Zürcher Hochschule
für Angewandte Wissenschaften

School of
Management and Law

Winsights Track «Usable Privacy»
- Online-Tracking und rechtskonforme Umsetzung

Building Competence. Crossing Borders.

Kaj Seidl-Nussbaumer (Probst Partner AG)
kaj.seidl-nussbaumer@probstpartner.ch

Dr. Nico Ebert (ZHAW)
nico.ebert@zhaw.ch

Dr. Nico Ebert (Dozent für Wirtschaftsinformatik)

nico.ebert@zhaw.ch

- Studienleiter MAS Business Engineering
- Dozent u.a. im
  - CAS Business Analysis und Methods
  - CAS Prozessdigitalisierung
  - CAS Datenschutzverantwortliche
- Ab Frühjahr schweizweit erste Weiterbildung in «Privacy by Design» (WBK Privacy by Design)
- Forschung im Bereich technischer Datenschutz

Kaj Seidl-Nussbaumer

- Wirtschaftsanwalt, spezialisiert auf
  - Digitalisierung,
  - IT-Recht,
  - Technologie-Recht
  - Datenschutzrecht

kaj.seidl-nussbaumer@probstpartner.ch

- Dozent im
  - CAS Digitale Technologie und Innovation
  - BA Digitalization and Law

Agenda

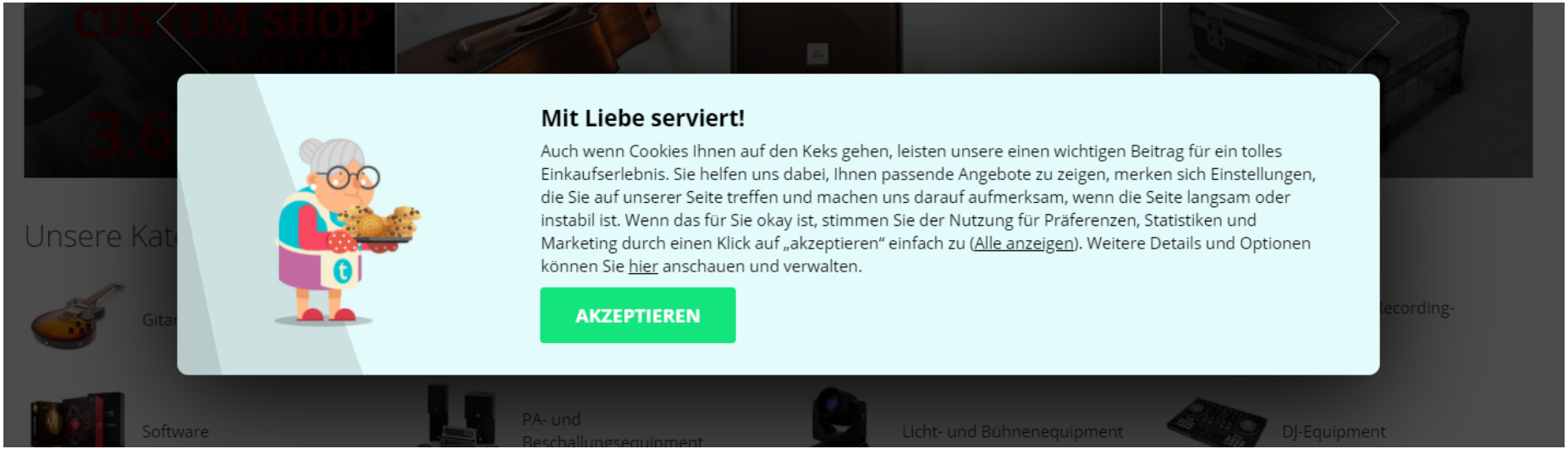
Arten von Online-Tracking

Verbreitung: ausgewählte CH-Studien zum Online-Tracking

Einwilligung beim Online-Tracking (Web)

Rechtskonforme Umsetzung des Online-Trackings

Darum geht es…



Gefunden
von Max Meisterhans
24.09.2020

Quiz 1

Stellen Sie sich vor, Sie besuchen die Webseite einer Schweizer Bank und es erscheint ein Cookie-Banner….

Beispiel: Webseite der Bank Schweiz AG

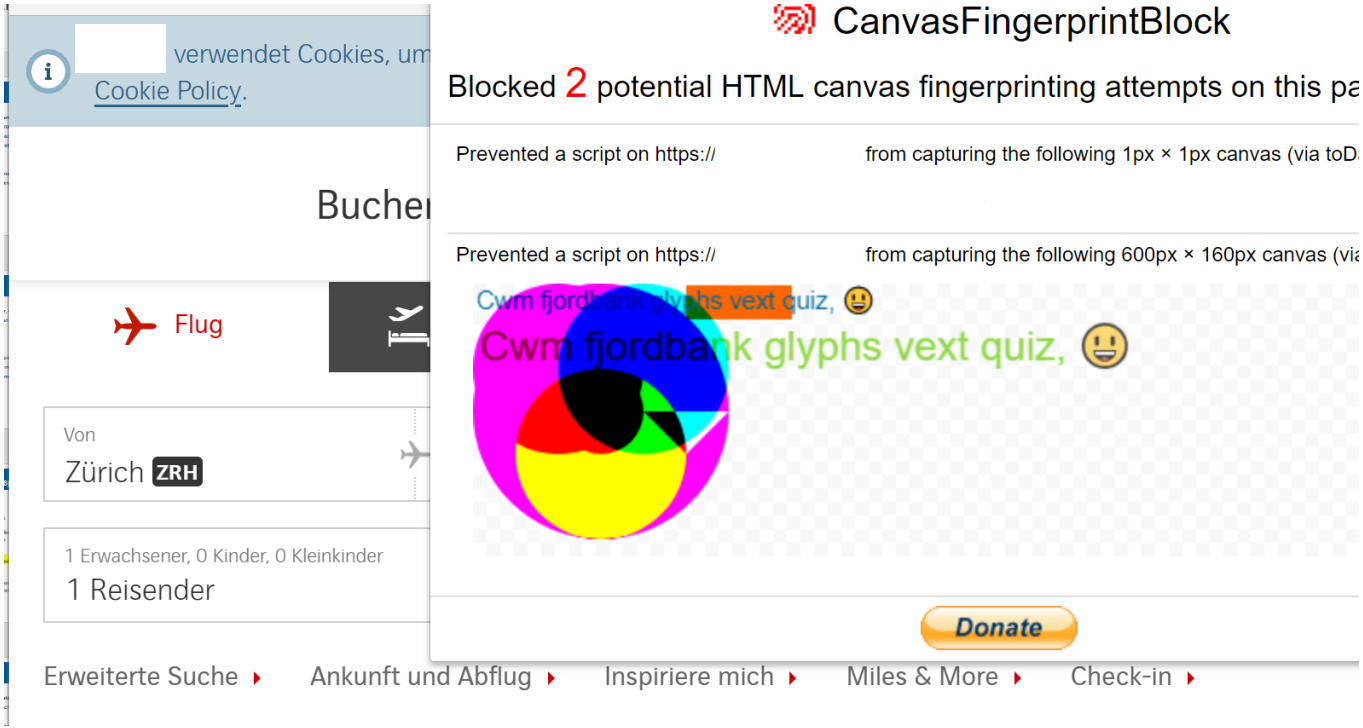
Web-Tracking bei der Bank Schweiz AG

- Gewährleistung der Funktionalität der Website
- Optimierung der Website
- Personalisierung der Website
- Personalisierung der Werbung (auch ausserhalb der Website)
- Einbindung von Social-Media
- Personalisierung der gesamten Dienstleistung (über Verknüpfung mit weiteren Datentöpfen wie CRM-Daten)

Tracker auf den Servern der Bank Schweiz AG

Tracker auf Servern diverser Drittparteien (z.B. Google, Facebook)

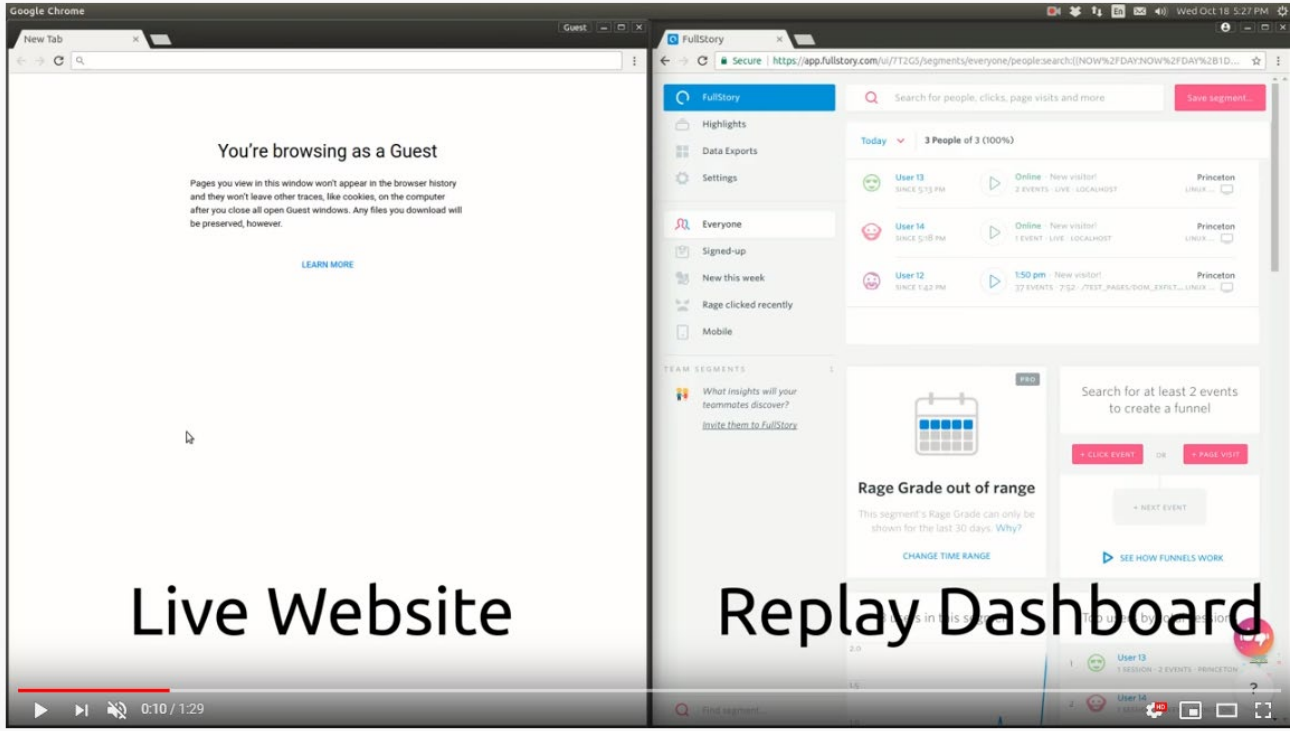
Webseiten: Cookies, Fingerprinting oder lokale Datenbanken, …



https://privacy-bits.com/2018/03/15/webtracking-auf-schweizer-websites-fingerprinting-und-session-replay/

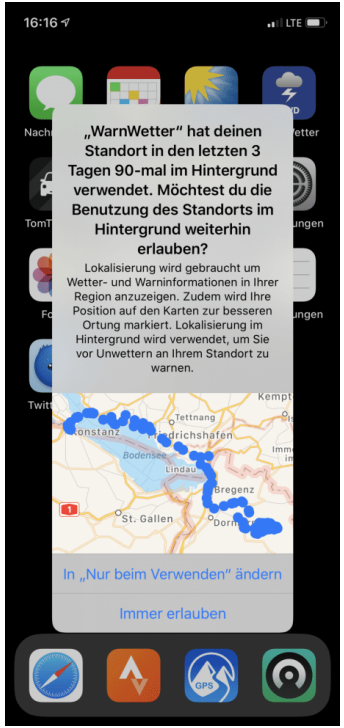
Webseiten: Session Replay (Aufzeichnung aller Tastaturanschläge/Mausbewegungen)

https://www.youtube.com/watch?v=i-VXFqQb3yg



School of Management and Law

Apps: lokale Speicherung, Werbe-ID, …



Agenda

Arten von Online-Tracking

Verbreitung: ausgewählte CH-Studien zum Online-Tracking

Einwilligung beim Online-Tracking (Web)

Rechtskonforme Umsetzung des Online-Trackings

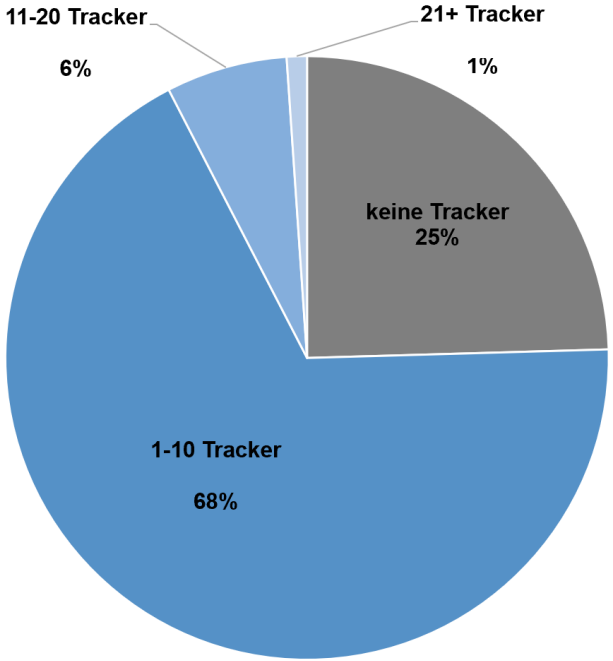
Studie 1: Fingerprinting / Session Replay auf Top 374 Websites in CH (2018)

Website	Fingerprint_Script	Fingerprint_Canvas	Fingerprint_CanvasFont	Fingerprint_WebRTC	Sessionreplay_Script	Sessionreplay_Hotjar	Sessionreplay_Yandex	Sessionreplay_Clicktale	Sessionreplay_Smartlook	Sessionreplay_Mouseflow	Sessionreplay_Luckorange
Gesamt absolut	**90**	**49**	**3**	**2**	**28**	**23**	**2**	**1**	**1**	**1**	**1**
Gesamt prozentual	**24.1%**	**13.1%**	**0.8%**	**0.5%**	**7.5%**	**6.1%**	**0.5%**	**0.3%**	**0.3%**	**0.3%**	**0.3%**
1815.ch											
20min.ch	dakt										
24heures.ch	dakt										
3plus.tv											
4plus.tv											

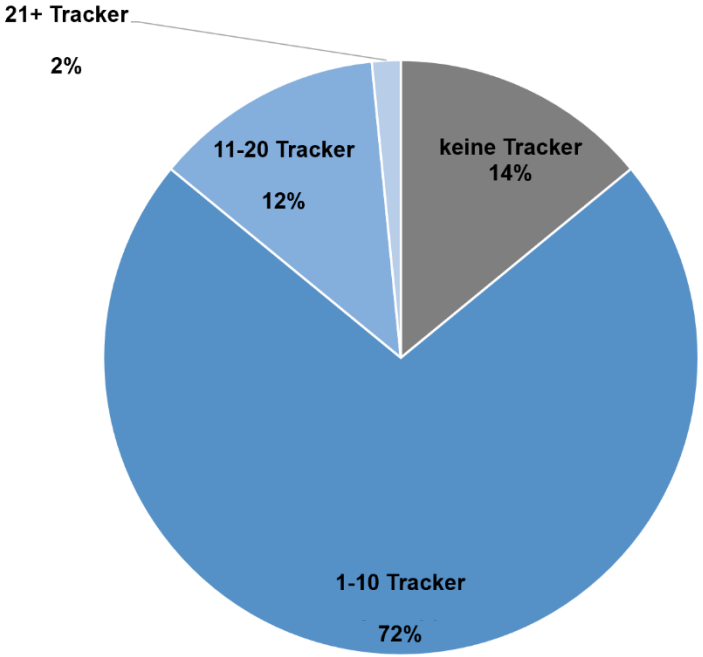
Ebert (2018) Webtracking auf Schweizer Websites, PrivacyBits Blog

Studie 2: Web-Tracking bei Banken und Versicherungen (2019)

Häufigkeit von Trackern auf den Webseiten von Mitgliedern von SwissBanking [%]
n = 277, März 2019



Häufigkeit von Trackern auf den Webseiten von Mitgliedern des SVV [%]
n = 64, März 2019



Schweizer/Ebert (2019) Web-Tracking bei Schweizer Versicherungen und Banken, Winsights Blog

Studie 2: Web-Tracking bei Banken und Versicherungen (2019) - Fokus: Session-Replay

SwissBanking-Webseiten

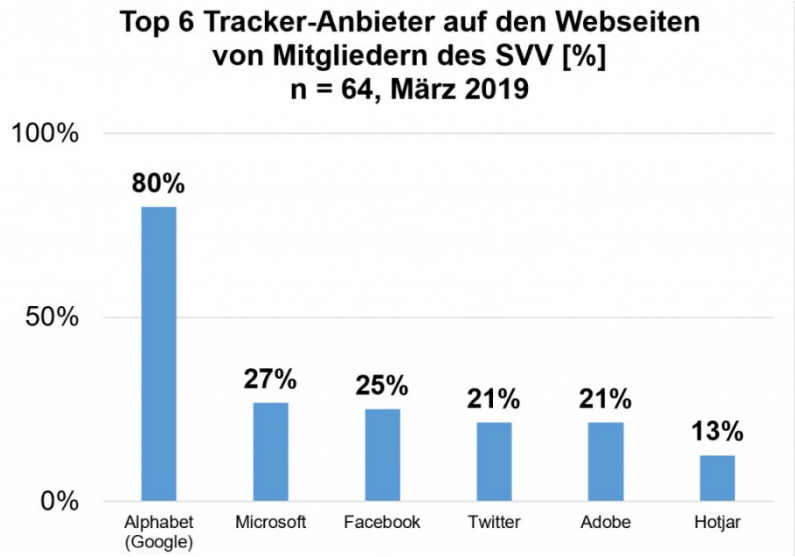
bankfab.com/en-ch	Hotjar
bcn.ch/	Hotjar
bdo.ch/en-gb/home-en	CrazyEgg
blkb.ch/	Dynatrace
bonhote.ch/	Hotjar
cembra.ch/	Hotjar
ch.leonteq.com/	Hotjar
credit-suisse.com/ch/en.html	Decibel Insight
graffenried.ch/privatbank	Hotjar
group.pictet/	Decibel Insight
ig.com/ch/kontakt-GVA	Decibel Insight
jsafrasarasin.ch/internet/ch/	Matomo
ml.com/	Tealeaf
online.citi.com/US/login.do	Glassbox
pwc.ch/	Hotjar
schroders.com/de/ch/	SessionCam
vermoegenszentrum.ch/individuals.html	Hotjar

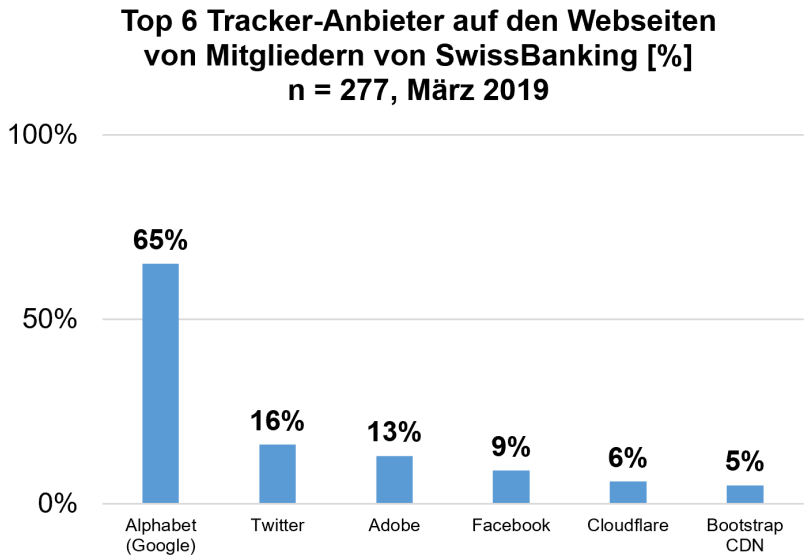
SVV-Webseiten

Top Level URL	Sessionreplaytool
aspen.co/Reinsurance/	Hotjar
axaxl.com/	Dynatrace
axaxl.com/insurance	Dynatrace
aig.com/	SessionCam
assura.ch/fr	Hotjar
axa.ch/en/private-customers.html	Dynatrace
helsana.ch/en/individuals	Hotjar
helvetia.com/ch/web/en/private-customers.html	Dynatrace
helvetia.com/corporate/web/de/home.html	Dynatrace
pax.ch/	Hotjar
retraitespopulaires.ch/	Hotjar
sanitas.com/en/private-customers.html	M-Pathy
vaudoise.ch/	Hotjar
zurich.ch/	Hotjar

Schweizer/Ebert (2019) Web-Tracking bei Schweizer Versicherungen und Banken, Winsights Blog

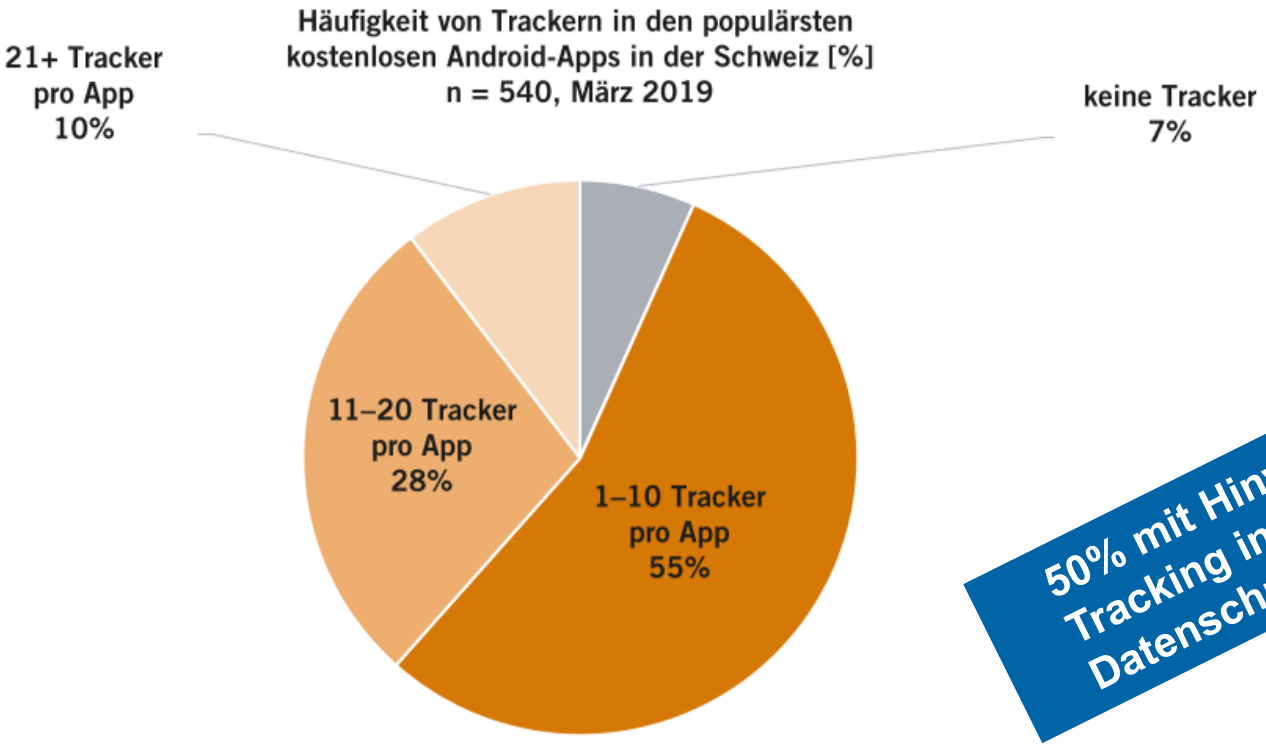
Studie 2: Web-Tracking bei Banken und Versicherungen (2019) - Fokus: Tracker-Anbieter





Schweizer/Ebert (2019) Web-Tracking bei Schweizer Versicherungen und Banken, Winsights Blog

Studie 3: App-Tracking in Top 540 Schweizer Gratis-Apps (2019)



50% mit Hinweisen auf Tracking in der Datenschutzerklärung

Ebert/Schmid/Böni (2019) Verbreitung von App-Tracking in der Schweiz digma 4/2019

Studie 4: App-Tracking in Bundes-Apps (2019)

Laufzeitanalyse von 51 Apps auf Tracking*

Stichtag der Auswertung	01.04.2019
App-Name	absolute Anzahl Tracker
Die Volkswirtschaft	6
SmokeFree Buddy App	4
MeteoSwiss	4
MySwissFoodPyramid	3
Alertswiss	3
QuickZoll	3
EcoDriver	3
Treibstoffverbrauch	3
SwissRookie	3
cheminfo	2
cheminfo business	2
DRW-Nukmed	2
Flight Safety Swiss Air Force	2
Patrouille Suisse	2
SAT	2
armafolio	2
airCHeck	1
Swiss parks	1
Dance it!	1
Landesmuseum Zürich	1
ready - fir for #teamarmee	1

* nicht aufgeführt sind Apps mit Trackern, die zur Laufzeit nicht aktiv waren

Bei 25 der 51 Apps war im Google Play Store eine Datenschutzerklärung hinterlegt

Ebert/Schmid/Böni (2019) Verbreitung von App-Tracking in der Schweiz digma 4/2019

Online-Tracking: Agenda

Arten von Online-Tracking

Verbreitung: ausgewählte CH-Studien zum Online-Tracking

Einwilligung beim Online-Tracking (Web)

Rechtskonforme Umsetzung des Online-Trackings

Einwilligung ins Web-Tracking (BayLDB 2019)

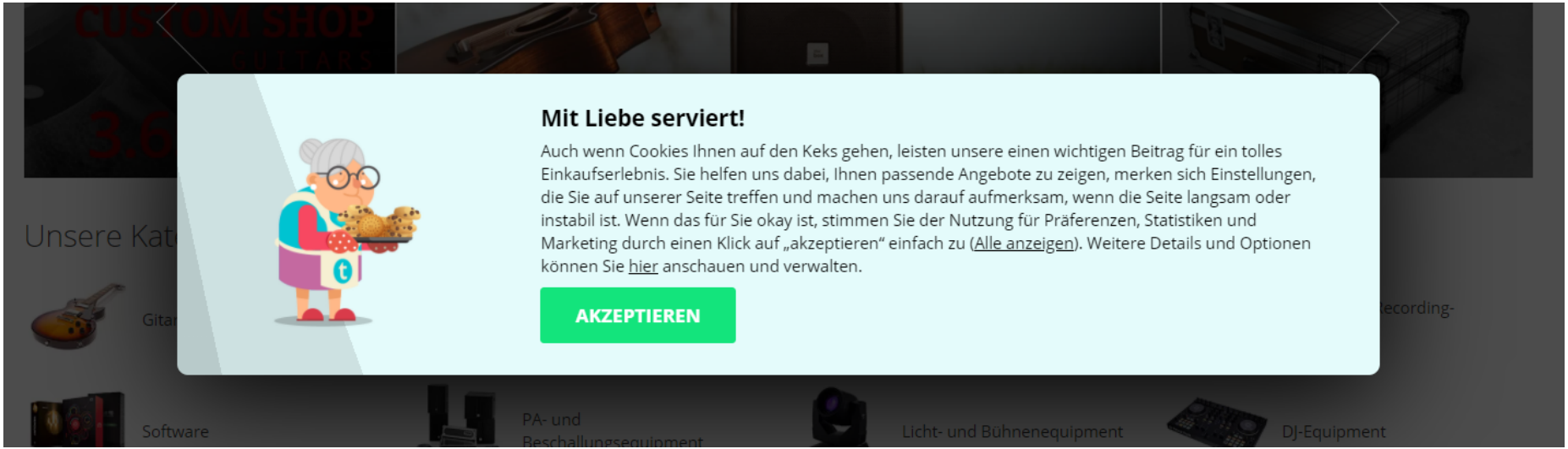
https://www.lda.bayern.de/media/sid_ergebnis_2019.pdf

Einwilligung ins Web-Tracking (INRIA 2020)

- Untersuchung von 1426 europäischen Webseiten, die sich offiziell an das TCF-Framework des IAB halten (Europäischer Werbeverband)
  - 141 registrieren Einwilligung ohne jegliche Nutzerinteraktion (und geben die Einwilligung an Drittparteien wie Facebook weiter)
  - 236 nutzen «Dark Patterns», um die Einwilligung zu erzwingen (z.B. Vorauswahl, keine Auswahl, etc.)
  - 27 registrieren Einwilligung trotz ausdrücklichem Widerspruch (und geben die Einwilligung an Drittparteien wie Facebook weiter)
  - Von 560 Webseiten, die detaillierter betrachtet wurden, weisen 54% eine mutmassliche rechtliche Verletzung auf

Matte, C., Bielova, N., & Santos, C. (2020, May). Do Cookie Banners Respect my Choice?: Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. In 2020 IEEE Symposium on Security and Privacy (SP)

«Dark Pattern» bei der Einholung der Einwilligung



Quiz 2

Was ist Ihre subjektive Meinung als Privatperson zu «Dark Pattern» und Tracking?

Agenda

Arten von Online-Tracking

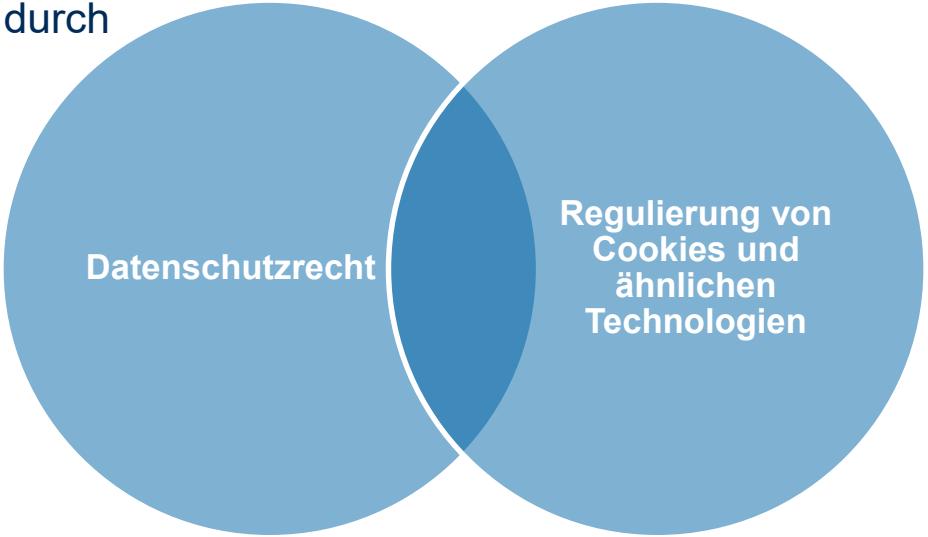
Verbreitung: ausgewählte CH-Studien zum Online-Tracking

Einwilligung beim Online-Tracking (Web)

Rechtskonforme Umsetzung des Online-Trackings

Rechtskonforme Umsetzung des Online Trackings

– Tracking reguliert durch



wenn Personendaten

wenn gesetzliche Technologieumschreibung einschlägig

Datenschutzrecht und Technologieregulierung - Übersicht

	Datenschutz	Technologieregulierung
EU	DSGVO	ePrivacy Richtlinie (2002/58/EG), Einführung Opt-In mit Ergänzung 2009 (2009/136/EG)
Mitgliedstaaten	Nationale Datenschutzgesetze (wenig Spielraum, da VO)	häufig in Telekom oder verwandter Regulierung, wie z.B. in DE das Telemediengesetz (mehr Spielraum, da RL)
Schweiz	DSG	FMG 45c, orientiert an ePrivacy RL 2002

Technologieregulierung - Voraussetzungen

- Anknüpfungspunkt:
  - Bearbeiten (Speicherung/Zugriff)
  - von Informationen
  - auf Endgeräten

→ Nicht erfasst: alternative Tracking-Methoden

- **Art. 45c[1] Daten auf fremden Geräten**

Das Bearbeiten von Daten auf fremden Geräten durch fernmeldetechnische Übertragung ist nur erlaubt:

a. für die Fernmeldedienste und ihre Abrechnung; oder

b. wenn die Benutzerinnen und Benutzer über die Bearbeitung und ihren Zweck informiert und darauf hingewiesen werden, dass sie die Bearbeitung ablehnen können.

(3) Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.

Anwendbares Recht?

- Erhebliche Differenzen in den Gesetzen, sowohl was Pflichten (z.B. Informationspflicht, Opt-In etc.) als auch Konsequenzen angeht (z.B. DSGVO-Bussen)
- Doch: welches Datenschutzrecht / Technologieregulierung gilt?

Anwendbares Recht - Datenschutzrecht

- Datenschutzrecht: DSGVO anwendbar?
  - Sitz in EU? Wenn nein:
  - Extraterritorialität?
    - Mache ich gezielt Angebot von Waren oder Dienstleistungen an Personen in der EU?
    - Beobachte ich Personen in der EU?

→ Tracking zielt in der Regel auf gezielte Identifikation des Users, insb. für Retargeting. Wer gezielt Tracking Technologien einsetzt und Personen in der EU/EWR (inkl. Liechtenstein!) nicht ausklammert, z.B. mittels Geo-Fencing, fällt in der Regel unter die Extraterritorialität

Anwendbares Recht – Technologieregulierung

- Technologieregulierung
  - ePrivacy Richtlinie
    - gilt in EU, aber nur indirekt (RL, nicht VO)
    - Ausblick: ePrivacy VO hängig; sieht Extraterritorialität und Bussen analog DSGVO vor
  - Lokale Fernmeldegesetze
    - von Land zu Land verschieden, in der Regel nationale Gültigkeit
    - Anwendbarkeit in der Schweiz fraglich
  - Fernmeldegesetz
    - für Unternehmen mit Sitz in der Schweiz verbindlich (unter anderem)

Evolution der Cookie Regulierung

- ePrivacy RL 2002: Information und Hinweis auf **Opt-Out**, gewisse Ausnahmen
- ePrivacy RL 2009: **Opt-In**, weitere Einschränkung der Ausnahmen
- EuGH C-673/17, Planet 49 vom 1.10.19: **keine vorangekreuzten Kästchen** für ePrivacy RL 5(3), zudem Information über **Funktionsdauer** und **Teilen** mit / Zugriff Dritter
- (formell Entscheid nur verbindlich in Deutschland: Deutscher BGH I ZR 7/16, Planet49 vom 28.5.2020: **Einwilligung nötig** bei Tracking für Werbezwecke nach Telemediengesetz)

Rechtskonforme Umsetzung

Tiefste Tracking Regulierungsdichte:
- Normale Personendaten
- Nur Schweizer Nutzer
- Nur alternative Trackingmethoden
- Nicht für Werbezwecke
- Nicht geteilt mit Dritten

Höchste Tracking Regulierungsdichte:
- Personendaten
- in EU
- mit «Cookies» o.ä.
- für Werbezwecke
- Geteilt mit Dritten

Rechtskonforme Umsetzung

- Minimal Risk Approach bei höchster Regulierungsdichte:
  - Generell keine Cookies setzen bei Erstaufruf
  - Information über
    - Verwendung und Zweck von Cookies bzw. anderen Tracking Technologien
    - Funktionsdauer
    - Zugriff durch / Teilen mit Dritten
    - Zusätzlich zu übrigen Datenschutzinformationen gemäss DSGVO (Rechte etc., möglich über Link)
  - Einwilligung abholen und dokumentieren für alle nicht unbedingt erforderlichen Cookies
  - Keine vorangekreuzten Kästchen verwenden
  - Einwilligung durch klare zustimmende Handlung, am wenigsten Risiko: klares Gegensatzpaar wie z.B. «Agree» und «Decline» (rechtliche Zulässigkeit des Nudgings / Dark Designs noch nicht geklärt)

ABER: viele Abstufungen bis hin zur tiefsten Regulierungsdichte. Je nach Wichtigkeit, im Einzelfall klären.

Rechtskonforme Umsetzung

- Mögliche Vorgehensweise bei tieferer Regulierungsdichte z.B.:
  - Kein Cookie Banner
  - Information in Datenschutzerklärung über
    - Verwendung und Zweck von Cookies bzw. anderen Tracking Technologien
    - Möglichkeit der Ablehnung

  - Wichtig: Begleitende Massnahmen, z.B. Geo-Fencing zur Sicherstellung, dass man ausserhalb DSGVO / ePrivacy RL Bereich operiert

zh aw School of Management and Law