Data Privacy Laws

Christian Sillaber

Agenda

10.000m view on privacy laws: principles and building blocks
GDPR: actors, entities, artifacts and rights
revSwissDSG, CCPA

In case you need less theory and more practice: https://cookieconsentspeed.run/

Privacy Laws – from first principles

A brief (and simplified) history of privacy

- Individual rights vs collective rights
- Constitution / Balancing of interests
- Citizen <> State and Citizen <> Citizen (Evil Corp.)
- Fairness, Transparency and Lawfulness
- Control and Self-determination

Richards, Neil M., Why Data Privacy Law Is (Mostly) Constitutional (October 2, 2013). Neil M. Richards, Why Data Privacy Law Is (Mostly) Constitutional, 56 Wm. & Mary L. Rev. 1501 (2015)., Available at SSRN: https://ssrn.com/abstract=2335196

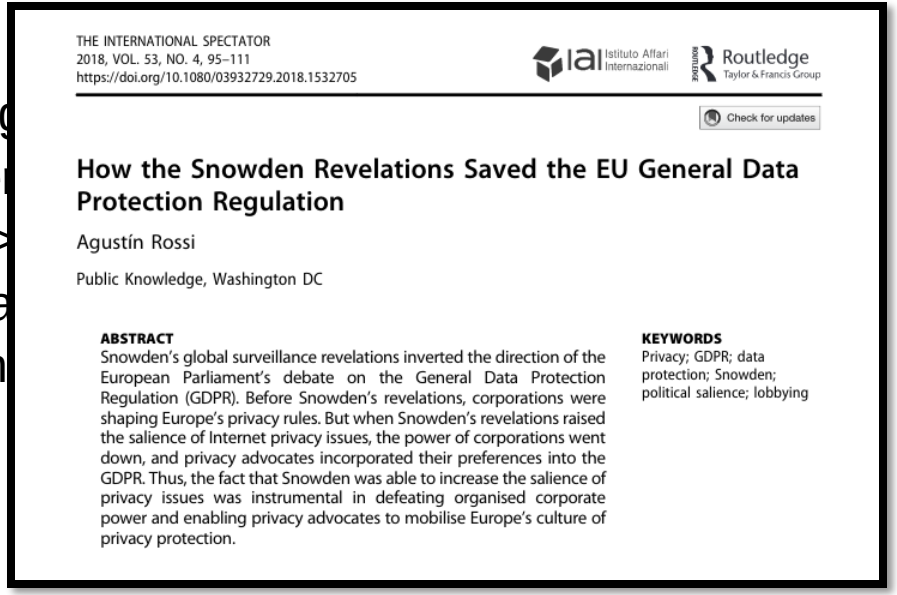
Privacy Laws – from first principles

A brief (and simplified) history of privacy

UNIVERSITÄT BERN

- Individual rights vs collective ri
- Constitution / Balancing of inte
- Citizen <> State and Citizen <>
- Fairness, Transparency and La
- Control and Self-determination

https://www.iai.it/sites/default/files/tis_rossi.pdf



THE INTERNATIONAL SPECTATOR
2018, VOL. 53, NO. 4, 95–111
https://doi.org/10.1080/03932729.2018.1532705

Istituto Affari Internazionali | Routledge Taylor & Francis Group

Check for updates

How the Snowden Revelations Saved the EU General Data Protection Regulation

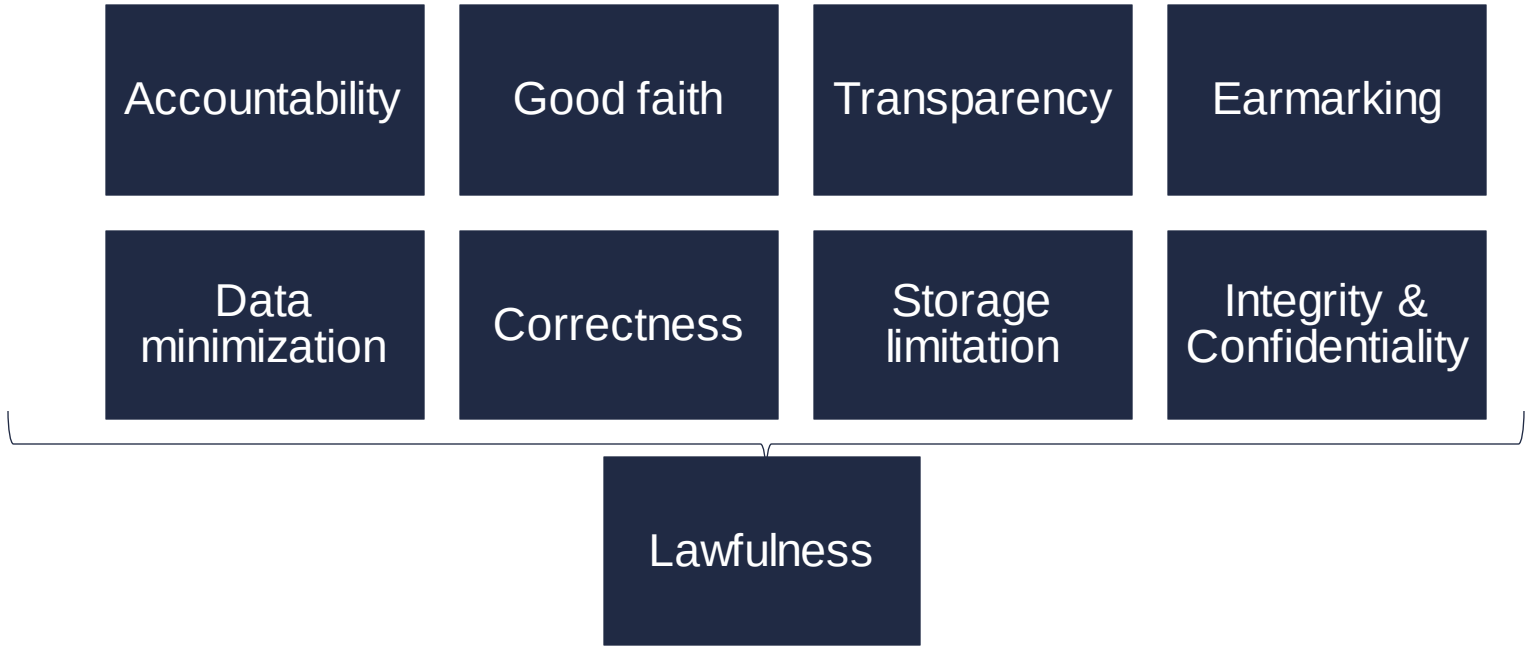
Agustín Rossi

Public Knowledge, Washington DC

ABSTRACT
Snowden's global surveillance revelations inverted the direction of the European Parliament's debate on the General Data Protection Regulation (GDPR). Before Snowden's revelations, corporations were shaping Europe's privacy rules. But when Snowden's revelations raised the salience of Internet privacy issues, the power of corporations went down, and privacy advocates incorporated their preferences into the GDPR. Thus, the fact that Snowden was able to increase the salience of privacy issues was instrumental in defeating organised corporate power and enabling privacy advocates to mobilise Europe's culture of privacy protection.

KEYWORDS
Privacy; GDPR; data protection; Snowden; political salience; lobbying

Principles


Accountability
Good faith
Transparency
Earmarking
Data minimization
Correctness
Storage limitation
Integrity & Confidentiality
Lawfulness

GDPR

Overview

UNIVERSITÄT BERN

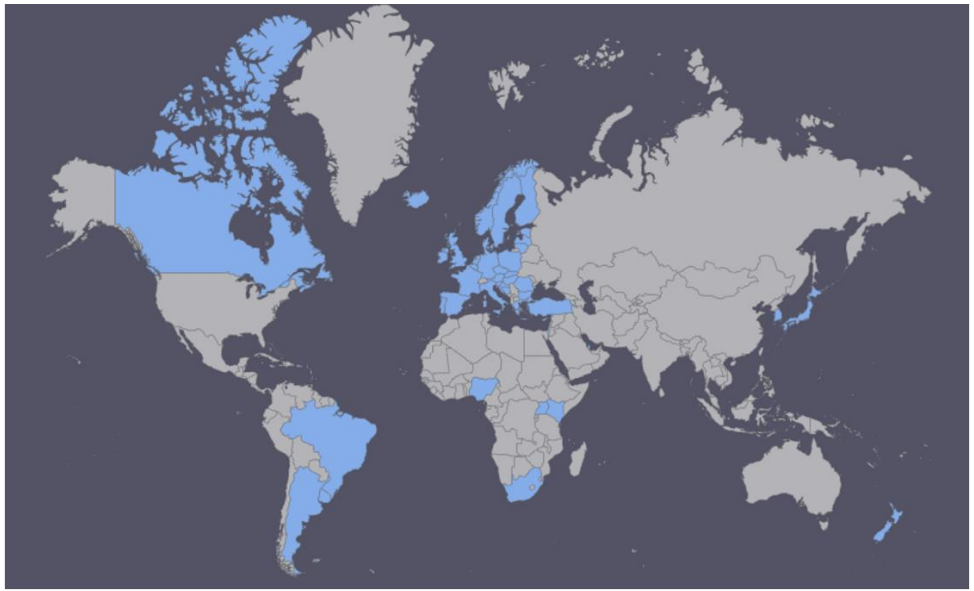
- General Data Protection Regulation (GDPR) in effect across the EU from May 25, 2018.
- Regulation is directly applicable to all processing of personal data in the EU / collected from EU data subjects.
- Regulation includes significant escalation in potential penalties.
  - Violations can result in fines of up to 4% of an entity's global revenues.

GDPR

Overview

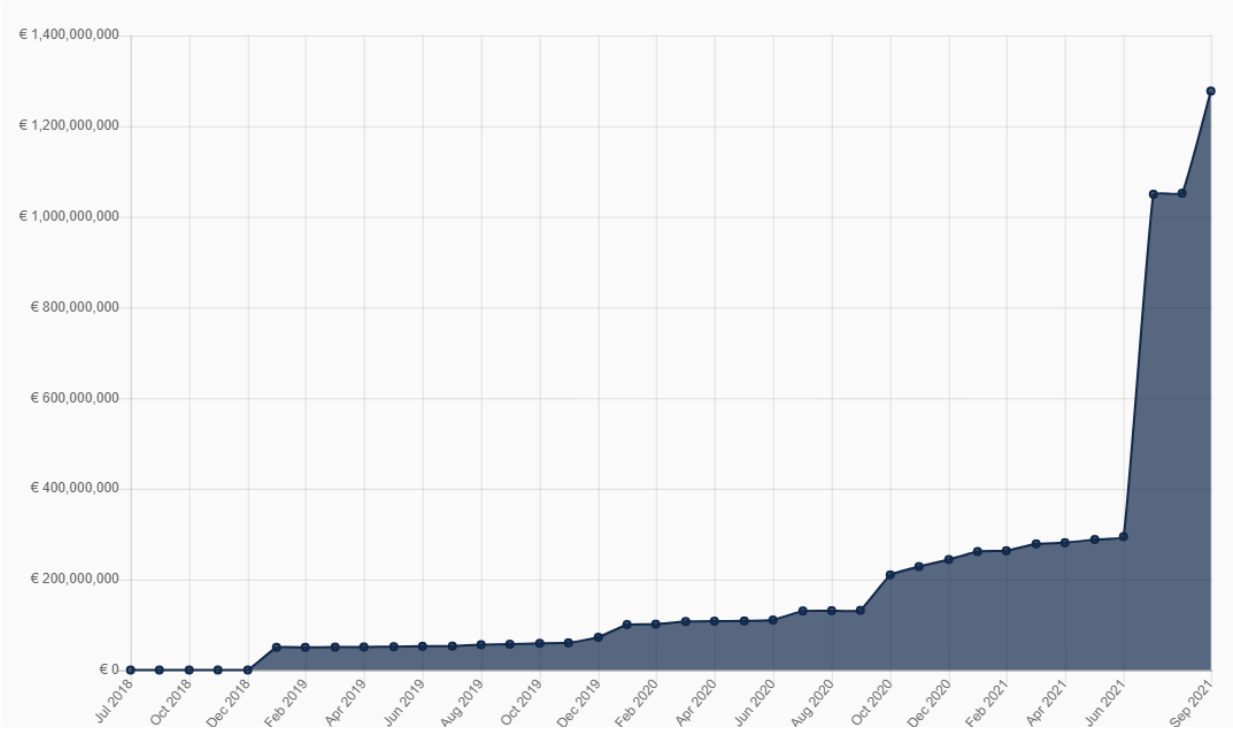
GDPR set off an avalanche

17 national laws
+ Many regional laws (e.g. CCPA)



GDPR

Enforcement activities



Overall sum of GDPR-related fines (cumulative). Source: enforcementtracker.com/?insights (2021-09-20)

Enforcement activities

Statistics: Highest individual fines (Top 10)

The following statistics shows the highest individual fines imposed to date per data controller (only top 10 fines).

	Controller	Sector	Country	Fine [€]	Type of Violation	Date
1	Amazon Europe Core S.à.r.l.	Industry and Commerce	LUXEMBOURG	746,000,000	Non-compliance with general data processing principles	16 Jul 2021
2	WhatsApp Ireland Ltd.	Media, Telecoms and Broadcasting	IRELAND	225,000,000	Insufficient fulfilment of information obligations	02 Sep 2021
3	Google LLC	Media, Telecoms and Broadcasting	FRANCE	50,000,000	Insufficient legal basis for data processing	21 Jan 2019
4	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Employment	GERMANY	35,258,708	Insufficient legal basis for data processing	01 Oct 2020
5	TIM (telecommunications operator)	Media, Telecoms and Broadcasting	ITALY	27,800,000	Insufficient legal basis for data processing	15 Jan 2020
6	British Airways	Transportation and Energy	UNITED KINGDOM	22,046,000	Insufficient technical and organisational measures to ensure information security	16 Oct 2020
7	Marriott International, Inc	Accomodation and Hospitalty	UNITED KINGDOM	20,450,000	Insufficient technical and organisational measures to ensure information security	30 Oct 2020
8	Wind Tre S.p.A.	Media, Telecoms and Broadcasting	ITALY	16,700,000	Insufficient legal basis for data processing	13 Jul 2020
9	Vodafone Italia S.p.A.	Media, Telecoms and Broadcasting	ITALY	12,251,601	Non-compliance with general data processing principles	12 Nov 2020
10	notebooksbilliger.de	Employment	GERMANY	10,400,000	Insufficient legal basis for data processing	08 Jan 2021

TOP 10. Source: enforcementtracker.com/?insights (2021-09-20)

GDPR

Overview

- **Applies to processing of "personal data" in the context of the activities of an establishment of a controller or a processor in the EU.**

- It also applies where a controller or processor is not established in the EU but its processing activities are related to:
  - Offering of goods or services to EU residents (regardless of whether payment is provided).
  - Monitoring the behavior of EU residents.

→ **"exterritorial applicability": If you want access to the EU digital market, better follow GDPR.**

GDPR

Overview

– In theory, a goal of the Regulation is to achieve greater harmonization of requirements across the EU.
– However, in many contexts, potential for variation exists: 27 Variations

GDPR

Overview

- In theory, a goal of the Regulation is to achieve greater harmonization of requirements across the EU.
- However, in many contexts, potential for variation exists: ~~27 Variations~~ 28 (UK)

GDPR

Overview

- In theory, a goal of the Regulation is to achieve greater harmonization of requirements across the EU.
- However, in many contexts, potential for variation exists: ~~27 Variations~~ ~~28 (UK)~~

31 (EU + UK + EFTA (Norway, Iceland, Liechtenstein))

Intermezzo GDPR vs UK-GDPR

- ICO (Information Commissioner's office; not related to crypto) announced plans for a 'business friendly approach'
- Might tackle cookie banners and enforce technical DNT solutions
- Announced plans for easier data transfer to US

GDPR – Core Concepts

UNIVERSITÄT BERN

- **Personal data:** Any information relating to an identified or identifiable natural person.
  - **Sensible data:** Personal data revealing racial, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life and sexual orientation, genetic data and biometric data.
  - **Criminal Offences**: Data relating to criminal offences and convictions.
  - Health Data: personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status

- **Pseudonymization**: "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

- **Anonymization:** eliminates personal data so that data subjects can no longer be identified. Anonymized data is excluded from GDPR regulation altogether because anonymized data is no longer "personal data."

- **Processing**: means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Dynamic IP Address (81.119.202.21)

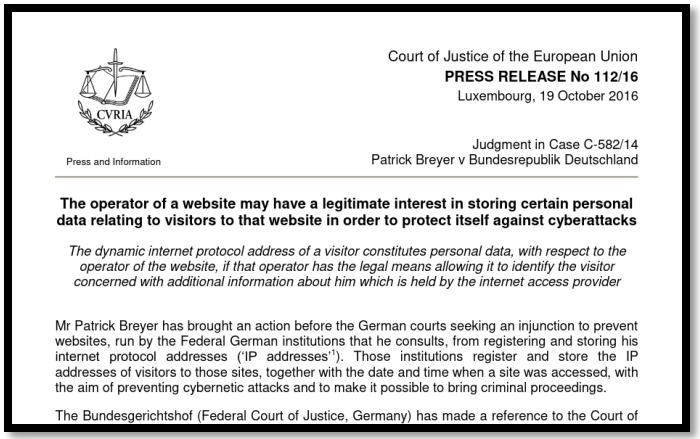
= =

Personal Data?

Dynamic IP Address (81.119.202.21)

= =

Personal Data!



Press and Information

Court of Justice of the European Union
PRESS RELEASE No 112/16
Luxembourg, 19 October 2016

Judgment in Case C-582/14
Patrick Breyer v Bundesrepublik Deutschland

The operator of a website may have a legitimate interest in storing certain personal data relating to visitors to that website in order to protect itself against cyberattacks

The dynamic internet protocol address of a visitor constitutes personal data, with respect to the operator of the website, if that operator has the legal means allowing it to identify the visitor concerned with additional information about him which is held by the internet access provider

Mr Patrick Breyer has brought an action before the German courts seeking an injunction to prevent websites, run by the Federal German institutions that he consults, from registering and storing his internet protocol addresses ('IP addresses'). Those institutions register and store the IP addresses of visitors to those sites, together with the date and time when a site was accessed, with the aim of preventing cybernetic attacks and to make it possible to bring criminal proceedings.

The Bundesgerichtshof (Federal Court of Justice, Germany) has made a reference to the Court of

https://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN

GDPR – Controller Processor

UNIVERSITÄT BERN

Controller (Art 24 GDPR)

Determines the “why and how” personal data is processed (purpose and means)

In general, controllers bear primary responsibility for ensuring that processing activities are compliant with EU data protection law

Processor (Art 28 GDPR)

Acts on the controller’s behalf.
Binding written agreement.
Controller must ensure processor’s compliance.

Joint Controller (Art 26 GDPR)

Example

- A Mecrosaft AG employee applies for a different job at Mecrosaft AG;
- For this, he/she uses the internal Mecrosaft 366 tool (mostly a word processor and email).
- Mecrosaft 366 runs on VMs in a Croatian data center.
- The VMs run on hardware bought from a now unprofitable Islandic bitcoin mining firm.
- All data is backed up daily to an USB stick of an employee of the data center who sold this "service" to the data center and takes it home daily.

Who is the:

- Data subject, if any?
- Controller, if any?
- Processor, if any?

The data subject rights

UNIVERSITÄT BERN

- Right of access (Art. 15)
- Right to rectification (Art. 16)
- Right to erasure (Art. 17)
- Right to restriction (Art. 18)
- Right to data portability (Art. 20)
- Right to object (Art. 21)
- Right not to be subject to decisions based solely on automated processing which produces legal or similarly significant effects (Art. 22)

GDPR - Processes and artifacts

Privacy by Design (PbD) and Data Protection Impact Assessments (DPIAs)

UNIVERSITÄT BERN

Data protection must be considered (and such considerations documented) in the design of all new processes and technologies for the processing of personal data.

Written DPIAs required whenever processing is likely to result in high risk to data subjects.

Includes (at least) processing of sensitive data and whenever automated processing/profiling results in decisions having legal effect.

- DPIA may evaluate an entire category of processing operations if they are sufficiently similar.
- DPIA must identify specific risks and describe privacy and security measures implemented to mitigate them.
- Mandatory consultation with data protection authority where processing poses high level of risk to data subjects that cannot be adequately mitigated.

GDPR – Processes and Artifacts

Records of Processing

- Controllers (and processors) must maintain detailed records on all data processing operations.
- Record-keeping replaces the registration requirements currently in place in some EU countries.
- Controller requirements:
  - Name and contact details
  - Description of processing activity
  - Purpose(s) of the processing
  - Data subject categories
  - Personal data categories
  - Retention period
  - Recipients and third-country transfers
  - Security measures

GDPR – Processes and Artifacts

Data Breach Notification

- Data controllers must notify the competent data protection authority without undue delay and, where feasible, within 72 hours of becoming aware of a breach, unless it is unlikely to result in a risk to data subjects.
- **Risks include**, inter alia, physical, material or moral damage to individuals such as discrimination, identity theft or fraud, financial loss, and damage to reputation.

Data controllers must notify data subjects without undue delay of breaches that are likely to result in a high risk to them.

GDPR - Roles

Data Protection Officers

- Companies that process sensitive data as core activity or whose core activities involve regular and systematic monitoring of data subjects must appoint a data protection officer that reports to the highest levels of management.

- DPO must be appointed for fixed term; may be dismissed only for failure to perform duties.
- DPO may perform other duties if they do not cause a conflict of interest.

GDPR - Sanctions

UNIVERSITÄT BERN

- Violations of a controller's obligations with respect to **record-keeping, security, breach notification, and privacy impact assessments are subject to a maximum administrative penalty of €10 million or 2% of the entity's global gross revenue**, whichever is higher.

- Violations of a controller's obligations with respect to **having a legal justification for processing, complying with the rights of data subjects, and cross-border data transfers are subject to a maximum penalty of €20 million or 4% of the entity's global gross revenue**, whichever is higher.

GDPR - Sanctions

UNIVERSITÄT BERN

- Data subjects have the right to compensation for any material or immaterial damage resulting from a violation of the Regulation. ➔ Often impossible to proof

- Data subjects can authorize non-profit, public interest bodies to bring complaints on their behalf for the same purposes. ➔ e.g. NOYB in Austria

Consent (to the processing of data)

UNIVERSITÄT BERN

Consent must be:

- Freely given
- Specific
- Informed
- Unambiguous indication of individual's wishes

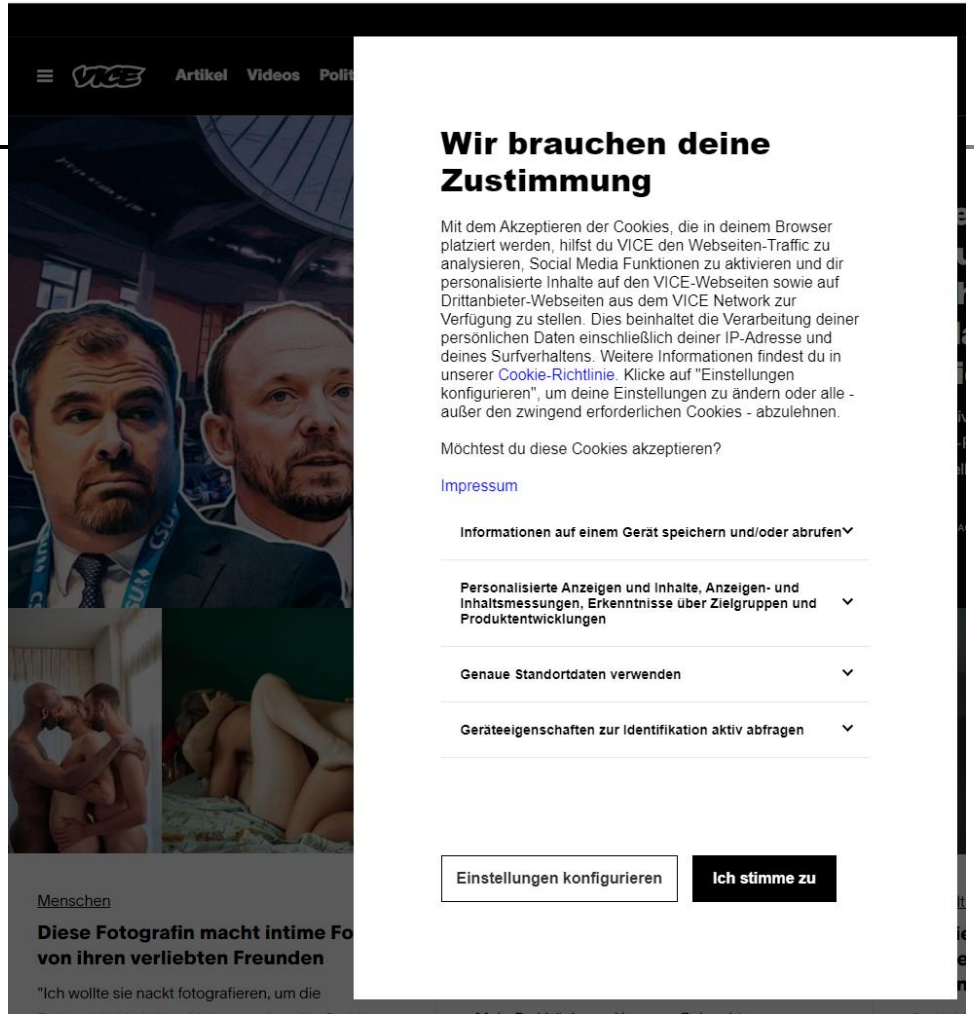
- Individual must be able to withdraw consent at any time without detriment.
- Controller must maintain a record of consent until related processing is complete.

Consent (to the processing of data)

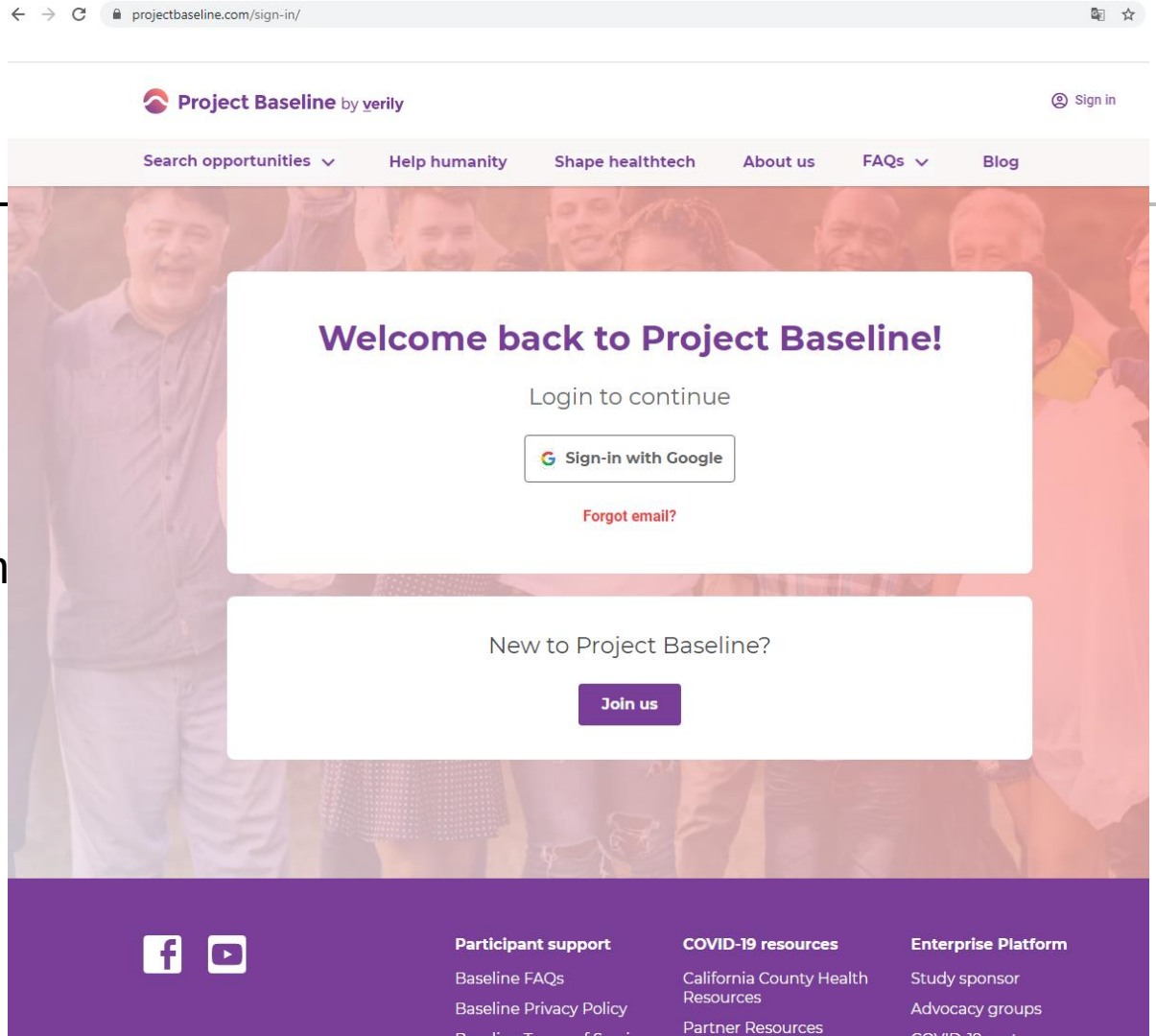
UNIVERSITÄT BERN

Freely Given: Individual must have a real choice, can't feel compelled to consent, and no negative consequences if consent not given.

- Consent can't be 'bundled' with acceptance of other terms and conditions.
- Consent can't be 'tied' to the provision of a contract or service where the processing is not strictly necessary for the performance of such contract or service.
- If the controller is able to show that a service includes the possibility to withdraw consent without any negative consequences (e.g., without the performance of the service being downgraded to the detriment of the user), this may show that the consent was given freely.
- Separate consent should be possible when engaging in multiple processing activities for more than one purpose.
- If the controller conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom.


vice.com/de
Artikel
Videos
Wir brauchen deine Zustimmung
Mit dem Akzeptieren der Cookies, die in deinem Browser platziert werden, hilfst du VICE den Webseiten-Traffic zu analysieren, Social Media Funktionen zu aktivieren und dir personalisierte Inhalte auf den VICE-Webseiten sowie auf Drittanbieter-Webseiten aus dem VICE Network zur Verfügung zu stellen. Dies beinhaltet die Verarbeitung deiner persönlichen Daten einschließlich deiner IP-Adresse und deines Surfverhaltens. Weitere Informationen findest du in unserer Cookie-Richtlinie. Klicke auf "Einstellungen konfigurieren", um deine Einstellungen zu ändern oder alle - außer den zwingend erforderlichen Cookies - abzulehnen.
Möchtest du diese Cookies akzeptieren?
Impressum
Informationen auf einem Gerät speichern und/oder abrufen
Personalisierte Anzeigen und Inhalte, Anzeigen- und Inhaltsmessungen, Erkenntnisse über Zielgruppen und Produktentwicklungen
Genaue Standortdaten verwenden
Geräteeigenschaften zur Identifikation aktiv abfragen
Einstellungen konfigurieren
Ich stimme zu
Menschen
Diese Fotografin macht intime Fo
von ihren verliebten Freunden
"Ich wollte sie nackt fotografieren, um die

– Question


projectbaseline.com/sign-in/
Project Baseline by verily
Sign in
Search opportunities
Help humanity
Shape healthtech
About us
FAQs
Blog
Welcome back to Project Baseline!
Login to continue
Sign-in with Google
Forgot email?
New to Project Baseline?
Join us
Participant support
Baseline FAQs
Baseline Privacy Policy
COVID-19 resources
California County Health Resources
Partner Resources
Enterprise Platform
Study sponsor
Advocacy groups

https://www.vox.com/recode/22351108/dark-patterns-ui-web-design-privacy

recode

By Sara Morrison | Apr 1, 2021, 11:20am EDT

SHARE

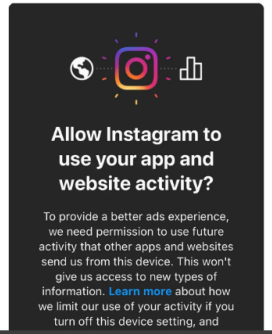
OPEN SOURCED

If you're an Instagram user, you may have recently seen a pop-up asking if you want the service to "use your app and website activity" to "provide a better ads experience." At the bottom there are two boxes: In a slightly darker shade of black than the pop-up background, you can choose to "Make ads less personalized." A bright blue box urges users to "Make ads more personalized."

This is an example of a dark pattern: design that manipulates or heavily influences users to make certain choices. Instagram uses terms like "activity" and "personalized" instead of "tracking" and "targeting," so the user may not realize what they're actually giving the app permission to do. Most people don't want Instagram and its parent company, Facebook, to know everything they do and everywhere they go. But a "better experience" sounds like a good thing, so Instagram makes the option it wants users to select more prominent and attractive than the one it hopes they'll avoid.

There's now a growing movement to ban dark patterns, and that may well lead to consumer protection laws and action as the Biden administration's technology policies and initiatives take shape. California is currently tackling dark patterns in its evolving privacy laws, and Washington state's latest privacy bill includes a provision about dark patterns.

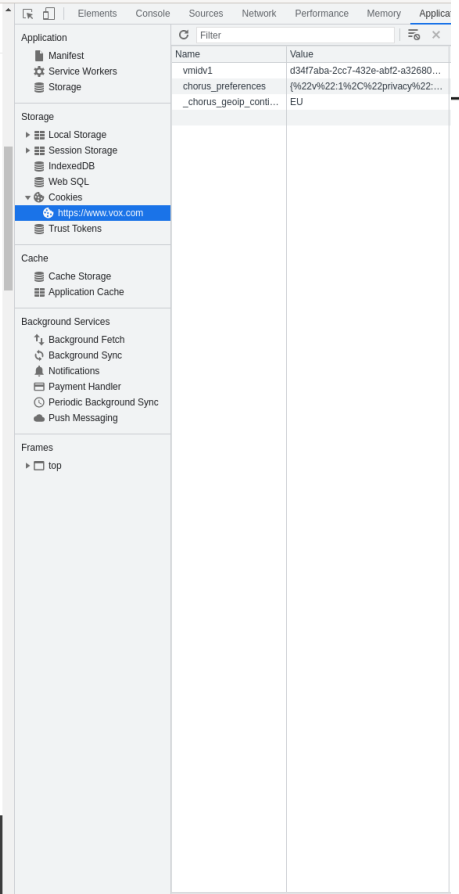
"When you look at the way dark patterns are employed across digital engagement, generally, [the internet allows them to be] substantially exacerbated and made less visible to consumers," Rebecca Kelly



We use cookies and other tracking technologies to improve your browsing experience on our site, show personalized content and targeted ads, analyze site traffic, and understand where our audiences come from. To learn more or opt-out, read our Cookie Policy. Please also read our Privacy Notice and Terms of Use, which became effective December 20, 2019.

By choosing I Accept, you consent to our use of cookies and other tracking technologies.

I Accept



Consent (the controller side)

Maintaining a Record of Consent

- Obligation of the controller to demonstrate a data subject's consent (**and ensure potential withdrawa**l).
- Should keep clear records of what a person has consented to, and when and how you got this consent, so that you can demonstrate compliance in the event of a complaint.
- In particular:
  - date of consent
  - the method of consent
  - who obtained consent,
  - and exactly what information was provided to the person consenting.
- Organizations must make sure that they can produce effective audit trails of how and when consent was given in order to give evidence of consent if challenged.

Challenge: give consent on https://java.com/en (or don't) and try to selectively revoke consent.

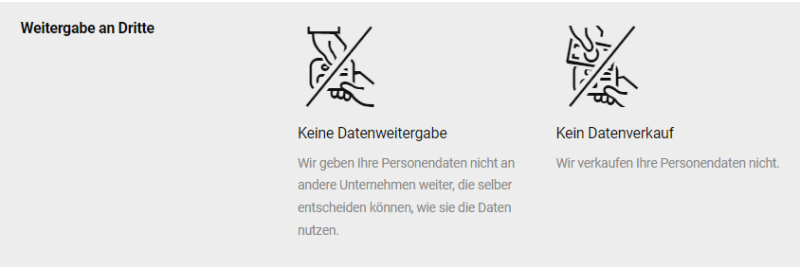
Lawfulness

- All processing of personal data requires a legal basis.
- Additional requirements when processing sensitive persona data.
- Data subjects have the right to receive a data privacy notice when data is collected about them.

Privacy Policy

Goals:

- Basic information and easily understandable description of processing activities.
- Data subject must be well informed after reading.
- Different approaches under development, e.g.: https://privacy-icons.ch/



– Privacy Laws

revDSG / rev DPA

UNIVERSITÄT BERN

- Revised Swiss Data Protection Act (revDPA), 2021-01-01
- Will implement many requirements of GDPR, but some key differences

revDSG / rev DPA

UNIVERSITÄT BERN

- **Core concepts, esp. personal data of natural persons**: Very similar to GDPR
- **Data breach notification**: Very similar
- **DPOs**: Not mandatory
- **Sanctions**: Lighter than GDPR, eg 250’000 CHF for legal entities
- **Cross-border data transfers**: No guidance yet, some tensions wrt GDPR expected

CCPA (California Consumer Protection Act)

UNIVERSITÄT BERN

- In force since 2021-01-01
- Applies to “large” businesses processing data from Californians

- Very similar to GDPR / revDPA in terms of data subject rights, but not a full subset
  - Easier litigation in case of data breaches (at least 100 USD per data subject)
  - Special rules for data brokers (https://oag.ca.gov/data-brokers)
  - Toll-free number for data subjects

Key takeaways

- Importance of data privacy increases
- Enforcement is ramping up around the globe
- See privacy by design and default as a competitive advantage