures:  
 “Whoever doesn’t say his/her name, is **suspicious**”

- **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:

Birthday:

Why do I need to provide my date of birth?

## *Mistake 3: Real identity 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**





WAS GEHT?

SEARCHING...SEEK & TÄG!

F.A.Q.

NDR.de

## NDR Wacken 2011 - Giga-Panorama

**Suche und finde dich und deine Freunde auf dem NDR Wacken 2011 - Giga-Panorama.**

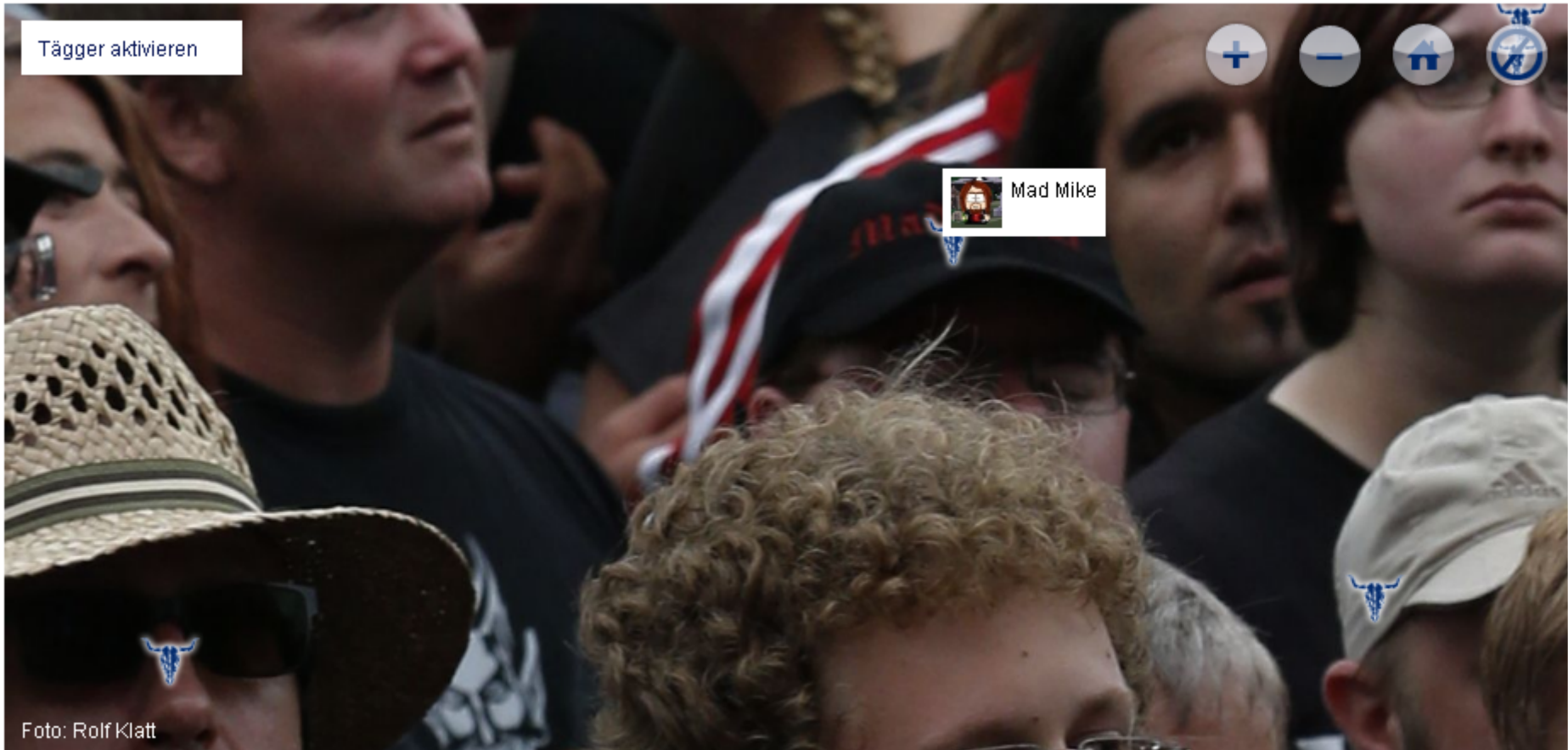
Wenn du dich gefunden hast, tagge deine Position und poste deinen Tag auf deiner Pinnwand in Facebook oder im Buschfunk im VZ Netzwerk.

### Wacken Open Air: Metal auf der Kuhweide

Bei NDR.de bist du mittendrin im Geschehen - Bildergalerien, Livestreams und Videos, Reportagen, ein Wacken-Quiz und vieles mehr gibt es im Internet-Special zum größten Heavy-Metal-Festival der Welt unter [www.ndr.de/wacken](http://www.ndr.de/wacken)









The screenshot shows a Mozilla Firefox browser window with the title 'Mad Mike - Mozilla Firefox'. The address bar displays 'https://www.facebook.com/mad.mike.904'. The Facebook profile page for 'Mad Mike' is visible, featuring a profile picture of a cartoon character with a beard and glasses, a name 'Mad Mike', and a gender 'Männlich'. There are buttons for 'FreundIn hinzufügen', 'Fotos', and 'Karte'.

*Most tagged individuals have a profile with real data.*



## *Facebook function: Photo tagging*



## *Specialty of photo tagging + biometric matching in Facebook*

- Photos are **not biometrically optimised** (unlike in eIDs)
- **Crowd approach** with ongoing correction (also for authentication)
- Photo tag **suggestion**: based on friend list
- Opt-out not for biometric matching engine
- **Because of privacy complaints deactivated** in Europe since Oct. 2012





Upload, link, or email an image from your favorite site or mobile app

Fun. Easy. Free.



iphone



android



facebook



instagram



any website



LATEST ARTICLES



September 18, 2012

### Busty Schoolteacher Looks Like A Porn Star!!!

So I live right by this middle school and everyday I'm out walking by after work and I see this teacher staring at me. She's a hot thing with blonde hair, nice big tits, a big smile, and long legs, and I just had to talk to her. So I go up to her and she ignores me and blows me off like she's some kind of important model. Instantly, I knew I had to get a picture of her so I could get back at her by finding her porn star match with [Naughty America's facematch tool](#). I wish she would have come over, but whatever; her results have made me happy time and time again.

[Click here](#) to see the busty schoolteacher's porn star look-a-like!

## try it

\* You must upload a JPG file. For best results, the uploaded picture should be a well lit photo with a face that is facing forward and not obscured by anything.

Upload Picture

I certify that I have the right to distribute this picture and I agree to the [Terms of Use](#).

Upload picture

Enter picture URL



Upload, link, or email an image



iphone



android



facebook



in

LATEST ARTICLES



September 18, 2012

**Busty School  
Like A Porn S**

So I live right by this mic walking by after work an She's a hot thing with b and long legs, and I just and she ignores me and of important model. Inst of her so I could get bac match with [Naughty Ame](#) would have come over, I made me happy time and

[Click here](#) to see the bu look-a-like!

**Upload Picture**




Durchsuchen...

I certify that I have the right to distribute this picture and I agree to the [Terms of Use](#).

**Enter picture URL**




I certify that I have the right to distribute this picture and I agree to the [Terms of Use](#).

ULD



NAUGHTYAMERICA

Upload, link, or email an image

Upload Picture



# Busty Schoolteacher Looks Like A Porn Star!!!

So I live right by this middle school and everyday I'm out walking by after work and I see this teacher staring at me.

She's a hot thing with blonde hair, nice big tits, a big smile, and long legs, and I just had to talk to her. So I go up to her and she ignores me and blows me off like she's some kind of important model. Instantly, I knew I had to get as picture of her so I could get back at her by finding her porn star match with [Naughty America's facematch tool](#). I wish she

htt

# Google, too?

## Facial Recognition: The One Technology Google Is Holding Back

The Huffington Post | Bianca Bosker | First Posted: 06/01/11 09:53 AM ET | Updated: 08/01/11 06:12 AM ET 

SHARE THIS STORY

Google has been known for ambitiously developing technology that seems more science fiction than Silicon Valley, such as self-driving cars, but former CEO Eric Schmidt shared one technology he thought was the only one Google has ever built, then decided to stop. Facial recognition.

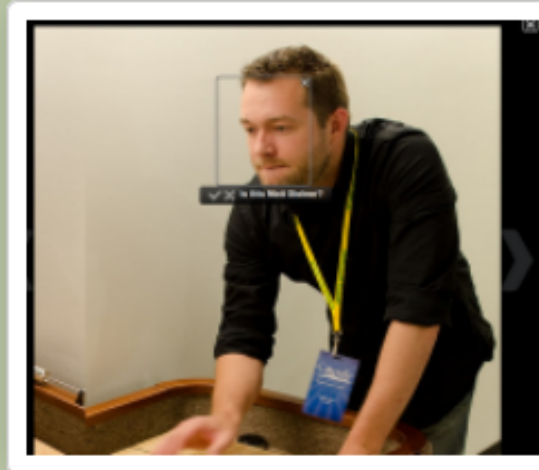
Saturday, December 10, 2011

### Facial Recognition No Longer "Too Dangerous" For Google

Activist Post

Only six months after former CEO of Google, Eric Schmidt, called facial recognition software "too dangerous to implement," Google introduces the 'Find My Face' tool for Google+ users.

This week, Google made the announcement that they were rolling out facial recognition tools in a Google Plus blog post, "It is now even easier to tag photos of yourself and your friends, thanks to a new feature we are rolling out called Find My Face, which will help your friends tag your photos if you are in their pictures, and help you tag them if they have activated Find My Face."



Matt Steiner Google Engineer  
Google Plus image

"This technology and we withheld it," Schmidt said at the All Things Digital conference in California. "As far as I know, this is the only technology Google has built and, after we decided to stop."

Schmidt expressed concern personally about the union of Google and face recognition," he explained, "the company feared that these tools could be used both for good and "in a bad way." Schmidt described a scenario in which a "bad actor" could use facial recognition to find people in a crowd and use the technology to identify citizens.

# *Siri: iPhone speech assistance in the iCloud*



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](#) 



## *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.)



# Nina: Similar to "Siri" for Android and iOS

## Nuance offers iOS, Android SDK for Siri-like Nina assistant

updated 12:55 pm EDT, Mon August 6, 2012



### Voice assistant includes voice biometrics for security

Nuance has released a software development kit for its [previously announced](#) virtual-assistant software, named [Nina](#) (Nuance Interactive Natural Assistant). The SDK will allow developers to add voice-based features to their apps, though Nuance suggests Nina is geared for businesses that want to automate their mobile product support, rather than providing the more general appointment scheduling and message composition services offered by Siri and Google Now.

Taking advantage of specific phrases such as either a call to a customer service representative, voice biometrics are also said to be used for account passwords.

**Built-in vocal biometrics are also said to recognize the speaker, allowing the software to handle account security without passwords.**

Developers can utilize the Nina Virtual Assistant SDK for both Android and iOS platforms, with initial support for US, British and Australian English—other languages are promised for later in the year. Nuance is also allowing organizations to brand their own virtual assistant persona, utilizing one from an existing range of Nuance text-to-speech voices or paying for a custom voice to be created. [\[via Engadget\]](#)

## *Mistake 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

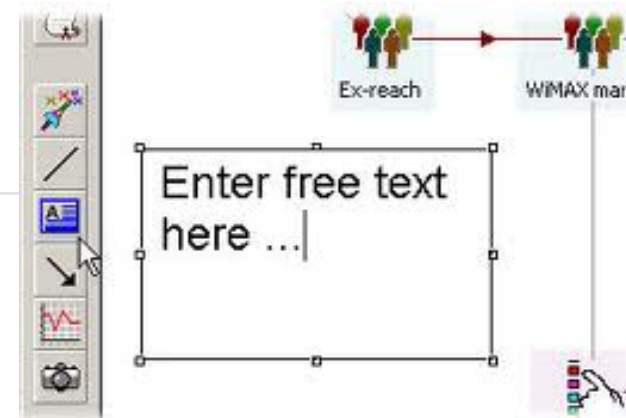
### function creep

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

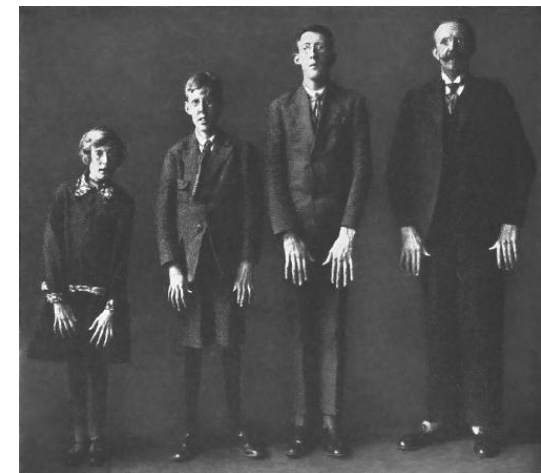


## *Example: Data retention + data usage*

- **Starting point (EU, <2006):** telecommunication providers (phone, e-mail) must erase personal usage data as soon as possible; they must not use available data for other than accounting purposes
- **2006:** The Europe Commission introduced the **Data Retention Directive**, forcing telcos to store usage data for 6 months;  
sole purpose: answering requests of law enforcement bodies
- Marketing departments of telcos demanded to use these retention data **for additional purposes**

## *Example: Additional information in biometrics*

- Face data:
  - Gender
  - Color of eyes, hair, skin
  - Ethnicity
  - Medical information
  - Drug usage
  - Mood
- Fingerprint data:
  - Skin abrasure (e.g. from work)
  - Health of mother during first three months of pregnancy
  - Ethnicity, geographical origin



Archiv f. Augenheilkunde, Band 104, 1931, S. 16; Verlag Bergmann, München

## *Mistake 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*

“We may also share Personal Information with third party service organisations **such as** DAI, SFAFT B.V., Kiwida and their related companies (as defined in the Companies Act 1993), employees and agents for our and SFAFT B.V.’s business purposes (**including but not limited to** improvement of our product marketing and advertising) and to implement Subway Express.”





## *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.

”  
...

## *Mistake 6: Invalid consent*

- **Legal requirements for consent:**
  - Freely given
  - Informed
  - Explicit
  - Specific, not coupled with other usages
  - Withdrawable with effect for the future
  
- **Problem:** many insufficient implementations of consent
  - ⇒ **Invalid consent cannot be baseline 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?)

**Allow** **Don't Allow**

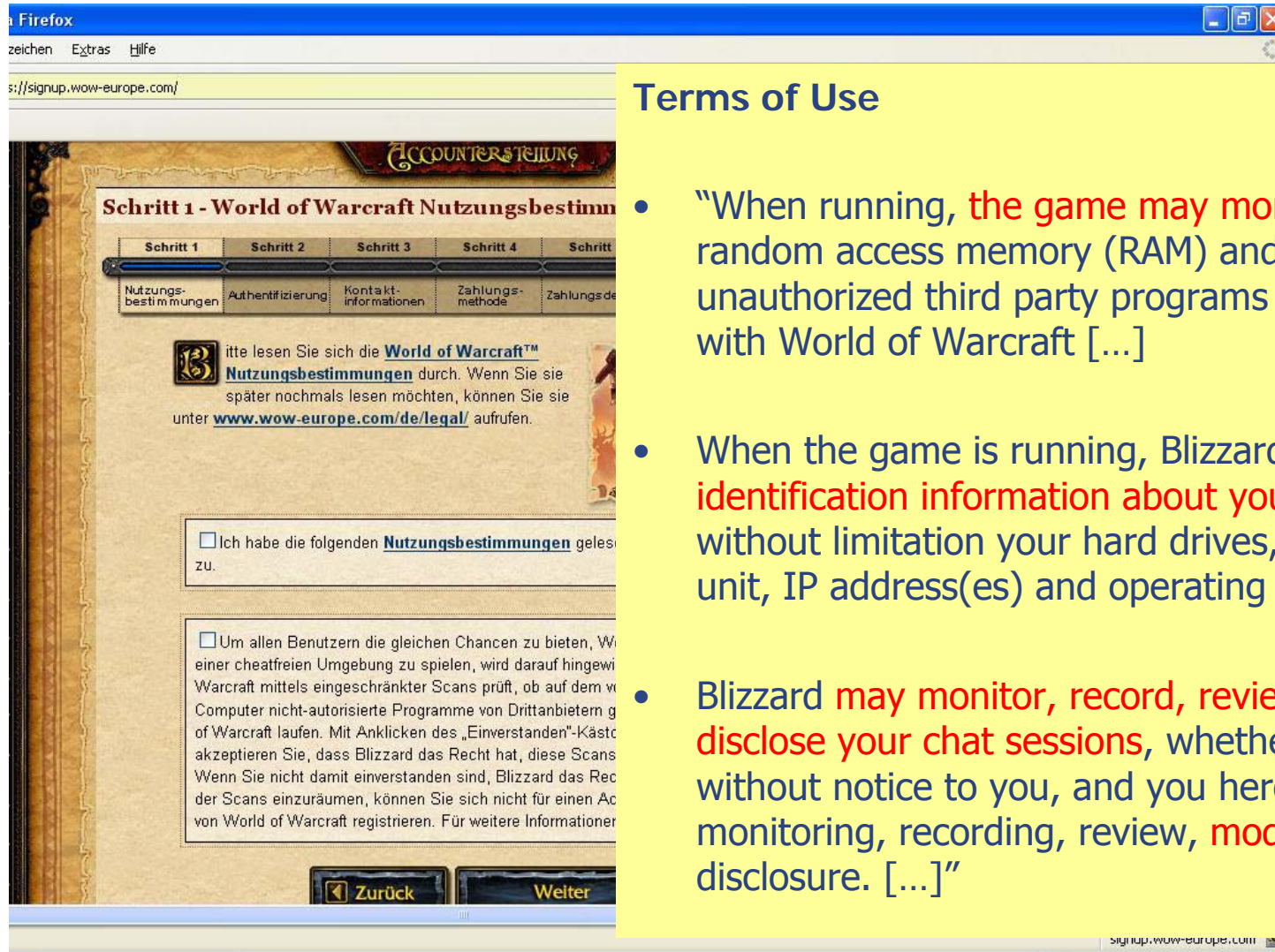
**Anwendungsinfo** 11:04

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
- 
**Netzwerkcommunication**  
 Vollständiger Internetzugriff
- 
**Anrufe**  
 Telefonstatus lesen
- 
**Kostenpflichtige Dienste**  
 SMS-Nachrichten senden

**Alle anzeigen**

# World of Warcraft: Scanning the user's PC



## Terms of Use

- “When running, the game may monitor your computer’s random access memory (RAM) and/or CPU processes for unauthorized third party programs running concurrently with World of Warcraft [...]
- When the game is running, Blizzard may obtain certain identification information about your computer, including without limitation your hard drives, central processing unit, IP address(es) and operating system(s) [...]
- Blizzard may monitor, record, review, modify and/or disclose your chat sessions, whether voice or text, without notice to you, and you hereby consent to such monitoring, recording, review, modification and/or disclosure. [...]

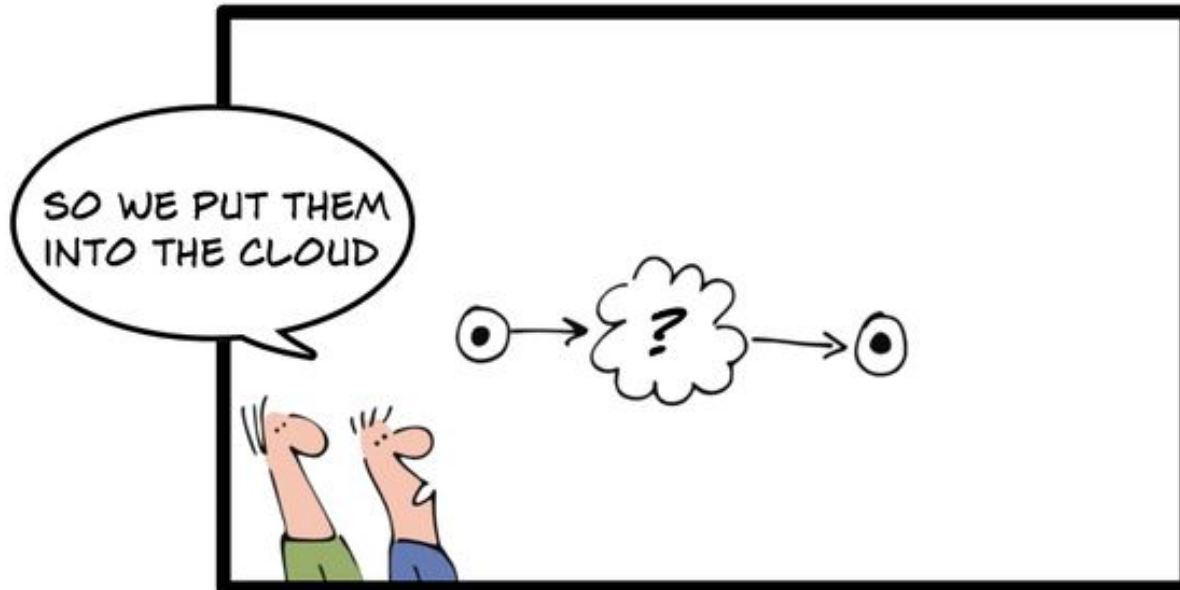
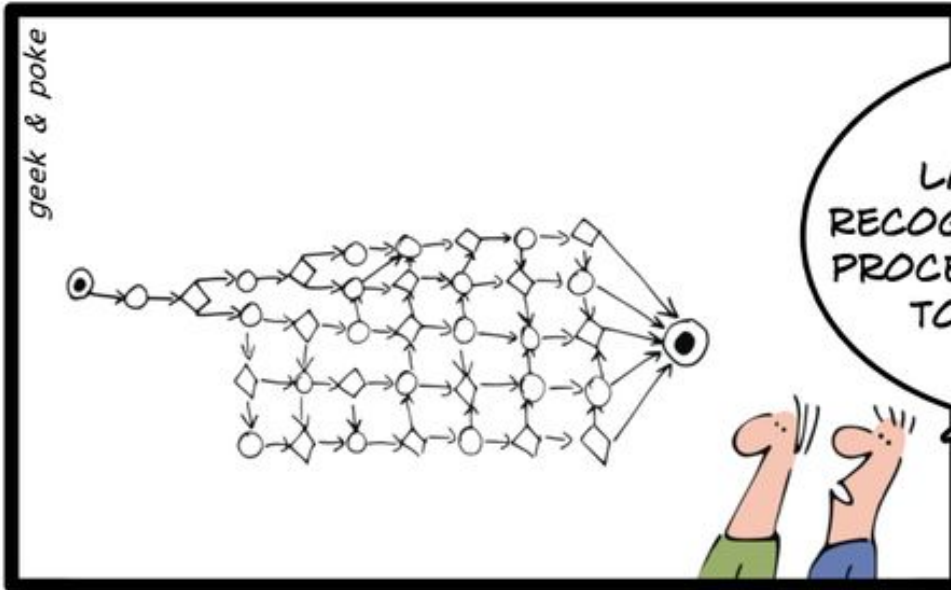


## *Mistake 7: Integration of 3rd parties & "Location doesn't matter"*

- **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

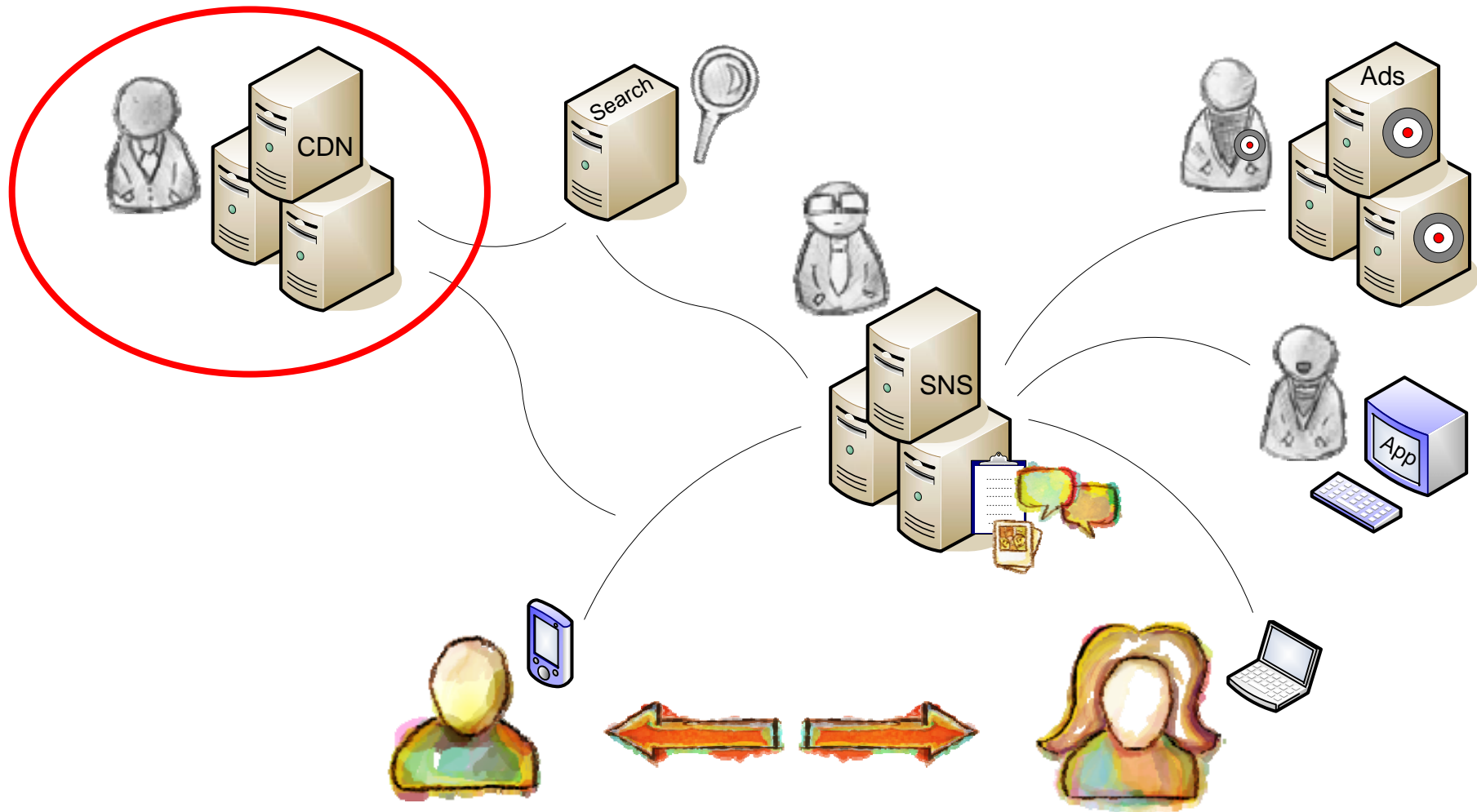


von Oliver Widder



LET THE CLOUDS MAKE YOUR LIFE EASIER

# *Example: Integrating 3rd party services*



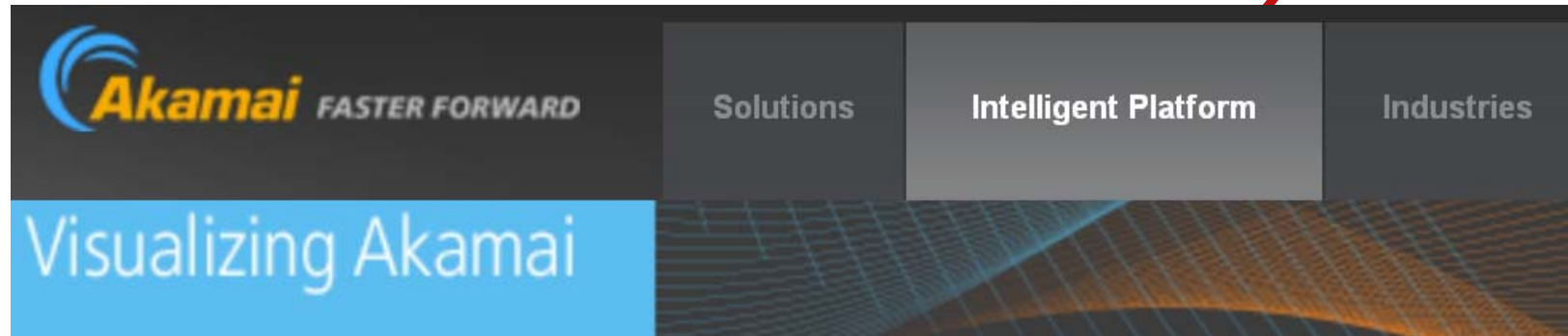




## *Example: Integrating 3rd party services – Content Delivery Networks*

- 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)?**


# Web linkability by 3rd parties visualised: "Collusion"


## Collusion


[about](#) | [site info](#) | [filters](#) | [credits](#)

 Reset

 Export

 Zoom In






 Zoom Out

 Hide Panel

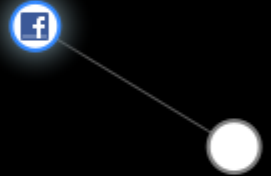
Keep browsing the web. As you do so, the graph on this page will change. Each circle represents a website.


Hover your mouse over the circles to learn more about them.

### Legend

-  Site you have visited
-  Site you have not visited
-   has sent data about you to 

This add-on is still in development and is not guaranteed to be entirely accurate.

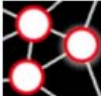




## ADD-ONS

[EXTENSIONS](#) | [PERSONAS](#) | [THEMES](#) | [COLLECTIONS](#) | [MORE...](#)

[Home](#) » [Extensions](#) » [Collusion](#)



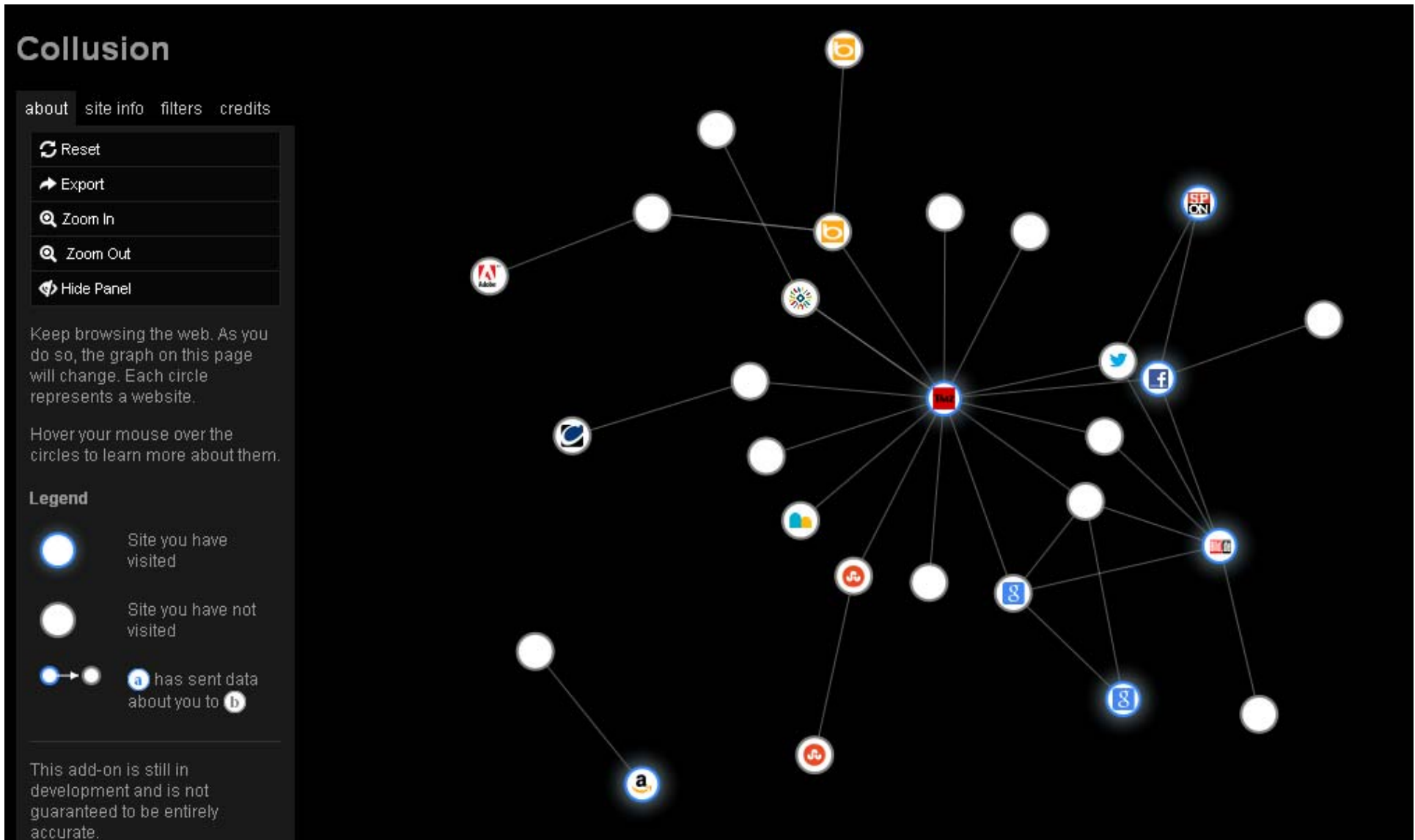
### Collusion 0.24

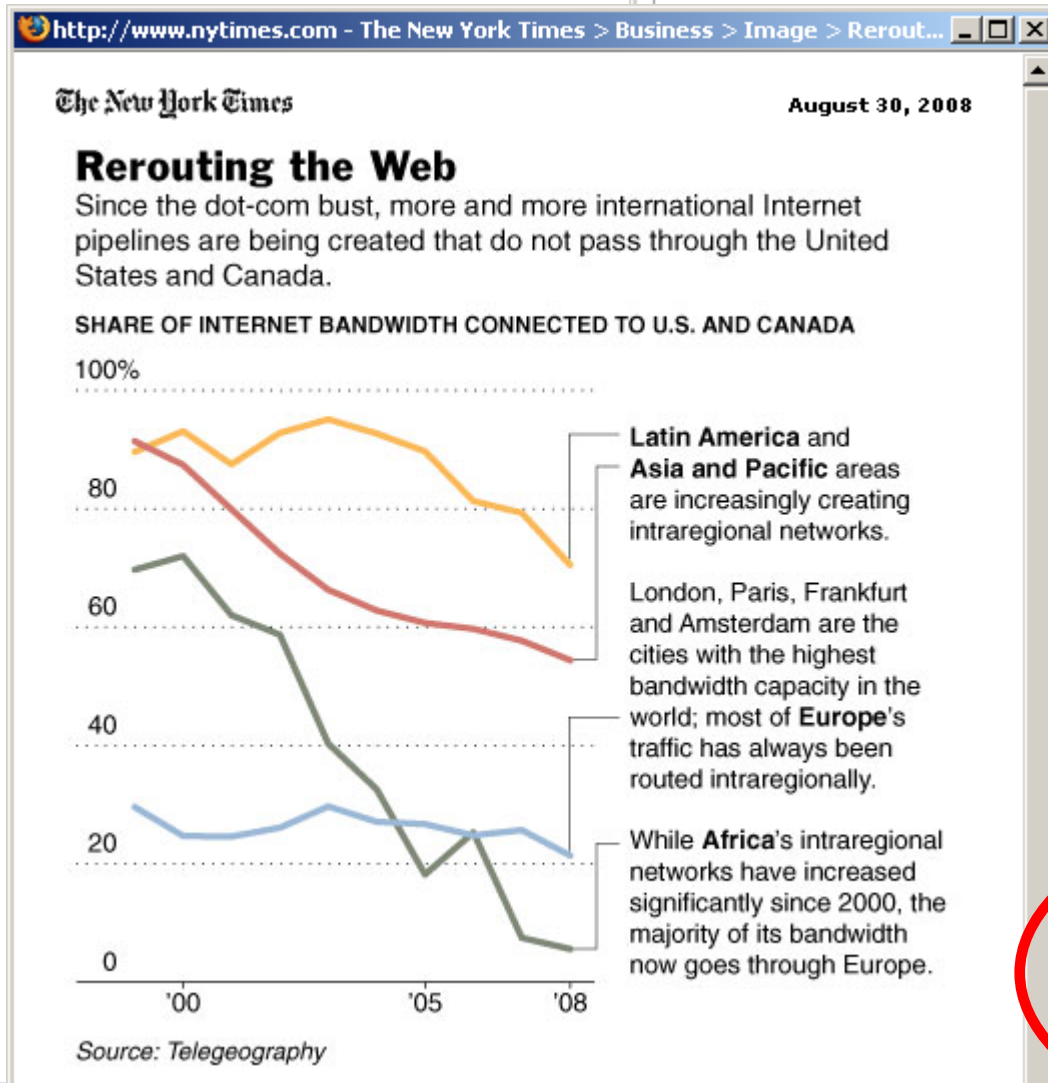
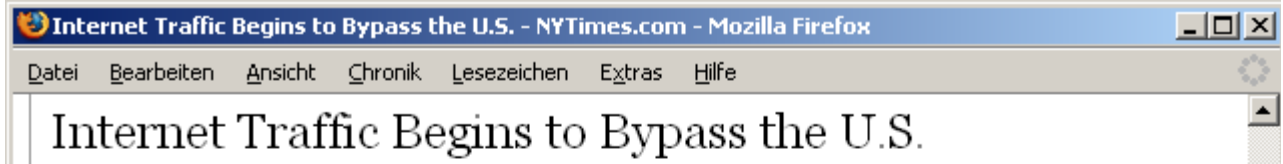
by Jono X, Dethe Elza

NO RESTART

Visualize who's tracking you in real time. To get started, click on the Collusion icon in the bottom-right corner of your browser. (You may need to show the Add-on Bar to see the icon.)

# Web linkability by 3rd parties visualised: "Collusion" (after 3 clicks)





of the American Internet is ending.

Invented by American computer scientists during the 1970s, the Internet has been embraced around the globe. During the network's first three decades, most Internet traffic flowed through the United States. In many cases, data sent between two locations within a given country also passed through the United States.



Engineers who help run the Internet said that it would have been impossible for the United States to maintain its hegemony over the long run because of the very nature of the Internet; it has no central point of control.

And now, the balance of power is shifting. Data is increasingly flowing around the United States, which may have intelligence — and conceivably military — consequences.

American intelligence officials have warned about this

# Patriot Act affects European cloud adoption

By Zack Whittaker | August 2, 2011, 2:06pm PDT

**Summary:** *Microsoft's admission, made at the Office 365 launch, that EU data is vulnerable to U.S. inspection is hampering cloud uptake and growth.*

More and more organisations are abstaining from the cloud, according to a report [by a leading newspaper](#), due to the reach of the Patriot Act in Europe and further afield.

According [to the Financial Times](#) (available via Google without registering), the discussions were brought up during private FT meetings last month, and data privacy and cloud services topped the concerns of IT bosses.

During the Office 365 launch in London in June, [Microsoft admitted to ZDNet](#) that any data stored, processed or owned in Europe and further afield — including email, file storage and web applications — are liable for U.S. government inspection under the Patriot Act.

The FT's report is crucial to understand the feeling in the wider room amongst IT chiefs. As many are data controllers as well as processors of the data, it could lead to civil or criminal action against cloud users for mismanagement of data.

Due to the disparity between European and U.S. law, wholly-owned subsidiaries cannot comply with the European Data Protection Directive — which requires companies to inform their users that data will leave the European zone — because [U.S. law can 'gag' them with existing legislation](#).

Microsoft's admission sets precedent across the board, applying to every other cloud-service provider with an entity in the United States, including Amazon, Intel, Apple and Google.

# Patriot Act affects European cloud adoption

By Zack Whittaker | August 2, 2011, 2:06pm PDT

**Summary:** *Microsoft's admission, made at the Office 365 launch, that EU data is vulnerable to U.S. inspection is hampering cloud uptake and growth.*

More and more organisations are abstaining from the cloud, according to a report [by a leading newspaper](#), due to the reach of the Patriot Act in Europe and further afield.

According [to the Financial Times](#) (available via Google without registering), the discussions were brought up during private FT meetings last month, and data privacy and cloud services topped the concerns of IT bosses.

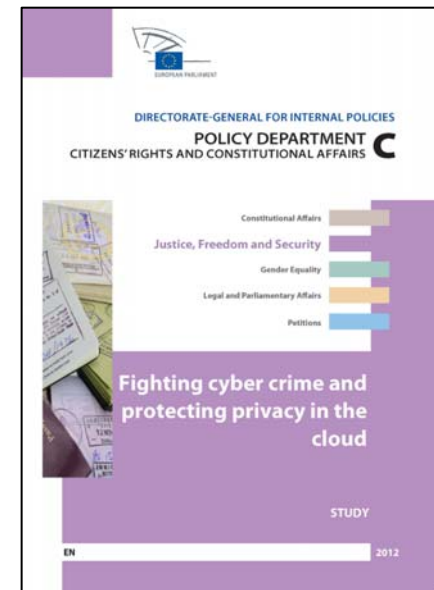
During the Office 365 launch in London in June, [Microsoft admitted to ZDNet](#) that any data stored, processed or owned in Europe and further afield — including email, file storage and web applications — are liable for U.S. government inspection under the Patriot Act.

Due to the disparity between European and U.S. law, wholly-owned subsidiaries cannot comply with the European Data Protection Directive — which requires companies to inform their users that data will leave the European zone — because [U.S. law can 'gag' them with existing legislation](#).

Microsoft's admission sets precedent across the board, applying to every other cloud-service provider with an entity in the United States, including Amazon, Intel, Apple and Google.

## *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?



DG Internal Policies (2012): Fighting cyber crime and protecting privacy in the cloud. Study.

<http://www.europarl.europa.eu/committees/fr/studiesdownload.html?languageDocument=EN&file=79050>





## *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*

- **Intervenability needs transparency**
- **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



## *Mistake 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**



## *Mistake 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?

## *Overview*

- The legal perspective of privacy and data protection
- Top mistakes in system design from a privacy perspective
- **Conclusion**

## *Summary of top mistakes*

### **Unlinkability:**

- Storage
- Linkability
- Real identity
- Function creep

### **Transparency:**

5. Fuzzy & incomplete information
6. Invalid consent

### **Intervenability:**

- Third party integration: location underestimated
- Little support of intervention
- No lifecycle assessment
- Changing assumptions / surplus functionality

*Reality check: Do PETs change that?*



*Thank you for your attention!*

