TRANSPARENT ODER GLÄSERN ?

— Big Data und Schweigepflicht —

Hans Metsch

Das Auditorium
Düsseldorf
16.4.2016

Ein kurzer Blick in die Geschichte:

Konrad Zuse (1910-1995)

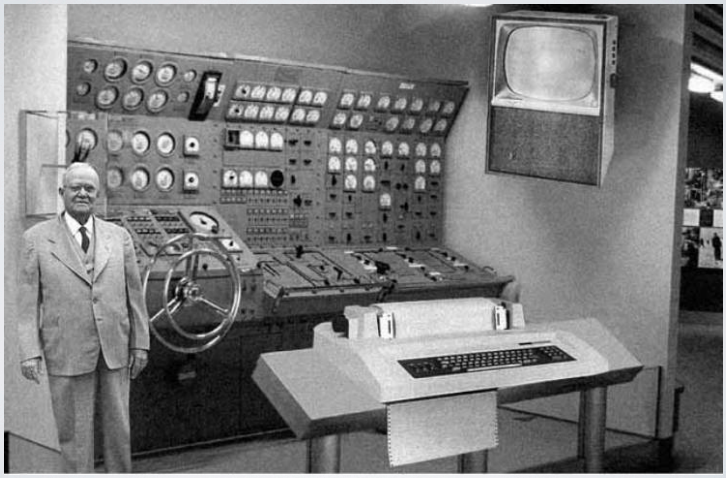
„Ich denke, dass es einen Weltmarkt für vielleicht fünf Computer gibt."

Thomas Watson, IBM-Vorsitzender, 1943

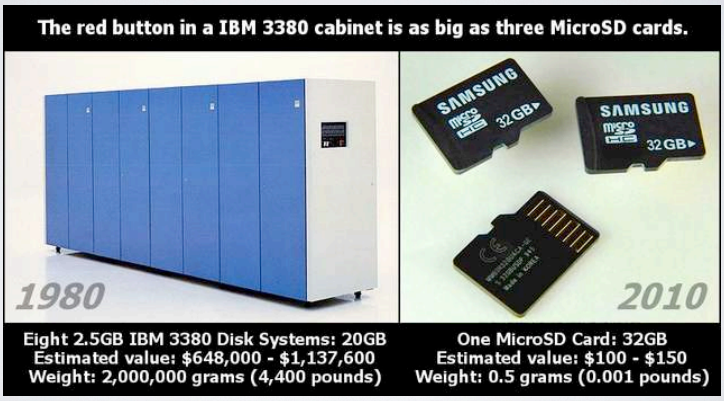
„Es gibt keinen Grund, warum irgend jemand einen Computer in seinem Haus wollen würde."

Ken Olsen, Vorsitzender und Gründer
der Digital Equipment Corp., 1977

So stellte man sich 1954 einen Heimcomputer vor:



30 GB Speicherplatz 1980 (3 Tonnen)
und 2010 (0,5 Gramm)



1982: der legendäre **Commodore64**.

64 kB Arbeitsspeicher.
Externes Cassetten- oder 5¼″-Disketten-Laufwerk.
Ca. 20 Millionen verkaufte Exemplare.

CERN, Genf, 1991:

Tim Berners-Lee präsentiert das "World Wide Web".

Und heute?

Nur *ein* Beispiel:

Estimated video upload to YouTube:
300 hours per minute.

Zwei grundsätzliche Deals:

1. NSA, GHCQ, etc:
Wir kriegen eure Daten.
Ihr kriegt Sicherheit vor Terroristen.

2. Google, Apple, Facebook, etc:
Wir kriegen eure Daten.
Ihr kriegt kostenlose, bequeme Dienste.

"There is no such thing as a free lunch."

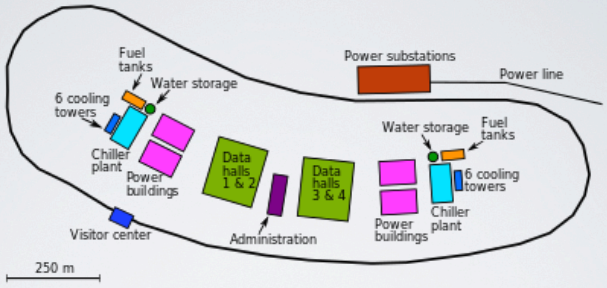
1. NSA, GHCQ, etc:
Wir kriegen eure Daten.
Ihr kriegt Sicherheit vor Terroristen.

Der Macht dieser demokratisch nicht mehr kontrollierbaren Institutionen haben wir wenig entgegenzusetzen.
Man kann es ihnen schwerer machen, aber im Grunde haben sie bereits gewonnen.

(US-Geheimdienste haben mindestens 80.000 meist höchstqualifizierte Mitarbeiter und ein jährliches Budget von wenigstens 55 Milliarden Dollar.)

NSA Data Center, Bluffdale, Utah

NSA Data Center, Bluffdale, Utah



Jede der beiden grünen Datenhallen misst ungefähr 140 x 160 m (≈2,2 ha).
(Sie erinnern sich: 0,5 g pro 30GB!)

"Grad bei den Amerikanern ist ein besonders starkes Gerede von Freiheit. Wie ich schon vorhin gesagt hab: es ist verdächtig. Damit einer von Freiheit redet, muß ihn der Schuh drücken. Von Menschen, die in gutem Schuhwerk herumgehn, werdens selten erleben, daß sie in einem fort davon reden, wie leicht ihre Schuh sind und wie sie passen und nicht drücken und daß sie keine Hühneraugen haben und keine dulden würden."

Bertolt Brecht,
Flüchtlingsgespräche

2. Google, Apple, Facebook, etc:

Wir kriegen eure Daten.
Ihr kriegt kostenlose, bequeme Dienste.

Hier geht schon eher was.
Aber es geht auf Kosten der Bequemlichkeit.

Privatsphäre:

"If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."

Eric Schmidt, CEO Google,
CNBC interview, 2009

quoted from:
https://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy

"Schmidt blacklisted CNET reporters from Google after [they] published an article with information about his salary, neighborhood, hobbies, and political donations -- all obtained from Google searches."

loc.cit.

Eines der 13 Google Datenzentren:

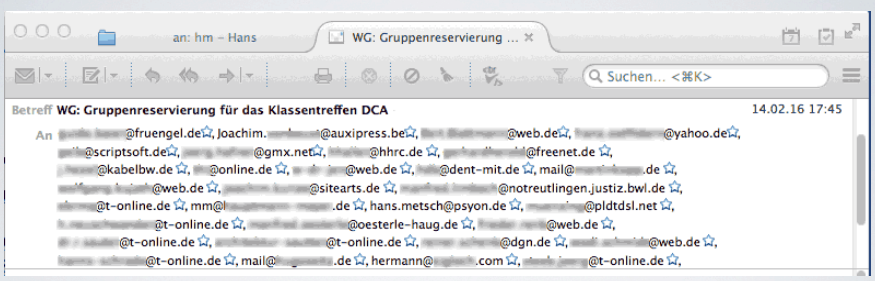
Ein paar praktische Hinweise.

"Vertraue auf Gott.
Und binde dein Kamel an."

Arabisches Sprichwort

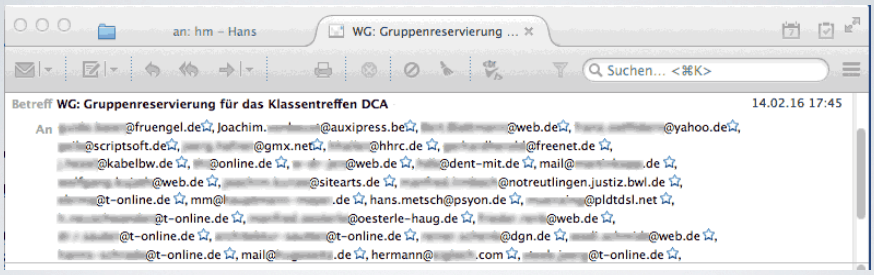
e-Mail

Kamel anbinden, Teil 1:



Das ist transparent. Keiner fühlt sich übergangen.

Alle wissen, wer dazugehört ...



... auch die Spammer.

Besser: e-mail an sich selber schicken; alle anderen Empfänger

BCC

Technisch z.B. folgendermaßen :

Richten Sie die BCC-Empfänger für eine Gruppe einmal ein, geben Sie die Empfänger (nur Namen) im Text an und speichern Sie es als "Vorlage". (Das geht ohne Adressbuch.)

Und...

Adressbuch
des Mail client
leer lassen.

Absolut keine e-mails
unbekannter Absender öffnen!

Z.Zt. grassieren "Erpressungs-Trojaner", die ihren gesamten Rechner verschlüsseln und ihn erst nach Lösegeldzahlung wieder freigeben!

Gehen Sie davon aus, dass Mails von Diensten wie
Googlemail (gmail)
auch inhaltlich ausgewertet werden.

Solche Dienste sind nur gut für *Junk-accounts*.

web.de, gmx und Telekom haben das Projekt

"e-Mail made in Germany"

zur Verschlüsselung von e-Mails.

Aber Vorsicht: Verschlüsselung nur zwischen e-Mail Server und Endgerät!

Auf dem gmx/web/Telekom-Server kommen die Mails unverschlüsselt an!

Es gibt aber inzwischen echte

Ende-zu-Ende-Verschlüsselung.

Threema (Schweiz)
Protonmail (Schweiz, CERN)

Server stehen in der Schweiz.
Keine physische Präsenz in den USA!

Seit neuestem ist auch **Whatsapp**
zuverlässig Ende-zu-Ende verschlüsselt !!

e-Mail
und
Schweigepflicht

Exkurs:

Telefon

Rufnummernunterdrückung
(Caller-ID)

www

"Surfen" im Internet heißt:

• Mittels eines **Browsers** wird eine Verbindung ins Netz hergestellt. Browser-Rangliste März 2016: Google Chrome (70%); Firefox (18%); Internet Explorer (6%); Safari (4%).

• Der Browser sendet an *alle* (!) direkt oder indirekt aufgerufenen Adressen einen **http-Header und weitere Daten**, holt die entsprechenden Seiten, und führt zur Darstellung der Seite die in ihrem Code enthaltenen Befehle aus (HTML, Javascript, PHP, usw.).

• Intern legt der Browser eine **History** aller besuchten Seiten an, speichert die von den Seiten abgelegten **Cookies** und sendet weiterhin Daten.

Gesendete Daten umfassen u.a.

- *IP-Adresse* (Internet-Protokoll; IPv4 vs. IPv6) (dynamische vs statische Zuweisung)
- *User agent*: Browser, Browser plugins (!), Details zum Betriebssystem, Browser-Einstellungen
- *HTTP Accept Header*: z.B Sprache des Betriebssystems.
- *HTTP Refer(r)er*: woher (von welcher Seite) kommt die Anfrage und wohin verlasse ich die Seite.

• ***Alle diese Daten werden von Google, Apple, Facebook und anderen dauerhaft gespeichert!***

Mein Laptop sendet auf diese Weise ca.**18 bit** an Unterscheidender Information.

Er ist damit unter 262.144 Rechnern (2^18) einzigartig und kann mit hoher Wahrscheinlichkeit (durch die lokale Zuweisung der IP-Adresse) identifiziert werden.

Um eine Million Rechner eindeutig und sicher zu unterscheiden, genügen 20 bit.

Sobald **IPv6** flächendeckend implementiert ist, genügt im Prinzip die IP-Adresse um *jedes* elektronische Gerät auf der Welt eindeutig zu identifizieren.

Das ist z.B. eine Voraussetzung für das "Internet der Dinge".

Sie können auch Ihren eigenen Rechner einmal testen:

Die *Electronic Frontier Foundation (EFF)*, eine gemeinnützige Stiftung zur Internet-Sicherheit stellt einen solchen Test bereit unter

https://panopticlick.eff.org/

Kamel anbinden, Teil 2

Tablets und Smartphones...

... erlauben nur sehr eingeschränkte Kontrollen durch den Anwender.

Das beginnt schon damit, dass man manche von ihnen nicht ausschalten kann ohne sie physisch zu zerstören. Man kann auch viele Apps nicht wirklich schließen.

In diesen Geräten sehen Hersteller die Zukunft. Sie minimieren die Einflussmöglichkeiten des Anwenders und **konditionieren** uns nach der Devise: *Don't worry, be happy*.

(Die Lerngesetze gelten auch für Psychologen).

Beispiele: Flugmodus
GPS

Schweigepflicht.

Ich würde deshalb davon abraten, irgendwelche Patientendaten auf diesen Geräten zu speichern.

Dasselbe gilt für die **Cloud**.
Es ist praktisch und bequem, alle Rechner durch Auslagerung von Dateien automatisch synchronisieren zu können.

Aber: man muss damit rechnen, dass alles, was durchs Netz läuft, im Prinzip kompromittiert ist.

Facebook, Twitter, Instagram, etc.
gehören zu den meistverwendeten Apps auf Tablets und Smartphones. (Facebook hat auch sonst Tracker auf jeder zweiten Seite und deshalb auf meinen Rechnern root-level Hausverbot).

Schweigepflicht. Sicherheitshalber schriftliche Zustimmung der Patienten bei Kontaktaufnahme oder Terminvereinbarung über diese Dienste.

... Soll man mit Patienten 'befreundet' sein? Soll man posts von ihnen lesen, 'liken' oder kommentieren? Soll man, wie es viele Software-Firmen anpreisen, mit der Praxis auf Facebook sein?

Bei "richtigen" Computern sieht die Lage etwas besser aus. Einige Empfehlungen:

• Zusätzliche Firewall (*ZoneAlarm, Little Snitch),* zur Überwachung der ein- und ausgehenden Verbindungen.

• Aktuelles(!) Virenschutzprogramm (auch für Macs!)

• Backups, backups, backups!
(Idealerweise externe Festplatte nach dem täglichen Backup vom Rechner trennen, sonst werden sie von der neueren "Ransomware" ebenfalls verschlüsselt.)

./.

• Passwörter:
"123456" ist kein Passwort. "Julia" auch nicht.

Ganze Sätze oder Formeln schon eher:
"E=m*c^2istvonEinstein".

Aktuelle Nachrichten zu Sicherheitsfragen gibt es — auch per RSS-Feed — bei

http://www.heise.de/security/

Schweigepflicht.

Die *sichere* Lösung:

Sie haben zwei Rechner.

Der Praxisrechner hat zu keiner Zeit irgendeine Außenverbindung.

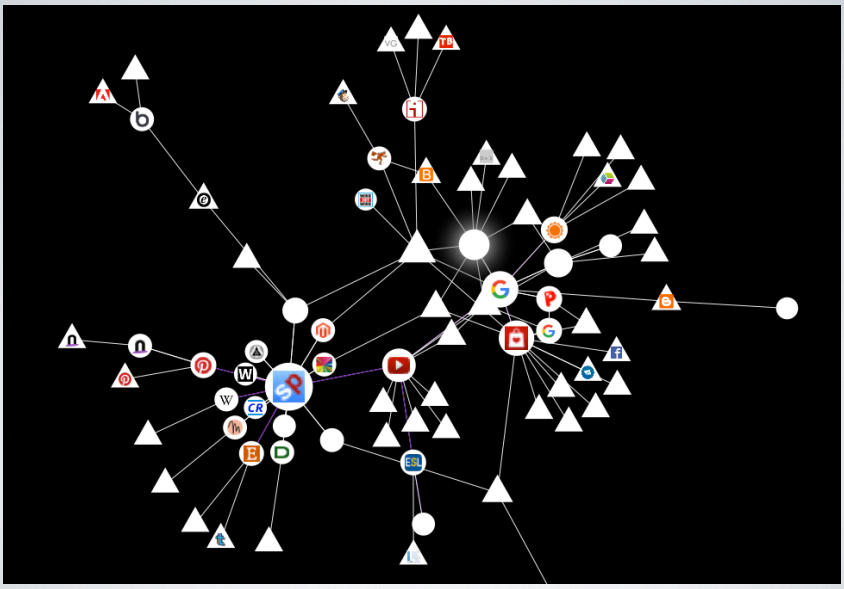
Schweigepflicht.

Die *akzeptable* Lösung:

Der Rechner ist einigermaßen gesichert.

Zweite Firewall, Virenschutz, sichere Passwörter und ein paar Einstellungen ("Tweaks") am Browser.

Schon nach kurzer Zeit im Internet sehen nämlich Verbindungen besuchter Webseiten *untereinander* ungefähr so aus:



Die wichtigsten Browser-Einstellungen
(am Beispiel Firefox):

- Adobe-Flash-Plugin sperren!
- Prüfen, ob eine sichere Verbindung (https via SSL) möglich ist und sie ggf. wählen.
  Dazu gibt es eine *Erweiterung: "HTTPS Everywhere".*
- *Javascript* nur selektiv erlauben. *("NoScript")*
- Werbung blockieren. *("AdBlock Plus")*
- Tracker blockieren. *("Ghostery")*

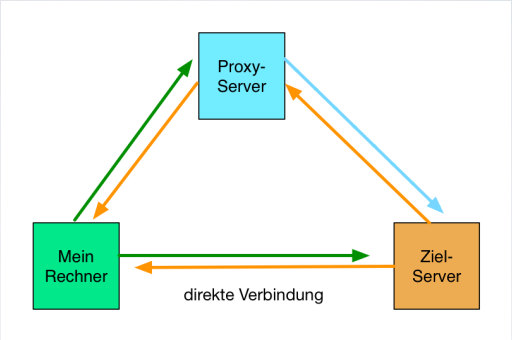
./.

die wichtigsten Browser-Einstellungen
(Forts.):

- Cookies und History beim Schließen des Browsers löschen oder "private browsing"-Fenster verwenden. Browser dann täglich schließen.
- Flash-cookies löschen *("Better Privacy")*.
- **Google nicht als Suchmaschine verwenden.**

Es gibt die europäische Alternative "**Startpage**", die zwar die Google-engine verwendet (und deshalb dieselben Ergebnisse liefert) aber keine Daten an Google sendet.
Startpage bietet auch einen **Proxy-Service**:

Proxy (Stellvertreter):



Der Proxy-Server sendet nicht *meine*, sondern *seine* Daten an den Zielserver.

Und schließlich: Wo geht's hin?

FOCUS (11/2016) brachte eine Titelgeschichte über Depression, in der von Pharmaka, Apps, Daten-Armbändern die Rede ist und Psychotherapie mit keinem Wort erwähnt wird.

- Es wird Video-Konsultationen geben *(NHK 3/2016)*.
- Es wird Gesundheits- und Forschungs-Apps geben, wie im Trailer gezeigt.
- Es wird online-Therapie geben.

Virtuelle Beziehungen sind möglich. Aber ist nicht die therapeutische Beziehung viel eher eine therapeutische *Bindung*? Gibt es virtuelle Bindung?

"But lo! Men have become the tools of their tools."

Henry David Thoreau,
Walden, 1854.

- Die Entwicklung wird weitergehen.
  Sie hat schon immer darauf beruht, dass wir unsere anfänglichen Bedenken ernst nehmen und einige dann doch in den Wind schlagen.
- Wir werden uns — und manche unserer Werte — dieser Entwicklung anpassen.
  Auch das war schon immer so.

"Es ist ganz wahr, [...] daß das Leben rückwärts verstanden werden muß. Aber darüber vergißt man den andern Satz, daß vorwärts gelebt werden muß."

Søren Kierkegaard,
Tagebücher

Ich danke Ihnen
für Ihre Aufmerksamkeit.