Crypto-Seminar
Fachhochschule Bielefeld

12. Dezember 2019

Digitalcourage e.V.

- Gemeinnütziger Verein für Datenschutz und Bürgerrechte
  - "Für eine lebenswerte Welt im digitalen Zeitalter"
  - Big Brother Awards
  - Aktionen zu aktuellen Themen

- Digitalcourage-Hochschulgruppe
  (www.digitalcourage.de/hsg)
  - CryptoPartys, Backup-Partys, Linux-Install-Partys
  - Regelmäßige Treffen an der Uni

CryptoParty

- Digitale Selbstverteidigung
- Schutz vor Massenüberwachung
- Einsteigerfreundlich
- Öffentlich, nicht-kommerziell, weltweit
- Von AnwenderInnen für AnwenderInnen
- Mach mit und werde Teil der CryptoParty-Bewegung

- https://cryptoparty.in

Das Seminar im Überblick

DONNERSTAG

- **Warum** sollte ich eigentlich **verschlüsseln**?
  - 14:00 bis 15:00
- **Browser**
  - 15:00 bis 16:00
- **Passwörter**
  - 16:10 bis 16:40
  - **PRAXIS BIS 18:00**

FREITAG

- Wie kann ich meine **E-Mails** verschlüsseln?
- Wie richte ich mein **Smartphone** sicher ein?

Welche Daten nutzt Facebook?

- Ort; Alter; Geschlecht; Bildungsniveau; Einkommen und Eigenkapital;
- Hausbesitz und Hauswert; Grundstücksgröße; Hausgröße in Quadratmetern;
- Nutzer, die frisch verheiratet sind; Beziehungsstatus;
- Nutzer, die planen, ein Auto zu kaufen (welche Art/Marke, und wann);
- Betriebssystem, Emailanbieter, Art der Internetverbindung;
- Nutzer, die Browserspiele spielen;
- Nutzer, die eine Facebook-Veranstaltung erstellt haben;
- Anzahl der Kredite;
- Nutzer, die aktiv eine Kreditkarte benutzen;
- Arten von Kleidung, die der Haushalt des Nutzers kauft;
- Die Zeit im Jahr, in der der Haushalt des Nutzers am meisten einkauft;
- Nutzer, die „sehr viel“ Bier, Wein oder Spirituosen kaufen;
- Nutzer, die Medikamente gegen Allergien und Schnupfen/Grippe,
- Schmerzmittel und andere nicht-verschreibungspflichtige
- Arzneimittel einkaufen;
- Nutzer, die „empfänglich“ [sind] für [Werbung zu] Online-
- Autoversicherungen, Hochschulbildung oder Hypotheken, Prepaid-
- Debitkarten und Satellitenfernsehen;
- Wie lange der Nutzer sein Haus bereits bewohnt;
- Nutzer, die wahrscheinlich bald umziehen;
- etc.

Privatsphäre

Privatsphäre – was ist das?

- "Privat ist etwas genau dann, wenn man den Zugang dazu kontrollieren kann." (Rössler, 2001)

Quelle: Rössler, Beate (2001): Der Wert des Privaten. Frankfurt: Suhrkamp

Warum brauchen wir Privatphäre?

- „The right to be left alone.“
- Freie Entfaltung der Persönlichkeit
- Kontrolle über die Folgen des eigenen Handelns
- Selbstbestimmung (wer weiß was von mir)
- Schutz vor Kritik und Diskriminierung
- Sicherheit (Passwörter, Eigentum, ...)
- Freiheit
- Intimität?
  - **WICHTIG FÜR DAS INDIVIDUUM**

Warum brauchen wir Privatsphäre?

- Wichtig für die Gesellschaft:
- Essentiell für Demokratie und Rechtsstaat:
  - Verschwiegenheitspflicht (Medizin, Recht, Beratung, ...)
  - Journalismus (Quellenschutz)
  - Abwehrrecht gegen die Staatsmacht
- Soziale Rollen (unterschiedliches Verhalten)
- Fortschritt ermöglichen (Opposition zulassen)
  - Sobald Offenlegung sich zur sozialen Norm entwickelt, wird das Gegenteil zum Stigma
  - **WICHTIG FÜR DIE GESELLSCHAFT**

Was ist, wenn die Privatsphäre verletzt wird?

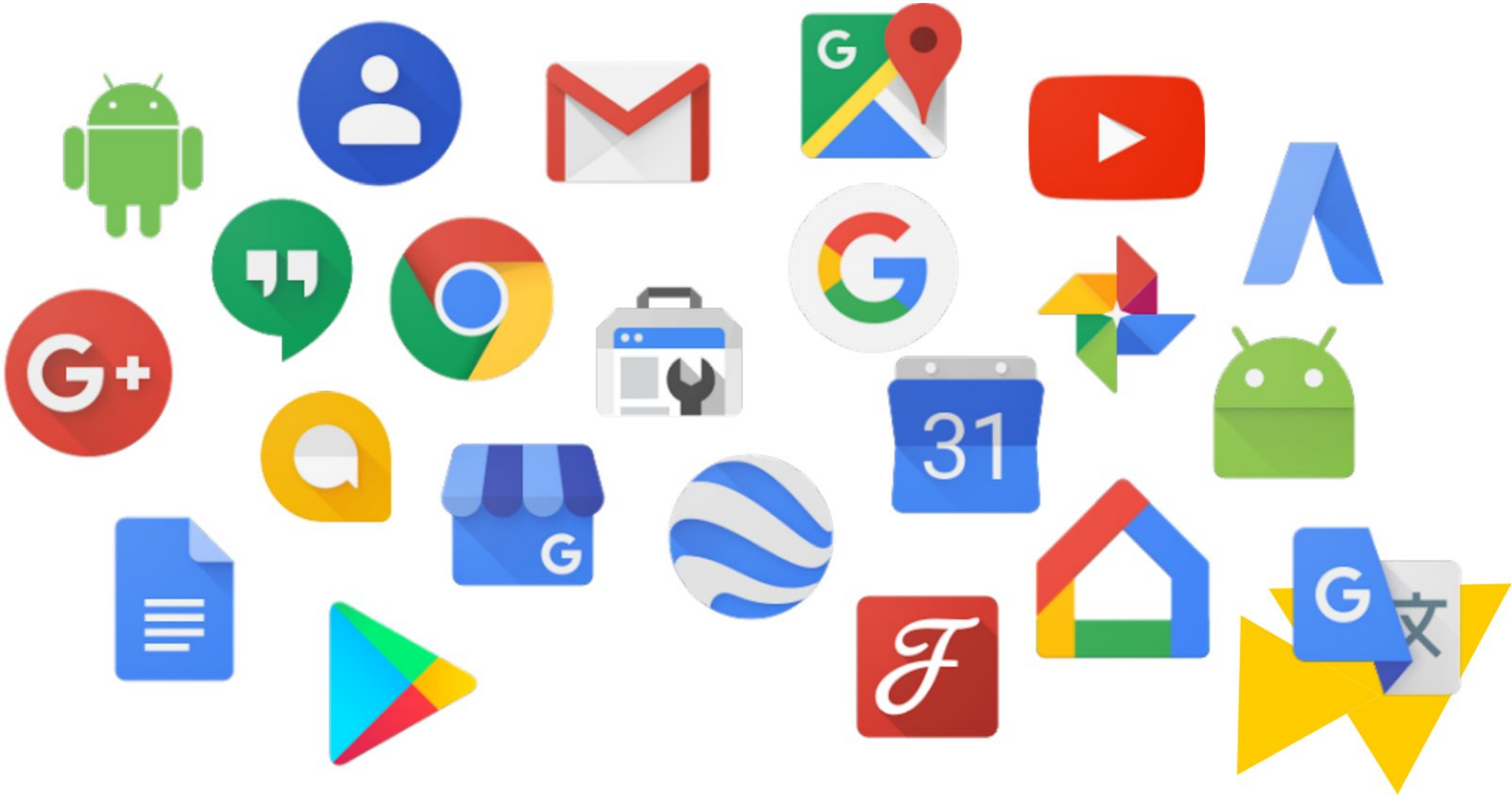
- Erpressbarkeit
- Chilling Effects

Privatsphäre

- **Analog**
  - Privatsphäre selbstverständlich akzeptiert
  - Einbrüche in Privates meist erkennbar
  - Gesetze zum Schutz der Privatsphäre
    - Unverletzlichkeit der Wohnung
    - Briefgeheimnis
    - Freie Entfaltung der Persönlichkeit
- **Digital**
  - Neuer Wirtschaftsraum
  - Neue technische Mechanismen / Möglichkeiten
  - Intransparente Datenerhebung und -nutzung
  - Technisches Verständnis häufig notwendig
  - Datenschutzgesetze nicht zeitgemäß, #neuland

Digitale Identität

Google-Dienste



Zu niemandem ist man ehrlicher als zum Suchfeld von Google.

Constanze Kurz, Chaos Computer Club

Was weiß Google?

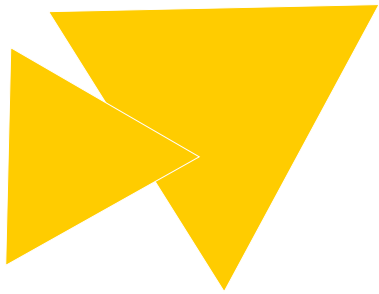
- Suchbegriffe (Search History)
- eingegeben, gesehen, angeklickt
- IP-Adresse
- Sprache
- Datum, Uhrzeit
- Gerät, Betriebssystem, Browser
- Standort (GPS oder Browser)
- https://myactivity.google.com/

Google Analytics

- Einbindung auf der Webseite
- Statistiken für die Betreiber der Webseite
- Tracking der Besucher beim Seitenaufruf
  - IP-Adresse, Sprache, Land
  - Datum, Uhrzeit
  - Gerät, Betriebssystem, Browser
  - Bildschirmauflösung
  - Referer (von welcher Webseite gekommen)

Datenwirtschaft

- "Kostenlose" Angebote
  - Daten sind eine neue Währung
  - Datenhändler kaufen Profile und verkaufen sie an die Werbeindustrie, Versicherungen, Schufa, etc.
- Geschlossene Systeme
  - Proprietäre Software
  - Keine offenen Schnittstellen
- Big Data
  - Zusammenführung, Analyse und Auswertung großer Datenmengen



Datenwirtschaft

- Sicherheit
  - Bedeutet Aufwand = Kosten
- Datenschutz
  - Weniger Daten für das Unternehmen
  - Weniger Rohmaterial zum Analysieren und Verkaufen
  - Privatsphäre "überholt"?

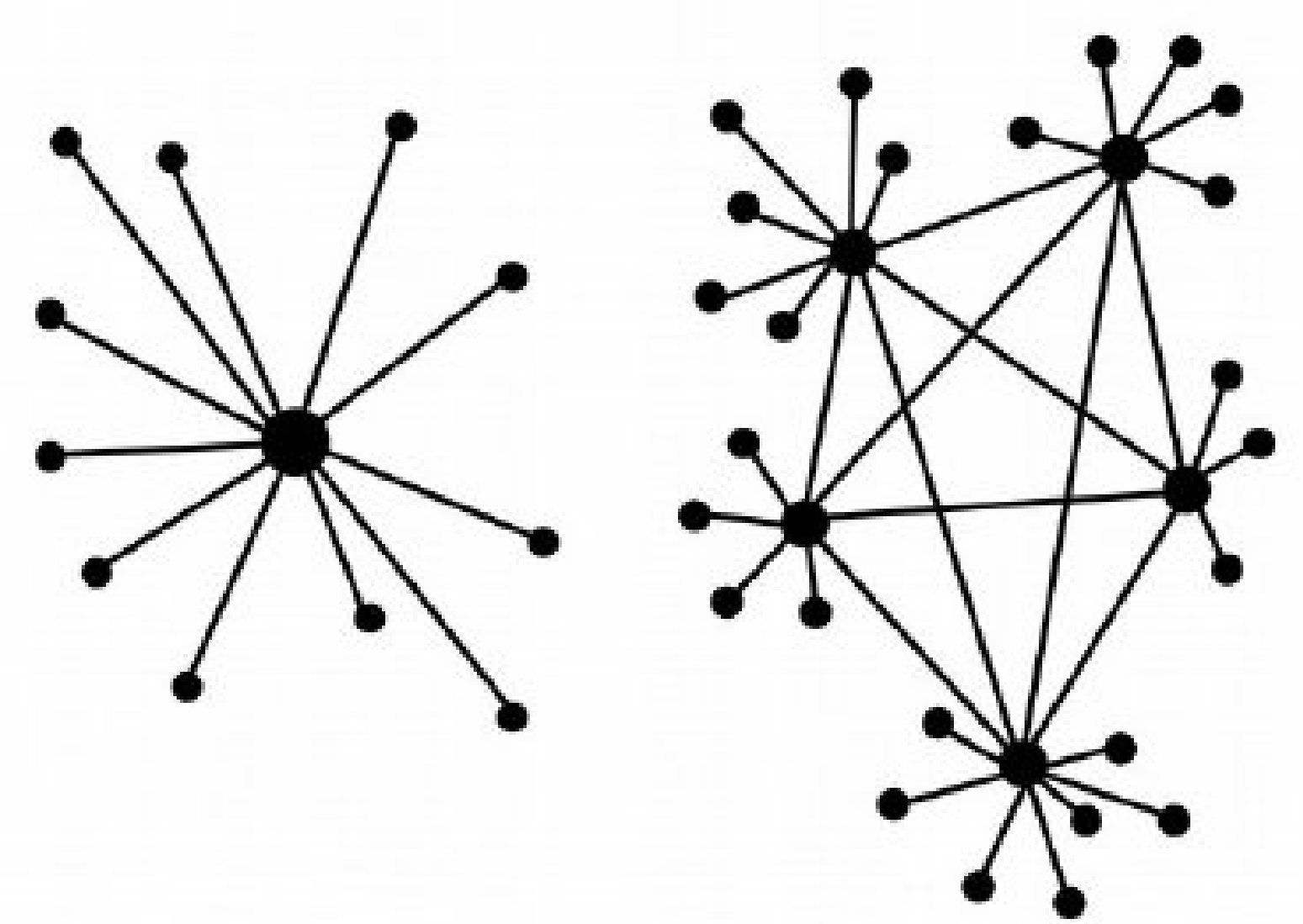
Facebook is watching you!

- Big Brother Award 2019 and *ZEIT ONLINE*, stellvertretend für rund 3/4 aller Onlinezeitungen

Name	Startseite	Artikelseite	Aboseite
FAZ	?	?	?
Handelsblatt	?	?	?
taz	✔	✔	✔
Neue Westfälische	✔	✔	✔
Westfalen-Blatt	✔	✔	✔

Quelle: https://netzpolitik.org/2019/konzern-liest-mit-facebook-trackt-nutzer-auf-drei-viertel-aller-deutschen-nachrichtenseiten/

Zentral vs. dezentral



Begriff: Metadaten

- Inhalt
- Metadaten (Nachricht)
  - Absender, Empfänger
  - Datum, Uhrzeit
  - IP-Adresse / Mobilfunknetz
- Metadaten (Foto)
  - Auflösung
  - Blende, Belichtungszeit
  - GPS Koordinaten

Metadaten

- In der Telekommunikation häufig Verbindungsdaten genannt.
- Kleine Datenmenge
- Leicht zu analysieren (im Gegensatz zu Inhalt)
- Schwierig zu verschlüsseln, da notwendig um die Kommunikation zu ermöglichen
- **Metadaten eignen sich perfekt zur Datenanalyse und Massenüberwachung!**

Metadaten – wo ist das Problem?

- **Kleine Datenmenge, aber sehr viel Wissen** über Nutzer.innen:
  - Interessen, Krankheiten, sexuelle Vorlieben, Bewegungsprofil, ...
- Leicht zu **analysieren** (im Gegensatz zu Inhalt)
- **Zusammenführung** von Daten verschiedener Quellen
  - Suche, YouTube, Gmail, Analytics, AdWords, Android,...
- **Big Data**: Suchtrends (regional, weltweit)
- **Datenhandel**: Werbung, Kreditwürdigkeit, Versicherungen...
- Schwierig zu verschlüsseln, da **notwendig** um die Kommunikation zu ermöglichen

We Kill People Based on Metadata

General Michael Hayden, Ex-Chef von NSA und CIA

Vorratsdatenspeicherung (Historie)

- 2006: EU-Richtlinie
  - Nach und nach von vielen Mitgliedsstaaten umgesetzt
- 2010: Vom Bundesverfassungsgericht als verfassungswiedrig erklärt
- 2014: Vom EuGh wegen Verstoß gegen die Charta der Grundrechte als ungültig erklärt

VDS-Zombie

- 2015 vom Bundestag beschlossen als:
  - „Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten“.
- Anfang 2017: Bundesverfassungsgericht lehnt Klärung im
- Eilrechtsschutzverfahren und Aufschub ab.
- Verfassungsbeschwerden laufen

Neusprech Award 2015

- Vorratsdatenspeicherung
- Mindestspeicherfrist, Mindestspeicherdauer
- Mindestdatenspeicherung
- Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten
- Private Vorsorgespeicherung
- Digitale Spurensicherung

VDS: Wer speichert?

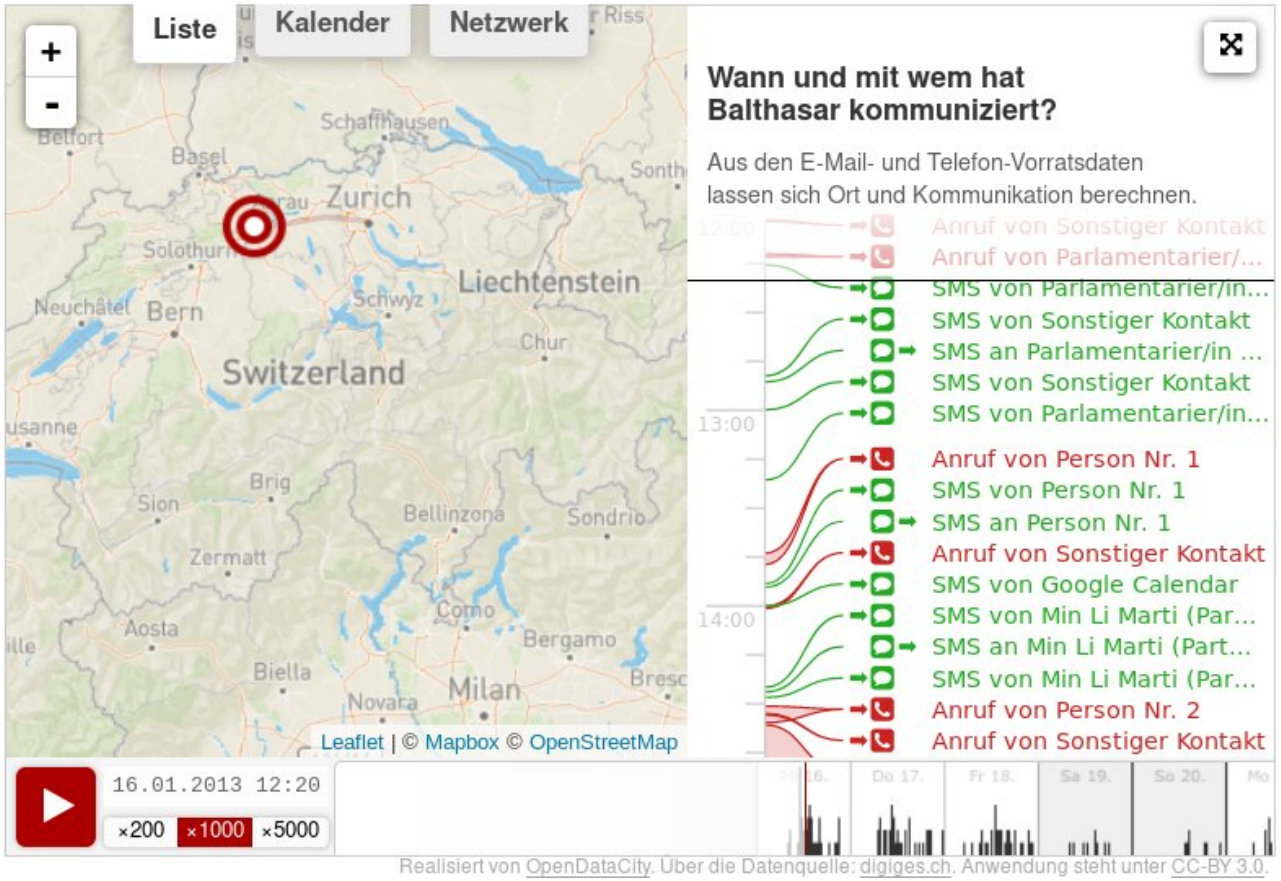
- Telekommunikationsanbieter
  - ISP (Internet-Service-Provider) & Mobilfunkanbieter
  - Outsourcing: VDS as a Service
- Polizeibehörden fordern Daten zur Aufklärung "schwerer Straftaten" an.

VDS: Was wird gespeichert?

- Standortdaten aller Mobiltelefonate bei Beginn des Telefonats (für 4 Wochen)
- Standortdaten bei Beginn einer mobilen Internetnutzung (für 4 Wochen)
- Rufnummern, Zeit und Dauer aller Telefonate (für 10 Wochen)
- Rufnummern, Sende- und Empfangszeit aller SMS-Nachrichten (für 10 Wochen)
- Zugewiesene IP-Adressen aller Internetnutzer sowie Zeit und Dauer der Internetnutzung (für 10 Wochen)

VDS Visualisierung

- Balthasar Glättli (Grüne, Schweiz): https://www.digitale-gesellschaft.ch/vorratsdatenspeicherung/
- Malte Spitz (Grüne, Deutschland): http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten



Telekommunikationsüberwachung 2015 nach Straftatbeständen

Quelle: https://netzpolitik.org/2015/statistiken-zur-telekommunikationsueberwachung-telefon-und-internet-ueberwachung-weiterhin-meistens-wegen-drogen/

VDS: Ausweitung

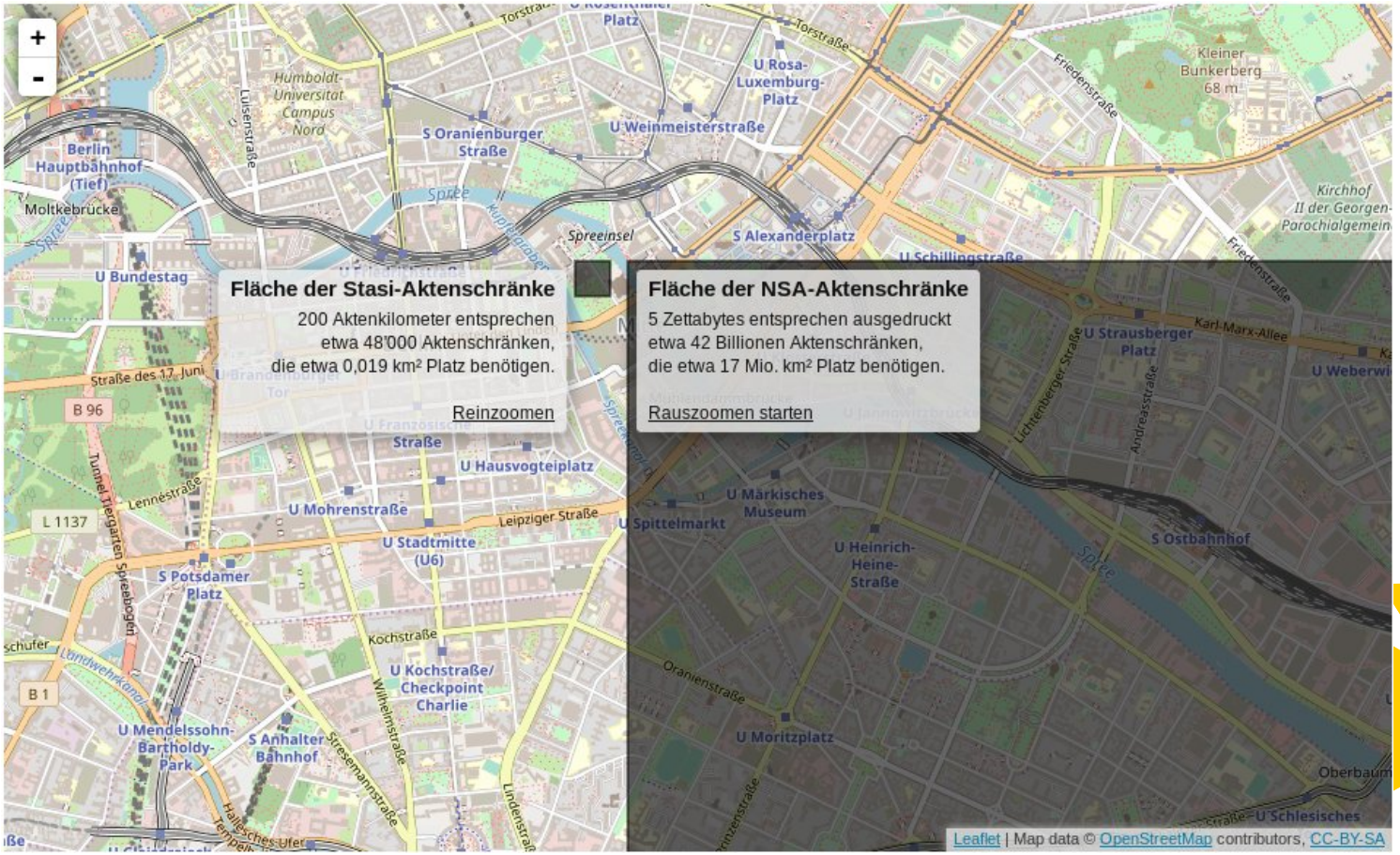
- Schon vor in Kraft treten des Gesetzes
- Vorratsdaten auch bei Wohnungseinbrüchen abfragen
- Zusätzlich Funkzellenabfrage
- Kritik: Technik erst etablieren, dann ausweiten

Folgen von Massenüberwachung

- Alle Bürger sind Verdächtige
- Schere im Kopf → Selbstzensur
- Chilling Effect → Angepasstes Verhalten
- Einschränkung vieler Grundrechte:
  - Meinungsfreiheit,
  - Briefgeheimnis,
  - Freie Entfaltung der Persönlichkeit

Massenüberwachung durch die NSA

- Stasi vs. NSA Flächenvergleich: https://apps.opendatacity.de/stasi-vs-nsa/



Leseempfehlungen

- https://netzpolitik.org
- Buch: "Die globale Überwachung" (Glenn Greenwald)
- Buch: "Was Google wirklich will" (Thomas Schulz)
- Videos: http://www.alexanderlehmann.net/

Freie Software

- **Freiheit 0**: Die Freiheit, das Programm auszuführen, wie man möchte, für *jeden Zweck.*
- **Freiheit 1**: Die Freiheit, die Funktionsweise des Programms zu untersuchen und eigenen Bedürfnissen der Datenverarbeitung anzupassen.
- **Freiheit 2**: Die Freiheit, das Programm weiterzuverbreiten und damit seinen Mitmenschen zu helfen.
- **Freiheit 3**: Die Freiheit, das Programm zu verbessern und diese Verbesserungen der Öffentlichkeit freizugeben, damit die gesamte Gemeinschaft davon profitiert.
- ⇒ Viel mehr als Open Source (offenlegen der Quelltexte)