

Angelehnt an:



<https://www.cryptoparty.in/berlin>

Krypto- party

Humanistische Akademie
27.4.2018
Berlin



Willkommen zu digitale Kompetenzen

mit



Xrs

(Chaos Computer Club)

ccc.de

&



Rainer Rehak

(Forum InformatikerInnen für Frieden und
gesellschaftliche Verantwortung)

fiff.de

Agenda

- Digitale Kompetenzen
Vortrag, Workshop und Kryptoparty
- Unser Input
- Eure Fragen
- Geräte auf die Tische und los

Komplexe Welt

- Wem vertrauen und warum?
- Beispiele: Nahrungsmittel, Banken und Kleidung
 - Bio, gesund?
 - Zutaten, Produktionsketten?
 - Soziale Aspekte, faire Herstellung?
 - Welche Werte werden vertreten und umgesetzt?
 - Neues Produkt → neue Recherche nötig

Komplexe Welt II

- Wem vertrauen und warum?
- Medien, Quellen, Informationen
 - Wer sind AutorInnen?
 - Herkunft der Informationen/Quellen?
 - Werden Texte teilweise automatisiert erstellt?
 - Sind es große Verlage oder kleine Blogs?
 - Umgang mit Falschmeldungen?
 - Welche Werte werden gelebt und verbreitet?

Komplexe Welt III

- Wem vertrauen und warum?
- Nun: Software/Services
 - Wer steckt dahinter?
 - Wie und wo wurde/n sie erstellt?
 - In Zusammenarbeit mit wem?
 - Was wird gespeichert und wozu verarbeitet?
 - Welche Werte werden umgesetzt?
 -

Urteilkraft

- Feste Regeln zur Beurteilung?
- Urteilkraft ist wesentliche Voraussetzung
- Freiheitsgrade zum Handeln erkennen
- Konsequenzen abschätzen (auch für andere)
- Digitalisierung schreitet fort
 - Kann gestaltet werden, aber Freiräume müssen vermessen und erstritten werden
- Informiert sein und vertrauen
- Bedingungen für Zugang zu Wissen reflektieren
- Große Dynamik → stetiges Lernen (lebenslanges Lernen)
 - Geschulte Sicht essentiell

Urteilstkraft II

- Virulent bei Allgegenwart Algorithmen, „künstlicher Intelligenz“
- automatisierte Entscheidungsproduktion
- Gegenseitige Abhängigkeit
 - Autonomie und Arbeitsteilung
 - Selbstbestimmung und Vernetzung
- Digitalisierung ist Werkzeug, aber wozu?
 - Fesselung durch Vernetzung (Abhängigkeit, Monotonie, Zentralität) ODER
 - Befreiung durch Vernetzung (Umstände wählen können, Alternativen nutzen, Dezentralität fördern)

Clara möchte ihre Fotos in die Cloud laden und überall darauf zugreifen können.



Monika und Hannes jedoch nicht, doch sie wissen davon nichts.

Frank möchte seine E-Mails von überall aus lesen können und speichert sie bei einer großen Firma zu deren komplexen Bedingungen.

Webmail

SCHREIBEN

Posteingang (6)

Markiert

Wichtig

Chats

Gesendet

Entwürfe

Alle Nachrichten

Spam (3)

Papierkorb

Anmelden

Nach deiner Anmeldung in Hangouts bist du in allen Hangouts-Clients auf Google angemeldet.

Weitere Informationen

Klick zum alten Chat-Client

Allgemein

Soziale Netzwerke 32 neu
YouTube; Google+ Team; Google+

Werbung

Folge 6 - Invitation to edit - ... has invited you to edit the

Folgen-Manuskripte - Invitation to collaborate - ...

Eine_Serie_Autoren - Invitation to collaborate - ... has in

Eine_Serie_Autoren - Invitation to collaborate - ...

Google Places heißt jetzt Google My Business. Entdecken Si

behrang.alavi@gmail.com hat einen Kalender für Sie freige

Invitation of your friend ! - Do you think that this email is a spam ?

Gmail-Update: Erreichen Sie mehr Menschen in Ihrem Bekanntenl

0 GB (0 %) von 15 GB belegt
Verwalten

Nutzungsbedingungen - Datenschutz

Seine Kommunikationspartner jedoch nicht unbedingt, doch sie können nichts dagegen tun.

Franziska steuert ihr SmartTV gern per Stimme, auch wenn die Stimmverarbeitung auf fernen Servern geschieht.



Ihre Freunde wissen noch nicht einmal, dass die Gespräche aufgezeichnet werden.

Johanna ist stolz auf ihr neues Auto, dessen Assistenzsystem selbständig die Fahrzeuge vor und hinter ihr "im Blick" behält und über die Cloud Verkehrsoptimierung macht.



Bert und seine Familien wissen weder, dass ihr Auto gescannt wird noch von wem.

Selbstbestimmung

- Ist also gesellschaftliches Problem, kein individuelles
 - technisch konkrete Frage nach individuelle wie kollektiver Selbstbestimmung
 - noch konkreter: Welche Techniken/Services/Software sollte genutzt werden, welche nicht
 - Regulierung, um Mindeststandards zu gewährleisten

Eigenschaften eines Extrems

- Google Mail/Docs
 - AGB gelesen?
 - Andere mit beeinflusst
 - Offenbarung gegenüber Google
 - Ggf. keine individuelle Entscheidung möglich
- Facebook („soziale Medien“)
 - AGB gelesen?
 - Offenbarung gegenüber Facebook
 - Direkt manipulierbar (Freude-Experiment, Cambridge Analytica, sexuelle Orientierung errechnen, transparente Gesellschaft für Facebook, Suicid-Ffälle)

Eigenschaften eines Extrems

- GoogleYoutube/Maps
 - nach deren Regeln konsumieren
 - „Nudging“ (Beispiel: Netflix)
 - kostenlos, aber nach Gnade der Firma
 - Macht zur (undemokratischen) Zensur
 - Aushebelung von Quellen kritischer Urteilsbildung?
 - Aktuelle Situation: LohnsklavInnen in Bangladesch oder KI als content moderation
 - kulturelle Unterschiede, kultureller Kolonialismus
 - abhängig, ausgeliefert?
 - bequem aber fremdbestimmt?

Überlegungen des anderen Extrems

- Dezentralität
 - Lokale Autonomie
- bestimmte Formen der Anonymität als Selbstbestimmung
 - wesentlich: Anonymität gegenüber wem?
- Fallbeispiel: Petitionskommentare mit/ohne Namen
- Fallbeispiel: Whistleblower/Hinweisgeber
- Pluralität von Nachrichtenmedien
 - Wissensallmende, nicht-kommerzielle

Überlegungen eines anderen Extrems

- Offene Quellcodes, freie Software
 - „Software respektiert die Freiheit der NutzerInnen“
 - Programmierte Selbstbestimmung?
- freie Internet-Services
 - offen, frei, Datenschutz, sogar nachhaltig, grün?
- Alternative Vertrauensnetze
 - nach freiheitlichen Idealen gestaltete Software

Konkretes Urteilen

- Urteil über:
 - Wahl des kommunikationswerkzeugs betrifft familie, freunde und bekannte
 - Wahl der kommunikationsart betrifft jeden (solange ethische standards der technik nicht umgesetzt sind)
- Wert des Andersseins, und Anders-sein-könnens
 - Handlungsalternativen aufrecht erhalten
 - Monopole

- Beispielhaft: Google Mail
- Frage in die Runde: Wer nutzt das?

Exemplarische Fragen

- Was will die Software von mir/von anderen?
- Wer macht die Software?
- Welche Motivation steckt dahinter?
- Mit welchen Mitteln wird sie umgesetzt?
- Welche Daten liegen dort?
- Wie/Wofür werden diese Daten genutzt?
- Was passiert mit dem verdienten Geld/was passiert damit nicht?
- Wie agiert der Hersteller in der physischen Welt?

Differenzieren

- Übung in Pädagogik und Kompetenz
- Paranoia-Skala ist nach oben offen
 - NSA
- Differenzen und Differenzierung aushalten
 - Es gibt Gewissheiten, aber wieviele?
 - Tor, Mathematik, Transparenz
 - Hohe Authentizität und (ethische) Integrität von Akteuren

Freie Software

- Nur freie Software ist perspektivisch sinnvoll, respektiert den Selbstbestimmungswunsch der Menschen
 - 0 Ausführen
 - 1 Analysieren
 - 2 Ändern
 - 3 Verbreiten
- Auch die kollektive Selbstbestimmung, Allmende, Wissen

Es gibt Alternativen!

- Whatsapp/Facebook Chat?
 - Signal Messenger !
- Google Mail?
 - Posteo.de !
- Klartext Emails ohne Herkunftsnachweis?
 - PGP nutzen !
- Smarte IoT-Geräte meiden
 - Wirklich! Das Zeug ist (bislang) totaler Mist!
- <https://berlin.fiff.de/kryptoparty2704.html>

Erste Schritte

- Browser
 - Nutze Firefox, nicht Safari oder den Internetexplorer (die sind nicht frei, telefonieren nach Hause und sind wenig konfigurierbar)
- Firefox-Add-ons:
 - „Self-Destroying Cookies" (über Extras → Add-ons, Cookies werden gelöscht, wenn man die jeweilige Seite verlässt)
 - „Adblock Edge" (über Extras → Add-ons, Werbeflexer ohne Ausnahmen)
 - „HTTPS-Everywhere" (immer auf die verschlüsselte Version von Webseiten umleiten) <https://www.eff.org/https-everywhere>
 - „Privacy badger". Blockiert aktive Trackingelemente auf Webseiten (Socialnetworks, Werbung)
- Suchmaschine
 - Metager (Deutsches Produkt aus einer Uni)
 - Startpage.com (anonymisiert Googleanfragen)

Erste Schritte II

- Mobile Kommunikation
 - Nutze Signal, statt Whatsapp/Threema/Telegram/usw. freie, sichere und damit diskutierbare Software, Snowden, Aménsty,
- Mailprovider:
 - Nutze kleinere Mailprovider, die eine Haltung haben, z.B. posteo.de uberspace.de, so36.net oder riseup.net
- Tor-Browser-Bundle (ein modifizierter Firefox inklusive aller nötigen Add-ons, der über das Anonymisierungsnetzwerk Tor läuft)
 - <https://www.torproject.org/download/download-easy.html>

Kryptoparty

- Kommunikation verschlüsseln
 - Sich und andere schützen
 - Solidarität mit Unbekannten/Schwächeren
- Technisches Konzept: Öffentliche/private Schlüssel
- Mobil: Signal-Messenger
- E-Mail: PGP-Verschlüsselung
 - Thunderbird, GnuPG, Enigmail

Links

- Notizen und Hinweise
<https://berlin.fiff.de/kryptoparty2704.html>
- Alexander Lehmanns Lehrfilme
missing link
- Mehr Cryptoparty?
<https://www.cryptoparty.in/berlin>
- FIFF
<https://www.fiff.de>
- CCC
<https://berlin.ccc.de>



Danke