Global Privacy: Key Developments

Privacy & Technology Law Forum
March 30, 2022

Dr. Gabriela Zanfir-Fortuna
VP Global Privacy, Future of Privacy Forum

Roadmap

1. **Transatlantic Transfers of Personal Data post-Schrems**
    1. Introducing the “Transatlantic Data Privacy Agreement”
    2. So is it all over now? (the ”Google Analytics” cases)
2. **The other side of the coin: Data Localization**
3. **Regulatory trends around the world**
    1. New or updated comprehensive privacy and data protection laws
    2. A regulatory shift: Data Governance – Data Sharing – AI – Digital Markets/Antitrust – Data, personal and non-personal

1. Transatlantic Transfers of Personal Data post-Schrems II

- The CJEU invalidated the EU-US Privacy Shield Agreement in July 2020, following the Schrems II Judgment (post-GDPR)
- The Privacy Shield Framework replaced the Safe Harbor Framework in 2016
- Previously, the CJEU had invalidated the EU-US Safe Harbor Framework in October 2015, following the Schrems Judgment (pre-GDPR)
  - Why? International Data Transfers Rules in EU law require an “Essentially Equivalent Level of Protection of Personal Data” in the third countries where personal data is transferred from the EU; Tiered approach: adequacy > additional safeguards > derogations
  - Key issues in the US: lack of individual redress; lack of independent oversight; lack of necessity and proportionality in government access to personal data -> all of them concerning national security activities and government access to personal data
  - The Court found breaches of the EU Charter of **Fundamental Rights** (Articles 7 – respect for private life; Article 8 – right to the protection of personal data; Article 47 – effective redress)

Landscape Post-Schrems II

- Legal Uncertainty
- Ongoing negotiations (USG – COM)
- Guidance on “supplementary measures” to SCCs (technical, organizational or contractual measures to fill the gaps in protection)
- Will they? Won’t they? (all eyes on DPAs)
- EU DPAs blocking transfers of personal data to the US in individual cases
  - Portuguese DPA – Cloudflare, National Institute of Statistics
  - German Court in Hesse – German University Website, DK-based CookieBot Consent Management Platform using a US based cloud service sub-processor
  - Most significantly: Three different DPA decisions in 2022 against EU based websites that used Google Analytics and Stripe cookies (EDPS, Austrian DPA, CNIL) -> as part of a series of 101 Complaints submitted by noyb in August 2020

The Google Analytics cases: Key findings

1. “Personal data” is being “processed” through cookies, even if users are not identified and even if the cookies are thought to be “inactive”

    1.1 Cookie identification numbers, by themselves, are personal data

    1.2 Cookie identification numbers combined with other elements are additional personal data

    1.3 Controllers and other persons “with lawful means and justifiable effort” will count for the identifiability test

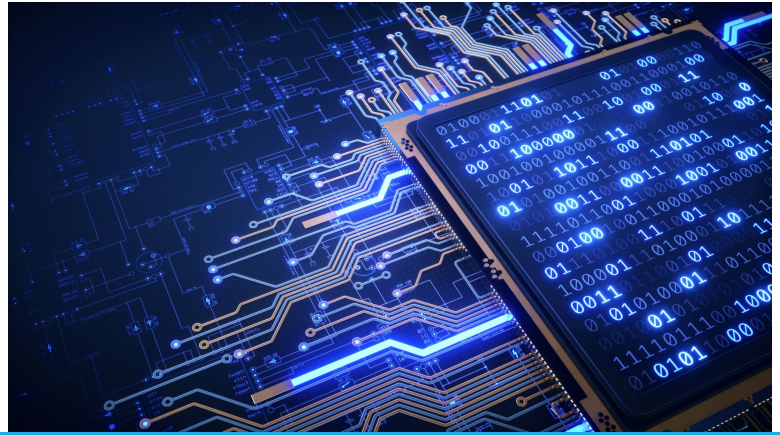
    1.4 Additional information potentially available to US intelligence authorities, taken into account for the identifiability test

2. Data transfers to the US are taking place by placing cookies provided by US-based companies on EU-based websites

2.1 In the absence of an adequacy decision, all data transfers to the US based on “additional safeguards”, like SCCs, need supplementary measures

2.2 Supplementary measures must **“eliminate the possibility of access”** of the government to the data, in order to be effective

What supplementary measures were put in place and considered insufficient by the DPAs?



FUTURE OF PRIVACY FORUM

The **contractual and organizational supplementary measures** considered:

- notification of the data subject about data requests (should this be permissible at all in individual cases),
- the publication of a transparency report,
- the publication of guidelines “for handling government requests”,
- careful consideration of any data requests.

The **technical supplementary measures** considered were:

- the protection of communications between Google services,
- the protection of data in transit between data centers,
- the protection of communications between users and websites,
- “on-site security”,
- encryption technologies, for example encryption of data at rest in data centers,
- processing pseudonymous personal data.

101 Identical Complaints

Strategic complaints

Coordinated Action of DPAs

A quick analysis of the HTML source code of major EU webpages shows that many companies still use Google Analytics or Facebook Connect one month after a major judgment by the Court of Justice of the European Union (CJEU) - despite both companies clearly falling under US surveillance laws, such as FISA 702. Neither Facebook nor Google seem to have a legal basis for the data transfers. Google still claims to rely on

FUTURE OF PRIVACY FORUM

Introducing the “Transatlantic Data Privacy Framework”

An agreement ”in principle” was announced last Friday in Brussels by **US President Joe Biden** and **European Commission President Ursula von der Leyen** for a new data transfers framework

- Significant escalation compared to 2016 and the Privacy Shield announcement
- 2016: February (announcement) – July (adoption)
- The White House and the European Commission published Factsheets after the announcement with very few, but insightful, details

FUTURE OF PRIVACY FORUM

US commitments:

- to “implement new safeguards” to ensure that SIGINT activities are “necessary and proportionate”
- creating a “new mechanism for the EU individuals to seek redress if they believe they are unlawfully targeted by signals intelligence activities”. This new mechanism was characterized by the White House as having “independent and binding authority”
  - “a new multi-layer redress mechanism that includes an **independent Data Protection Review Court** that would consist of individuals chosen from outside the US Government who would have full authority to adjudicate claims and direct remedial measures as needed”.
- “intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards”.

=> All 3 major issues identified by the CJEU will be addressed. But how effectively?

Of note!

One of the remarkable things about the White House announcement is that it includes several EU law-specific concepts: “necessary and proportionate”, “privacy, data protection” mentioned separately, “legal basis” for data flows.

the entire issue of ensuring safeguards for data flows is framed as more than a trade or commerce issue – with references to a “shared commitment to privacy, data protection, the rule of law, and our collective security as well as our mutual recognition of the importance of trans-Atlantic data flows to our respective citizens, economies, and societies”.

US framing the issue as a “privacy and civil liberties” one -> fundamental rights framing in the EU

Now what?

- The Political Agreement is nice, but it does not have legal effects
- The new framework cannot be used for transfers yet => formal adoption of an adequacy decision by the Commission is required
- USG has to adopt an Executive Order (at least) and perhaps take some other internal measures to include these commitments
- It is a matter of several months -> the Commission needs to consult the EDPB/EDPS on the adequacy decision; the European Parliament also has a role to play (even if only advisory); the governments of EU Members get to have a vote as well before final approval
- In the meantime: DPAs and Courts can continue enforcing Schrems II and the GDPR transfer rules

2. The other side of the coin: data localization

- Different shapes and forms: e.g. copies retained in the country, but data may flow outside; no copies or data allowed outside of the country
- Russia and China set the tone
- Increased appetite for positive retention obligations, particularly in Asia (see **Vietnam** and the 2018 Cybersecurity Law, in addition to the currently under debate Data Protection Decree; **India's** Data Protection Bill – which currently provides that sensitive personal data should not be transferred outside of India; **Sri Lanka**'s new Data Protection Law – but seemingly only in relation to personal data processed by government agencies)

China – evolving to a more nuanced approach

- While the new data protection and data security legal framework (PIPL; DSL 2021) solidified and added to pre-existing data localization requirements, it also clarified that data can be transferred or made accessible outside of China if specific conditions are met.
- Under Chinese law, data localization is only required in certain circumstances framed around two distinct conceptual pillars:
  - (1) which entity is processing the data; and
  - 2) what type of data is being processed.
- With respect to the first pillar, **certain special categories of controllers** must store their data in China due to their importance to China's national security and economy, and may only transfer data with the approval of regulatory authorities. For the second, controllers must store **"important data"** in China, and receive approval before transferring such data abroad.

FUTURE OF PRIVACY FORUM

DEMYSTIFYING DATA LOCALIZATION IN CHINA: A PRACTICAL GUIDE

Author: Hunter Dorwart
Policy Counsel, Future of Privacy Forum

February 2022

Source: https://fpf.org/blog/new-fpf-report-demystifying-data-localization-in-china-a-practical-guide/

FUTURE OF PRIVACY FORUM

Personal Data Transfers Requirements

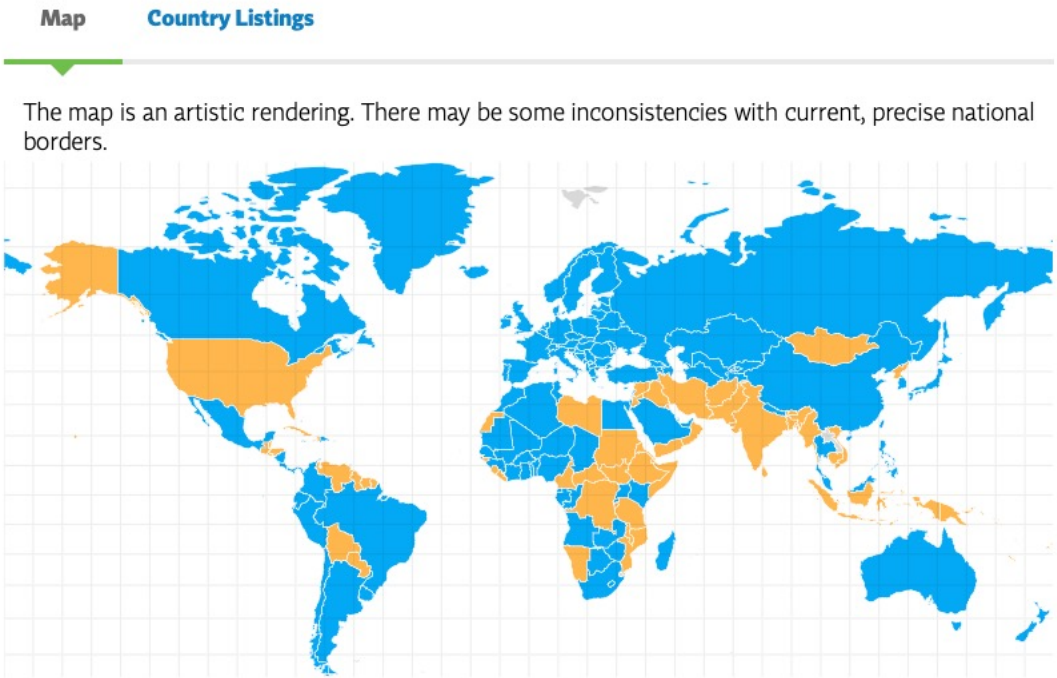
- Are meant to provide safeguards for the personal data being transferred, therefore, theoretically, their goal is to **facilitate** transfers, not to blanket block them
- Are being included in all modernized (post-GDPR) or newly adopted comprehensive data protection laws around the world, with a notable exception (can you guess?)
- Data localization regimes are most of the time a result of provisions in cybersecurity laws and other special laws, but they can be combined with data protection law provisions (e.g. Vietnam; China); a worrying trend is starting to see localization obligations in new data protection laws under cross-border transfer requirements (India; Sri Lanka for the public sector)

3. Regulatory Trends around the World

Blue: Comprehensive data protection law

Orange: Sectoral coverage or no data protection

Source: IAPP
https://iapp.org/resources/global-privacy-directory/



FUTURE OF PRIVACY FORUM

Only if we look back to the past couple of years…

New Comprehensive Data Protection/Privacy Laws:

China: PIPL, adopted Aug 2021, entered into force November 2021

California: CCPA (2018 -> 2020) -> CPRA (2020 -> 2023) (+ **Colorado** 2021, **Virginia** 2021; **Utah** 2022)

Brazil: LGPD (2020)

Kenya (2019)**, Egypt** (2020)**, Saudi Arabia** (2021 -> 2023)

Sri Lanka: adopted last week!

*__South Africa__ (entered into force 2021)

Updates/Amendments: **Japan** (2020 -> 2022), **South Korea** (2020), **Singapore** (2020), **New Zealand** (2020)

Ongoing Bills or Public Consultations: **India**; **Australia**; **Canada; Vietnam; Chile**

Looking towards the future…

- Personal Data/Non-Personal data blurred lines (EU's DGA and Data Act; India's Data Protection Bill)
- Next level of data governance regulation, focused on making data available for the public good, data sharing, data pooling (EU's Data Act, Data Governance Act)
- AI – but overlap with general data protection laws
- Competition in Digital Markets (EU's Digital Markets Act targeting "gatekeepers" with ex ante obligations)
- Dealing with online platforms (EU's DSA, but also India's already adopted IT Guidelines; Brazil; Australia)

FUTURE OF PRIVACY FORUM

Questions?

gzanfir-fortuna@fpf.org
@gabrielazanfir
www.fpf.org

FUTURE OF PRIVACY FORUM