FreieSoftwareOG –

10 Privatsphären-Probleme - (die oft übersehen werden)*

* mit einem 15-Folien-Vorwort...

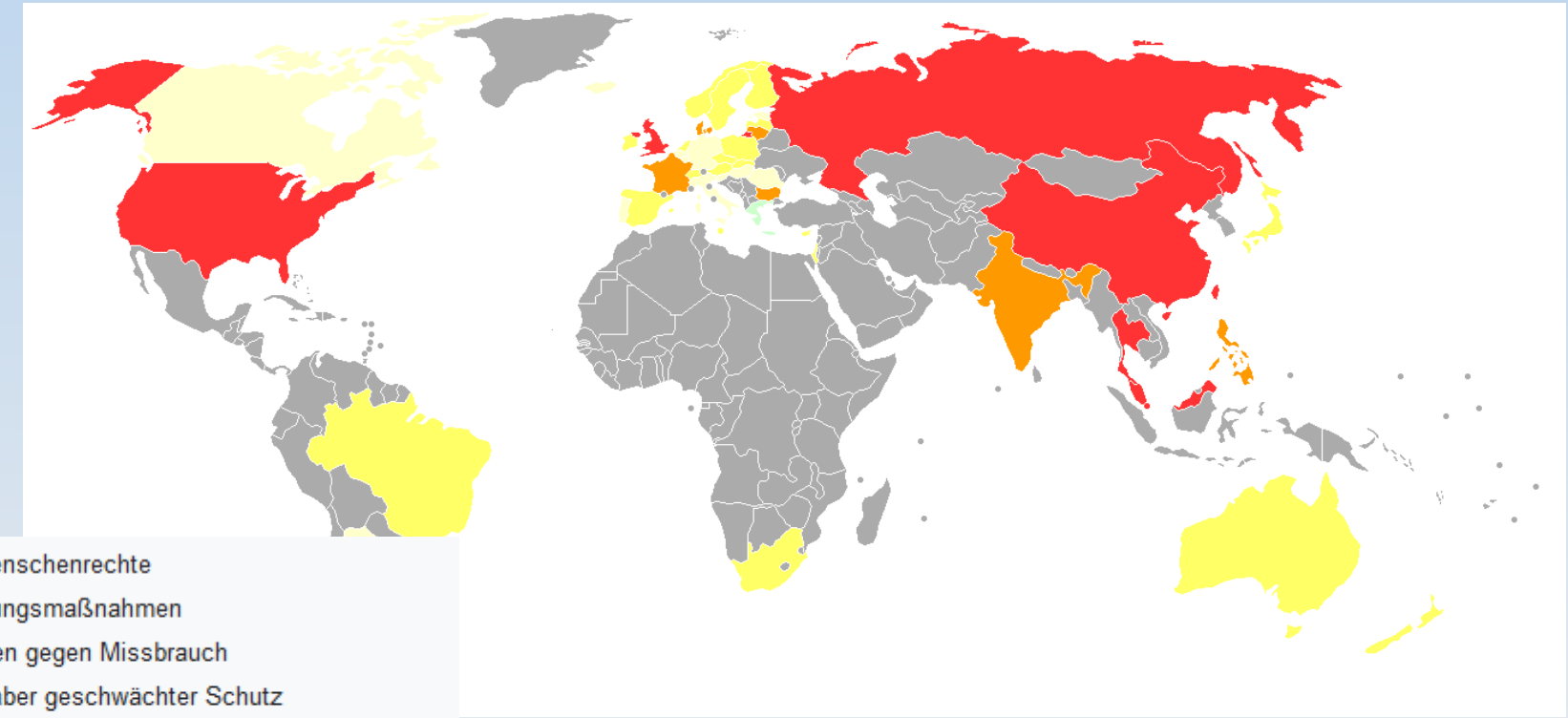
Privatsphäre – Begriffserklärung

Wikipedia:

„Privatsphäre bezeichnet den nichtöffentlichen Bereich, in dem ein Mensch unbehelligt von äußeren Einflüssen sein Recht auf freie Entfaltung der Persönlichkeit wahrnimmt.
Das Recht auf Privatsphäre ist als Menschenrecht in allen modernen Demokratien verankert. […]“

Privatsphäre – Begriffserklärung

Privacy Ranking 2007



- Konsistente Hochhaltung der Menschenrechte
- Signifikanter Schutz und Sicherungsmaßnahmen
- Adäquate Sicherungsmaßnahmen gegen Missbrauch
- Einige Sicherungsmaßnahmen aber geschwächter Schutz
- Systematisches Versagen die Sicherungsmaßnahmen aufrechtzuerhalten
- Verbreitete Überwachungsgesellschaften
- Endemische Überwachungsgesellschaften

Privatsphäre – Begriffserklärung

Internet Privacy Ranking 2022

Internet Privacy Ranking

Search:

Rank	Country	Privacy Score
1	Norway	90.1
2	Australia	89.1
3	Denmark	87.4
4	Sweden	85.2
5	Finland	83.6
6	Germany	83.3
7	Canada	81.8

Privatsphäre – Begriffserklärung

Neue Technologien haben dazu geführt, dass heute ein Verlust an Privatsphäre durch viele moderne „Errungenschaften“ wie z. B. Mobiltelefone, Bankkarten und Kreditkarten zu beklagen ist.
Oft ist es kaum möglich, vielen der nahezu omnipräsenten Überwachungstechnologien zu entgehen.
In diesem Zusammenhang werden folgende Beispiele genannt:

Privatsphäre – Begriffserklärung

- Client-Side-Scanning
- RFID
  - in Ausweisdokumenten
    (z.B. Reisepass, Elektronische Gesundheitskarte)
  - im menschlichen Körper als Ausweisdokument
- Bonussysteme
- genetischer Fingerabdruck, Daktyloskopie (Fingerabdruck)
- Gesichtserkennung

Privatsphäre – Begriffserklärung

- Iris-Erkennung
- Lifescan, Bewegungsprofile
  - durch satellitenbasierte PKW-Maut
  - durch automatische Kfz-Kennzeichenregistrierung (Zeichenerkennungssoftware)
  - durch städtische Gesichtserkennungssysteme (London/Peking)
  - durch Mobiltelefonortung (Sendemasten, GPS, stille SMS, Apps etc.)

Privatsphäre – Begriffserklärung

- TCG-Chips auf PC-Hauptplatinen (ehemals TCPA)
- Internetüberwachung
  - E-Mail-Überwachung
  - Analyse sozialer Netzwerke
  - Vorratsdatenspeicherung der Verbindungsdaten bei Providern
  - Cookies
  - durch Webcams

Privatsphäre – Begriffserklärung

- Internetüberwachung (fortgesetzt)
  - Verbindungen zu Drittseiten
    (Analyse, Soziale Netzwerke, Werbung etc.)
  - Browserprofile (Canvas Fingerprinting)
  - MAC Adressen („Seriennummer“ der Netzwerkkarte)

Privatsphäre – Begriffserklärung

- Viele Internetdienste und Technologien konvergieren
- Vergleichsweise strikte europäische Standards werden oft durch ausländische Firmen umgangen.
  Z.B. erlauben es viele Nutzer von sozialen Netzwerken wie Facebook, ihr E-Mail-Konto oder iPhone zu durchsuchen, um Freunde und Bekannte automatisch zu finden.
- Käufe bei Amazon können automatisch dem Facebook-Freundeskreis empfohlen werden.

Privatsphäre – Begriffserklärung

- Software erlaubt es inzwischen, Handy-Fotos automatisch mit Profilen aus sozialen Netzwerken zu verknüpfen.
- Für den Zugang zu sehr vielen Bereichen, auch zu behördlichen Diensten wie der Bundesagentur für Arbeit, wird eine E-Mail-Adresse benötigt.
- Internetdienstleister gehen zunehmend dazu über, persönliche Daten von Benutzern mit solchen zu verknüpfen, die diese nicht selber eingegeben haben.

Privatsphäre – Begriffserklärung

- Dabei helfen erhebliche theoretische und technische Fortschritte in dem Bereich des Data-Mining, die in den letzten Jahren gemacht wurden.
- Beispielsweise wurde berichtet, dass das Online-Versandhaus Amazon in Deutschland die Bestellung eines Mannes stornierte, weil für den Freund von dessen volljähriger, nicht mehr bei den Eltern lebender Tochter ein Zahlungsrückstand gespeichert war*.

* Quelle: Abbestellt. Sippenhaftung bei der Bonitätsprüfung von Amazon. In: c't Magazin für Computertechnik. Heise Verlag, Heft Nr. 1, 21. Dezember 2009, S. 66–67.

Privatsphäre – Begriffserklärung

- Die Legalität derartiger Datenverknüpfungen ist rechtlich bisher nur unzureichend geregelt.

STATT KAMERAS KOMMT IN DEN AMAZON GO STORES DER 2. GENERATION DIE NEUESTE MIKROFONTECHNOLOGIE ZUM EINSATZ.

Privatsphäre – Begriffserklärung

Wolfgang Sofsky schreibt, das nicht nur viele Unternehmen das Idealbild des gläsernen Bürgers haben, sondern auch der Staat.
Der Verdacht des Staates gegen seine Bürger sei nie und nimmer auszuräumen.
Für den Sicherheitsapparat sei die Offene Gesellschaft eine Ansammlung finsterer Gestalten, jedes Gehirn eine Quelle schwarzer Gedanken.

Privatsphäre – Begriffserklärung

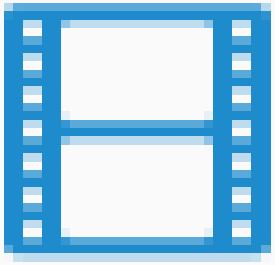
Anonyme Daten über Geburtenrate, Freizeitverhalten oder Verkehrsaufkommen erscheinen harmlos, aber sie können jederzeit kombiniert und einem Individuum zugeordnet werden.
Die Vernetzung der Daten ist nicht auf dieses beschränkt, der Staat will die sozialen Netzwerke erfassen, er wolle wissen welche Verbindungen zwischen den Gruppen, Gemeinschaften, Sekten und Zellen bestehen.

Privatsphäre – Begriffserklärung

Oh, mein Gott!
Das war nur die Einführung...

Wir machen 5 Minuten Pause...

Privatsphäre – Begriffserklärung



Problem #1 – Soziale Medien und Plattformen

Soziale Medien sind eine großartige Möglichkeit, mit Freunden und Familie in Kontakt zu bleiben.
Die wenigsten Menschen denken jedoch darüber nach, welche Art von Informationen sie jedes Mal preisgeben, wenn sie etwas auf einer Plattform posten.
Egal, ob es sich um Informationen über Geburtstage, den beruflichen Werdegang oder ähnliches handelt, wir geben immer mehr Daten preis, als wir denken.

Problem #1 – Soziale Medien und Plattformen

Cybersicherheitsexperten raten den Menschen, ihre Social-Media-Profile privat zu halten und die Informationen, die sie im Abschnitt "Über mich" ihres Profils veröffentlichen, einzuschränken, um es Hackern zu erschweren, Informationen über ein Opfer zusammenzustellen.

Problem #2 – Lebensmittel-Liefer-Apps und Dienste

Lebensmittelliefer-Apps und -Dienste sind dafür bekannt, dass sie Big-Data-Analysen nutzen, um wettbewerbsfähig zu bleiben und die Vorlieben ihrer Kunden zu verstehen.
Jedes Mal, wenn wir Lebensmittel über eine App bestellen, geben wir diesen Unternehmen Informationen darüber, was wir mögen und was nicht.
Wir teilen ihnen auch mit, wie oft wir bestimmte Artikel brauchen.

Problem #2 – Lebensmittel-Liefer-Apps und Dienste

Lebensmittelunternehmen und andere Dienstleister können diese Daten dann an ihre Lieferanten verkaufen und diese Informationen für die Erstellung von Anzeigen nutzen, die auf die gewünschten Kunden ausgerichtet sind.

Problem #3 – Virtuelle Assistenten

Virtuelle Assistenten arbeiten regelmäßig mit großen Mengen an sensiblen Informationen wie Verwaltungsformularen und Kundendaten.
Diese sind oft ein beliebtes Ziel für Hacker, die versuchen, Informationen zu stehlen.
Um sie zu schützen, ist es wichtig, verschiedene Arten von Antivirensoftware zu installieren und sicherzustellen, dass eine klare Datenschutzrichtlinie vorhanden ist.

Problem #4 – Standort-Informationen

Standortinformationen sind etwas, das wir oft preisgeben, ohne uns dessen bewusst zu sein.
Unser Telefon ist durch Navigations-Apps, die Wetter-App und Social-Media-Plattformen ein absoluter Standortanzeiger.

Problem #4 – Standort-Informationen

Die App könnte aufzeichnen, wie lange eine Person bei ihrem Arzttermin war, wie weit sie beim Wandern gegangen ist und wo sie übernachtet hat.

Beunruhigend, nicht?

Problem #5 – Streaming-Plattformen

Ähnlich wie Apps und Dienste, die Lebensmittel liefern, nutzen Streaming-Plattformen wie Netflix, Hulu und Amazon Prime Nutzerdaten, um herauszufinden, welche Programme und Dienste den Nutzern gefallen könnten.
Diese Streaming-Anbieter können dann neue Serien und Filme vermarkten und ausgewählte Nutzer ansprechen.

Problem #6 – Videokonferenz-Systeme und Dienste

Videokonferenzdienste wie Zoom, Microsoft Teams und Google Meets haben während der Pandemie erheblich an Popularität gewonnen.
Die Zahl der Zoom-Nutzer stieg von 10 Millionen im Dezember 2019 auf über 300 Millionen im April 2020.
Das ist zwar eine gute Nachricht für Zoom, aber es ist auch ein bevorzugtes Ziel für Cyberkriminelle und andere böswillige Dritte.

Problem #6 – Videokonferenz-Systeme und Dienste

Allein im April 2020 wurden mehrere Datenschutzprobleme und Sicherheitsverletzungen bei Zoom gemeldet, darunter ein Fehler, der es Hackern leicht machte, die Kontrolle über das Mikrofon oder die Webcam eines Nutzers zu übernehmen.

Problem #6 – Videokonferenz-Systeme und Dienste

Um sich vor potenziellen Hackern zu schützen, sollten Sie Ihre Videokonferenz-Apps immer abmelden und schließen, wenn sie nicht verwendet werden.
Achten Sie auch darauf, Ihre Webcam abzudecken, wenn sie nicht benutzt wird.
Wenn Sie die Webcam Ihres Laptops verwenden müssen, können Sie diese kleinen speziellen Abdeckungen kaufen, um sie auszuschalten.

Problem #7 – Online-Shopping Seiten

Haben Sie schon einmal in einem Online-Katalog nach einer Handtasche gesucht, nur um dann Werbung auf einer ganz anderen Website angezeigt zu bekommen?
Die Sache ist die:
Online-Shopping-Websites verfolgen regelmäßig, was sich Nutzer ansehen, um ihnen das Produkt erneut anzubieten, in der Hoffnung, dass es zu einem Kauf führt.

Problem #8 – Webcams

Für Sicherheitsenthusiasten können Webcams aus gutem Grund verdächtige Geräte sein.
Webcams können leicht gehackt werden, und Hacker schalten sie in der Regel gerne ein und zeichnen ihre Opfer auf.
Neben der Aufzeichnung ihrer Opfer können Hacker auch Malware oder Viren einschleusen, so dass ihre Opfer ihre Webcams nicht mehr benutzen können.

Problem #8 – Webcams

Die Opfer müssen dann für die Freischaltung ihrer Webcams bezahlen. Erschwerend kommt hinzu, dass die Hacker dies alles aus der Ferne tun können.
Um dies zu verhindern, sollten Sie auf die von Ihnen heruntergeladenen Browsererweiterungen achten und die Verwendung Ihrer Webcam nach Möglichkeit einschränken.

Problem #9 – Gesundheits-Apps

Gesundheits-Apps wie Kalorienzähler, Apps zur Vorhersage der Periode und Workout-Tracker sind ideal für alle, die in Sachen Fitness auf dem Laufenden bleiben wollen.
Diese Apps haben jedoch einen kleinen Nachteil:
Sie zeichnen immer Ihre Daten auf.

Problem #9 – Gesundheits-Apps

Apps zur Überwachung des Zeitraums sind in letzter Zeit in die Kritik geraten, weil sie angeblich die Daten ihrer Nutzer verkaufen.
Auch wenn es harmlos erscheinen mag, könnten diese Informationen, wenn sie mit Daten von anderen Social-Media-Seiten und Internet-Footprints gepaart werden, es Hackern ermöglichen, sich ein besseres Bild von ihrer Zielperson zu machen und Wege zu finden, sie auszunutzen.

Problem #10 – Bewertungs-Seiten und -Foren

Sie brauchen nur eine Restaurantkritik zu schreiben oder einen Kommentar in einem Forum zu verfassen, um Ihre Interessen und möglicherweise auch Ihren Standort preiszugeben.
Bewertungen und Kommentare können zwar für andere im Internet hilfreich sein, aber sie können auch unseren Aufenthaltsort preisgeben.

Privatsphäre – Software-Tips

Um Privatsphären-Problemen Herr zu werden, gibt es auch einige Software-“Lösungen“, welche helfen können*...

- Blokada (Android)
- Privacy Badger / NoScript / uBlock (Firefox, Chrome, Opera)*
- Tor-Browser / Brave Browser / Pale Moon / Libre Wolf
- DuckDuckGo / Startpage / ... *
- Signal

* Hey, Edi, sag’ was dazu!

Privatsphäre – Letzte Gedanken…

„Ich glaube, die einzig wirksame Verteidigung gegen das kommende Überwachungsregime besteht darin, eigene Schritte zum Schutz der Privatsphäre zu unternehmen, denn den Datenkraken, die heute alles abgreifen können, fehlt jeder Anreiz zur Selbstbeschränkung.
Man könnte eine historische Analogie zur Verbreitung des Händewaschens ziehen…

Privatsphäre – Letzte Gedanken...

...Bevor immer mehr Menschen von den Vorteilen der Handhygiene überzeugt waren, musste erst die Keimtheorie allgemein anerkannt und popularisiert werden.
Dann musste man den Menschen auch die Angst vor der Ausbreitung von Krankheiten auf diesem Weg einimpfen, vor der Infektion durch unappetitliches Zeug an den Händen, das unsichtbar war, genauso wie die Massenüberwachung unsichtbar ist...”

Privatsphäre – Letzte Gedanken...

„...Sobald die Leute ein ausreichendes Verständnis davon hatten, haben ihnen die Seifenfabrikanten dann Produkte zur Besänftigung ihrer Ansteckungsangst geliefert.
Es ist notwendig, den Leuten Angst einzujagen, damit sich ein Verständnis für das Problem entwickeln kann und schließlich genügend Nachfrage entsteht, um das Problem zu lösen...

Privatsphäre – Letzte Gedanken…

…Es gibt allerdings auch noch eine Schattenseite der Gleichung, nämlich Programme, die zwar ihrem Anspruch nach durch Verwendung von Kryptografie sicher sind, die aber in Wirklichkeit häufig Mogelpackungen sind, weil Verschlüsselung komplex ist und man den Betrug hinter Komplexität verstecken kann.“

Privatsphäre – Letzte Gedanken...

Bitte beachten

Auf der Homepage findet sich immer das

aktuelle Datum, sowie das Thema des nächsten Treffens!

Weitergehende Informationen

https://de.wikipedia.org/wiki/Privatsph%C3%A4re

https://www.privacyinternational.org/

https://www.privacytools.io/

Weitere Informationen bekommen Sie hier:

http://www.FreieSoftwareOG.org

und

Kontakt@FreieSoftwareOG.org

oder kommen Sie doch einfach zu unserem regelmäßigen Treffen,
jeden 1. Mittwoch im Monat ab 20:00 Uhr.
(Treffpunkt laut Webseite)