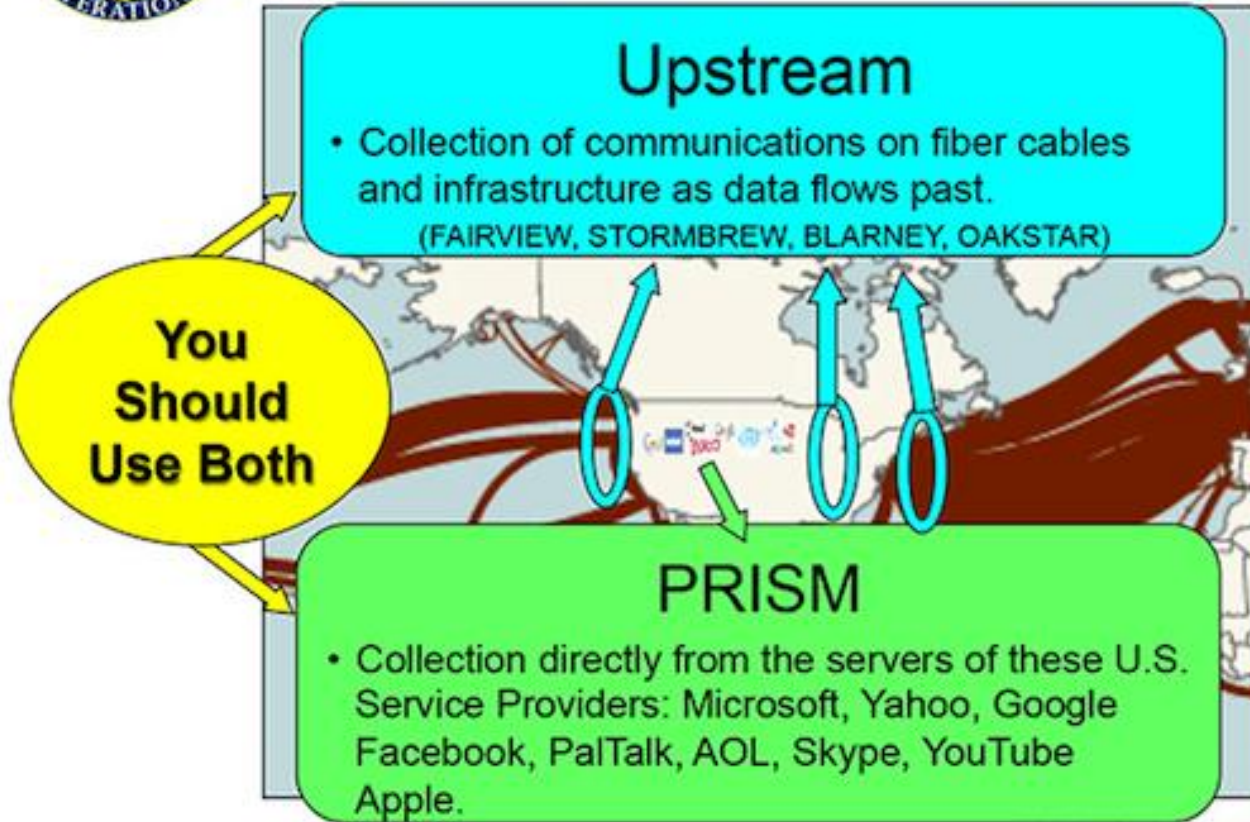


**CONFLICT OF JURISDICTIONS:  
WHO GOVERNS WHERE THIS IS RUNNING ON?**



# (TS//SI//NF) FAA702 Operations

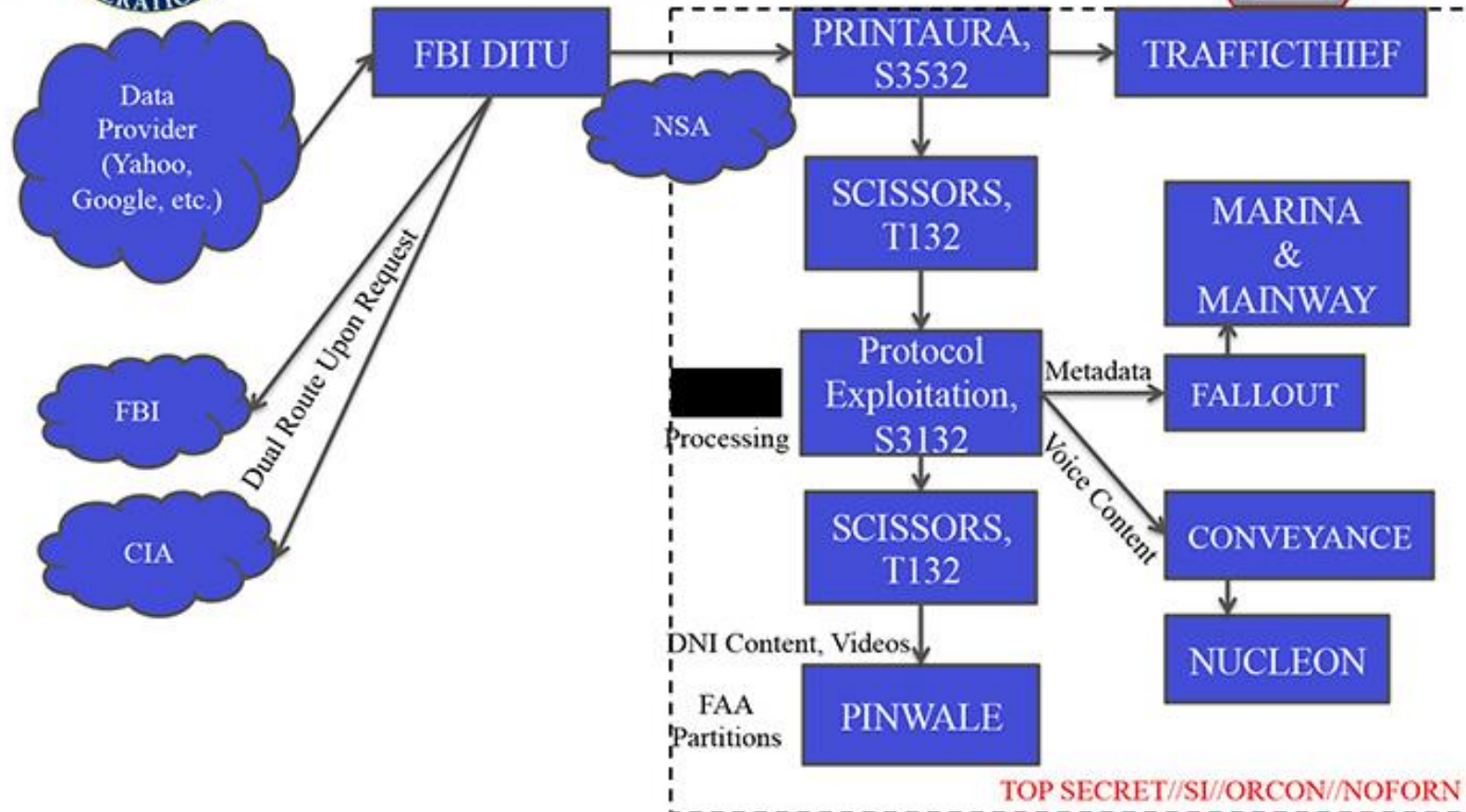
*Two Types of Collection*



TOP SECRET//SI//ORCON//NOFORN



# (TS//SI//NF) PRISM Collection Dataflow





# (TS//SI//NF) PRISM Case Notations

## P2ESQC120001234

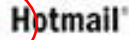
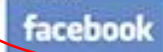
- PRISM Provider
- P1: Microsoft
  - P2: Yahoo
  - P3: Google
  - P4: Facebook
  - P5: PalTalk
  - P6: YouTube
  - P7: Skype
  - P8: AOL
  - PA: Apple

Fixed trigraph, denotes PRISM source collection

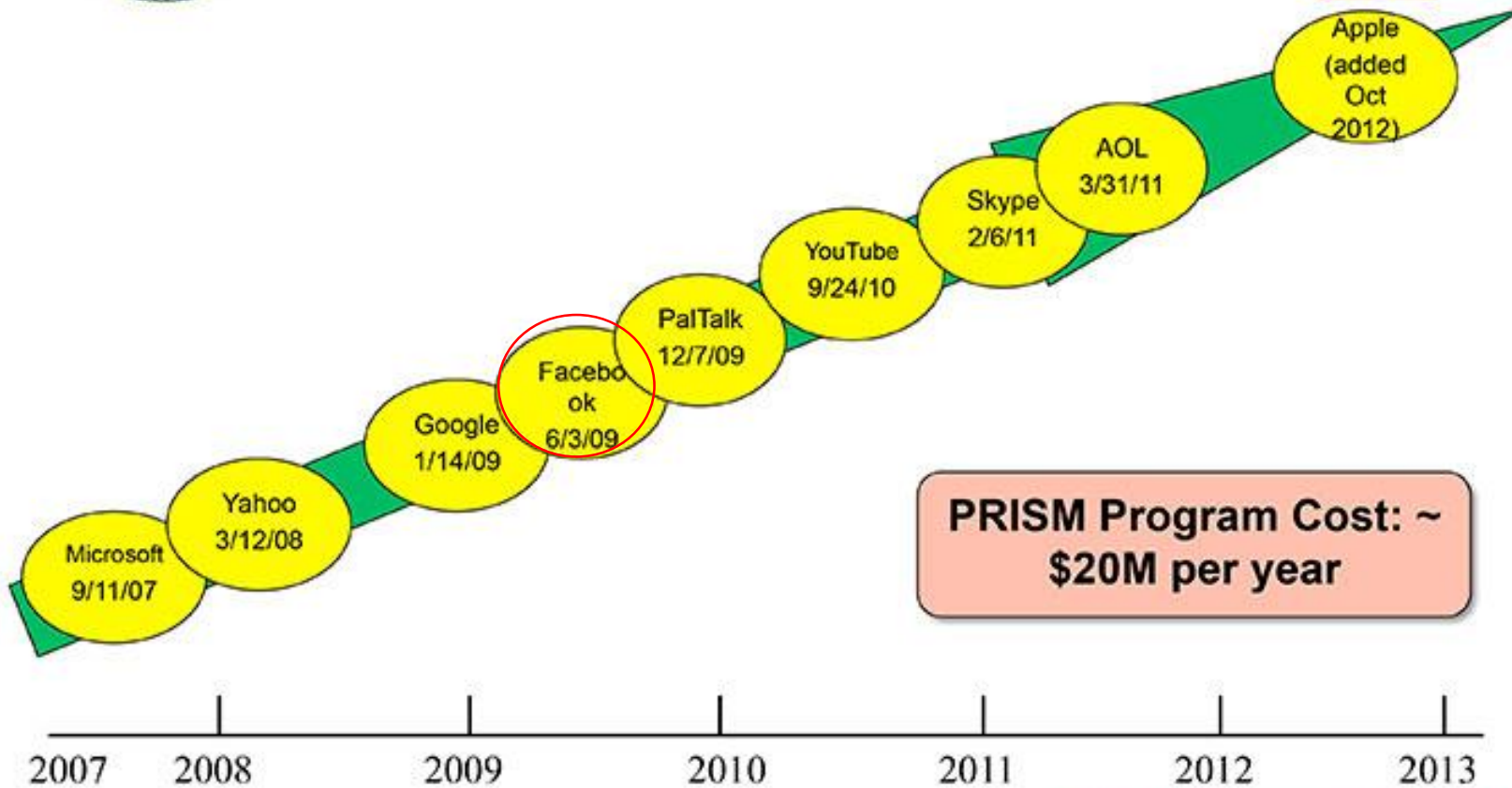
Year CASN established for selector

Serial #

- Content Type**
- A: Stored Comms (Search)
  - B: IM (chat)
  - C: RTN-EDC (real-time notification of an e-mail event such as a login or sent message)
  - D: RTN-IM (real-time notification of a chat login or logout event)
  - E: E-Mail
  - F: VoIP
  - G: Full (WebForum)
  - H: OSN Messaging (photos, wallposts, activity, etc.)
  - I: OSN Basic Subscriber Info
  - J: Videos
  - . (dot): Indicates multiple types



# (TS//SI//NF) Dates When PRISM Collection Began For Each Provider



**PRISM Program Cost: ~ \$20M per year**

2007 2008 2009 2010 2011 2012 2013

# FISA 702 (= 50 USC § 1881a)

noyb

- Electronic Communication Service Provider
  - “Foreign Intelligence Information”
- 
- “Certification” for one year („FISA Court”)
    - Minimizing / Targeting procedures (US persons)
  - “Directive” to the Service Provider
    - API (?)

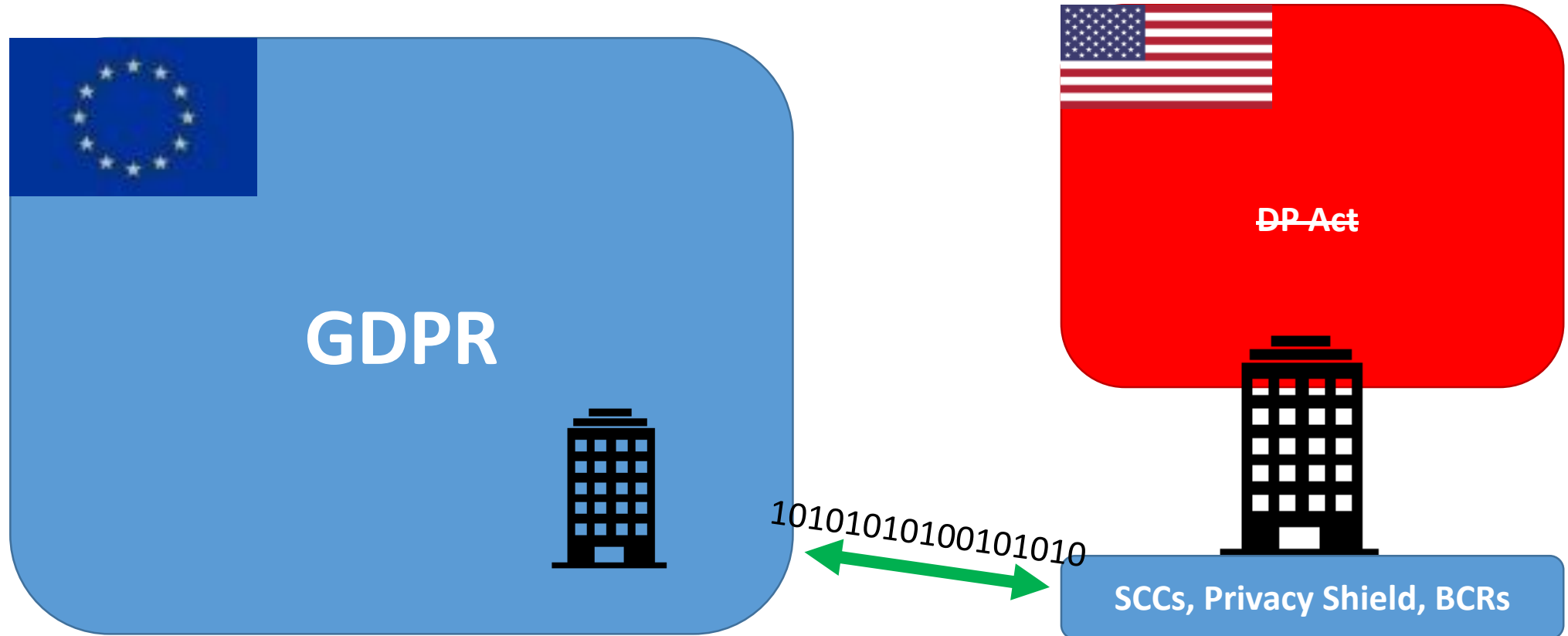
**CLASSIFIED**



# DATA TRANSFERS

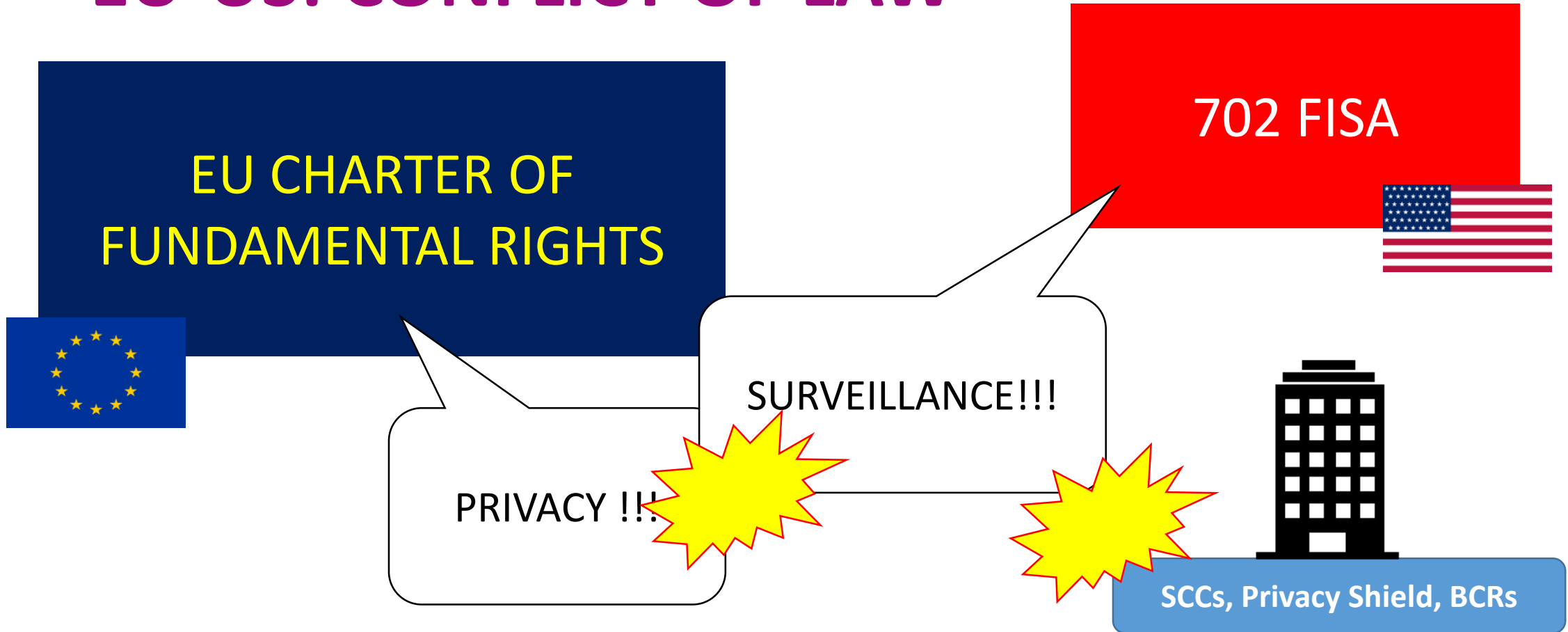
- **General Rule:** Export Prohibition on Personal Data
  - **Derogations:** “Necessary transfers”, non-structural (Art 49)
  - **Outsourcing:**
    - Adequacy (Art 45)
    - Standard Contractual Clause / Model Clauses (Art 46)
    - Binding Corporate Rules (Art 47)
- Expansion of GDPR rules in non-EU country

# PRIVACY “BUBBLE”: CONTRACTUAL





# EU-US: CONFLICT OF LAW



# FIRST ROUND: „SCHREMS I“

# RTE



*„I don't think it will come as much of a surprise that in fact US intelligence services do have access from US companies“*

Dear Mr Schrems,

With reference to your letter of 29<sup>th</sup> July 2013, please see the following points.

As previously stated, we consider that we have set out our position clearly in previous correspondence and the fact that we choose not to comment on all arguments you have presented should not be taken to mean that we agree with them. We therefore reserve the right to argue them as necessary in the course of judicial review proceedings.

„shall“= „may“

„frivolous“

To be clear we remain of the position that there is a basis within the Data Protection Acts 1988 and 2003 for the Commissioner to make a determination not to investigate a complaint and that in Judicial Review proceedings we reserve the right to seek to rely on Sections 10 (1) (a), 10 (1) (b) (i) or a combination thereof or indeed any other relevant legal basis including previous High Court decisions, in defending our position on this point or, should it arise, defending our position that there is no basis for an investigation of this complaint (“Complaint 23”).

Please be advised that we can no longer respond in detail to further correspondence where you seek to summarise or limit our position in this matter and instead we will refer you to our correspondence to date on this matter.

Yours sincerely,



Ciara O'Sullivan  
Senior Compliance Officer



# “ESSENCE”



1. Legitimate aim for the measure
2. Measure suitable to achieve the aim
3. Measure must be necessary to achieve the aim (Less onerous way?)
4. Measure must be reasonable, considering the competing interests of different groups at hand

# OTHER FINDINGS

- “Essentially Equivalent” Protection in 3<sup>rd</sup> Country
- Effective Detection and Supervision Mechanisms
- Legal Redress in Line with Art 47 CFR

*...higher standard than many MS?*





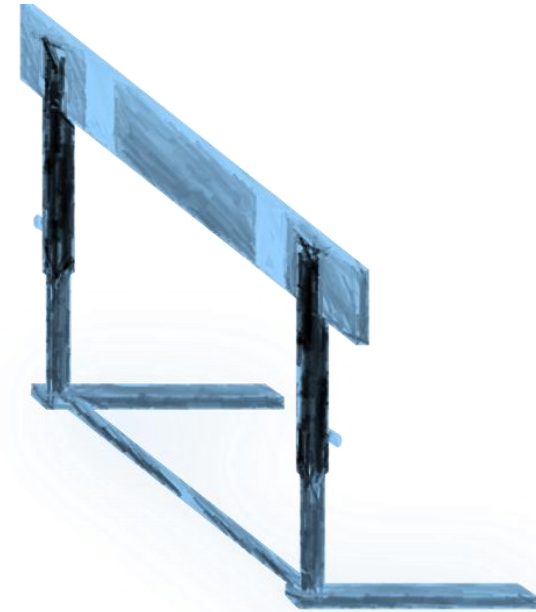
≈ **GDPR**



Art 44-50 of GDPR  
*„Ess. Equivalent“*



= **CFR**



CFR  
Art 7, 8 & 47







***“The US authorities ... assured there is no indiscriminate or mass surveillance by national security authorities.”***

## ANNEX VI, PAGE 4

PPD-28 also provides that signals intelligence collected in bulk can only be used for six specific purposes: detecting and countering certain activities of foreign powers; counterterrorism; counter-proliferation; cybersecurity; detecting and countering threats to U.S. or allied armed forces; and combating transnational criminal threats, including sanctions evasion. The President's National Security Advisor, in consultation with the Director for National Intelligence (DNI), will annually review these permissible uses of signals intelligence collected in bulk to see whether they should be changed. The DNI will make this list publicly available to the maximum extent feasible, consistent with national security. This provides an important and transparent limitation on the use of bulk signals intelligence collection.

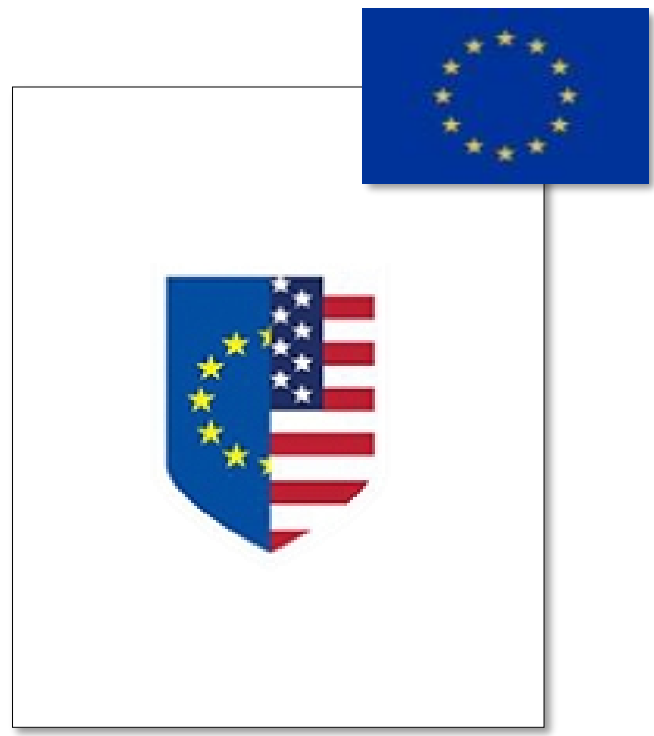
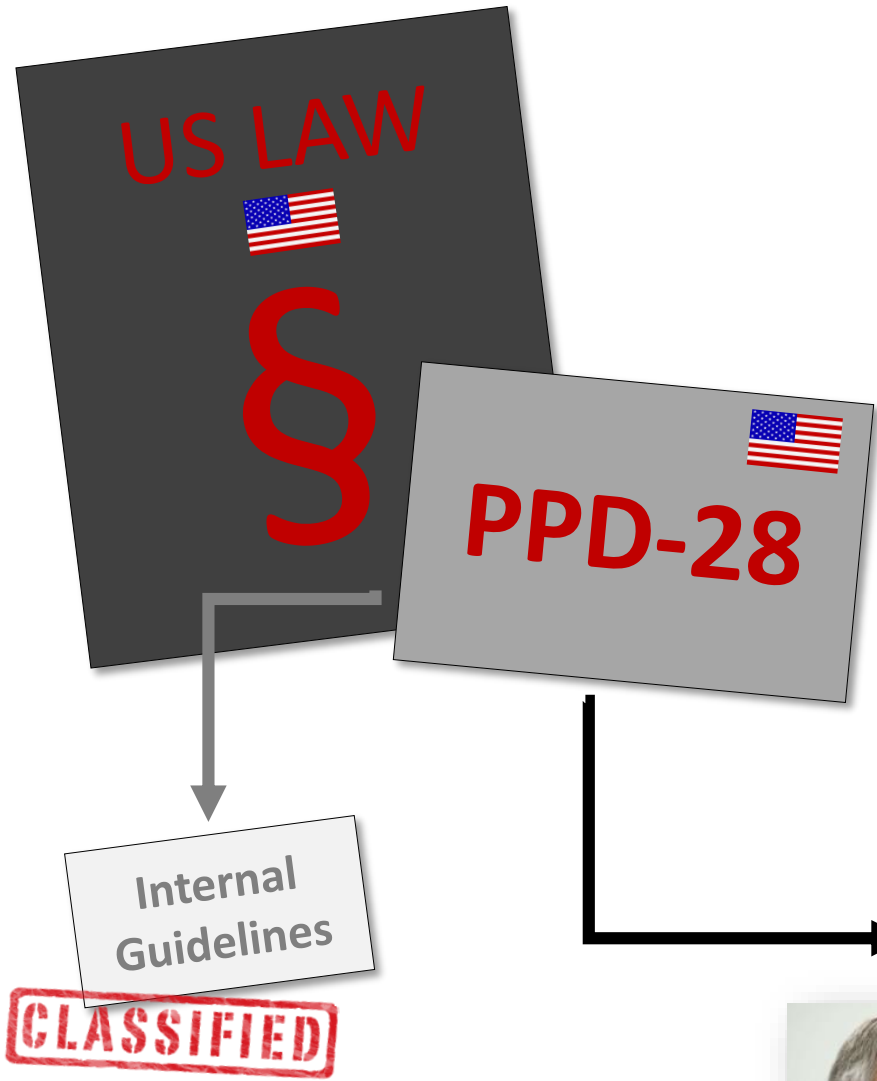
# PPD-28, PAGE 3

## Sec. 2. Limitations on the Use of Signals Intelligence Collected in Bulk.

Locating new or emerging threats and other vital national security information is difficult, as such information is often hidden within the large and complex system of modern global communications. The United States must consequently collect signals intelligence in bulk<sup>5</sup> in certain circumstances in order to identify these threats. Routine communications and communications of national security interest increasingly

# PPD-28, PAGE 3, FN 5

<sup>5</sup> The limitations contained in this section do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection. References to signals intelligence collected in "bulk" mean the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.).





DPA



(i) „has been investigated“  
(ii) „complied or remedied“

*„will neither confirm nor deny that whether the individual has been the target of surveillance“ nor „confirm specific remedy“*

*ANNEX III, Paragraph 4(e)*

# PRIVACY SHIELD - LIPSTICK ON A PIG?!





# SECOND ROUND: „SCHREMS II“

## Standard Contractual Clauses Case („DPC vs. Facebook & Schrems“):

- About 20 Solicitors / Barristers
- 6 weeks of Hearings in Ireland
- 45.000 pages of documents
- Four “Amicus” (EPIC, US Gov, BSA, DigitalEurope)
- Costs expected to be up to € 10 million

# CORE ARGUMENTS



- Facebook said it never used Safe Harbor, but SCCs
  - ➔ **No Surveillance beyond EU Law / No Problem (“Go away!”)**
- Schrems demanded the Irish DPC to make use of Article 4 of the SCCs for Facebook only
  - ➔ **Targeted Solution for FISA companies only (“Use Art 4!”)**
- Irish DPC identified a “systematic” problem and took the view the SCCs are invalid as a whole
  - ➔ **Invalidation of SCCs worldwide (“Nuclear Option”)**



**OUTCOME: CJEU**

# OUTCOME: PROCEDURAL LAW



**The “solution” is Article 4 of the SCCs** *(everyone but the DPC)*

- Individual enforcement action on “FISA” companies
- Invalidation of SCCs not relevant anymore

**Duty of DPAs to enforce the GDPR**

# OUTCOMES: MATERIAL LAW




**Facts:** “Mass Surveillance” became “Mass Processing”

**US Surveillance Law is not “proportionate” (less than in Schrems I)**

**US Redress is a violation of the “essence” (as in Schrems I)**

# **OUTCOME: PRACTICAL CONSEQUENCES**

# DATA TRANSFERS

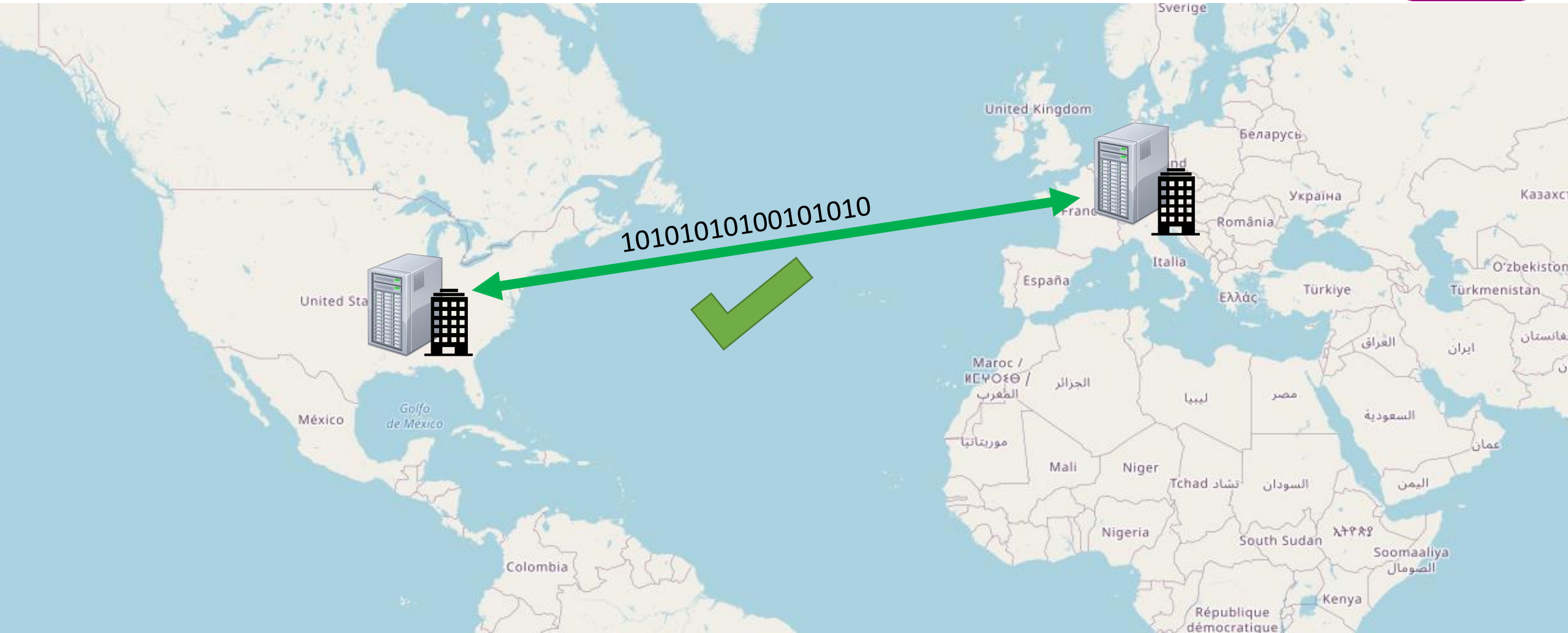
- **General Rule:** Export Prohibition on Personal Data
- **Derogations:** “Necessary transfers”, non-structural (Art 49)
- **Outsourcing:** 
  - Adequacy (Art 45)
  - Standard Contractual Clause / Model Clauses (Art 46)
  - Binding Corporate Rules (Art 47)

Expansion of  
GDPR rules in  
non-EU country

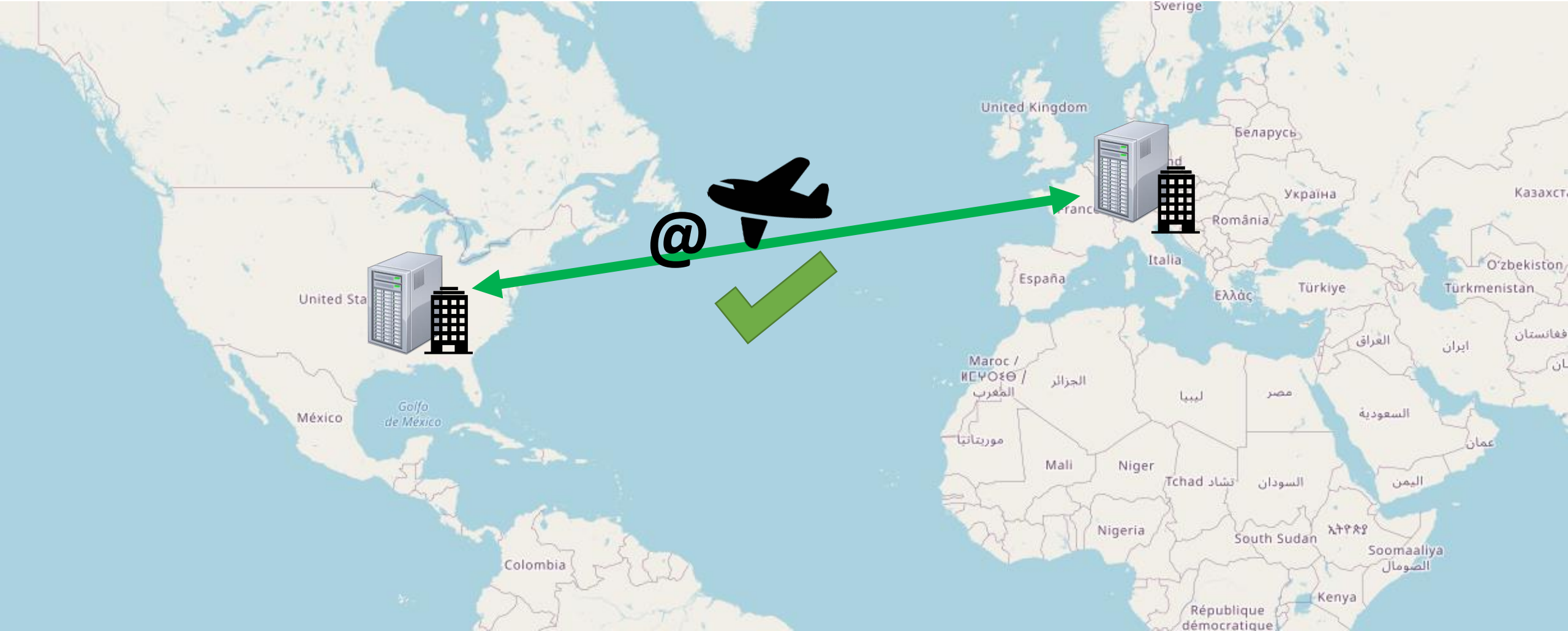


# TRANSFERS: NON-PERSONAL DATA

noyb

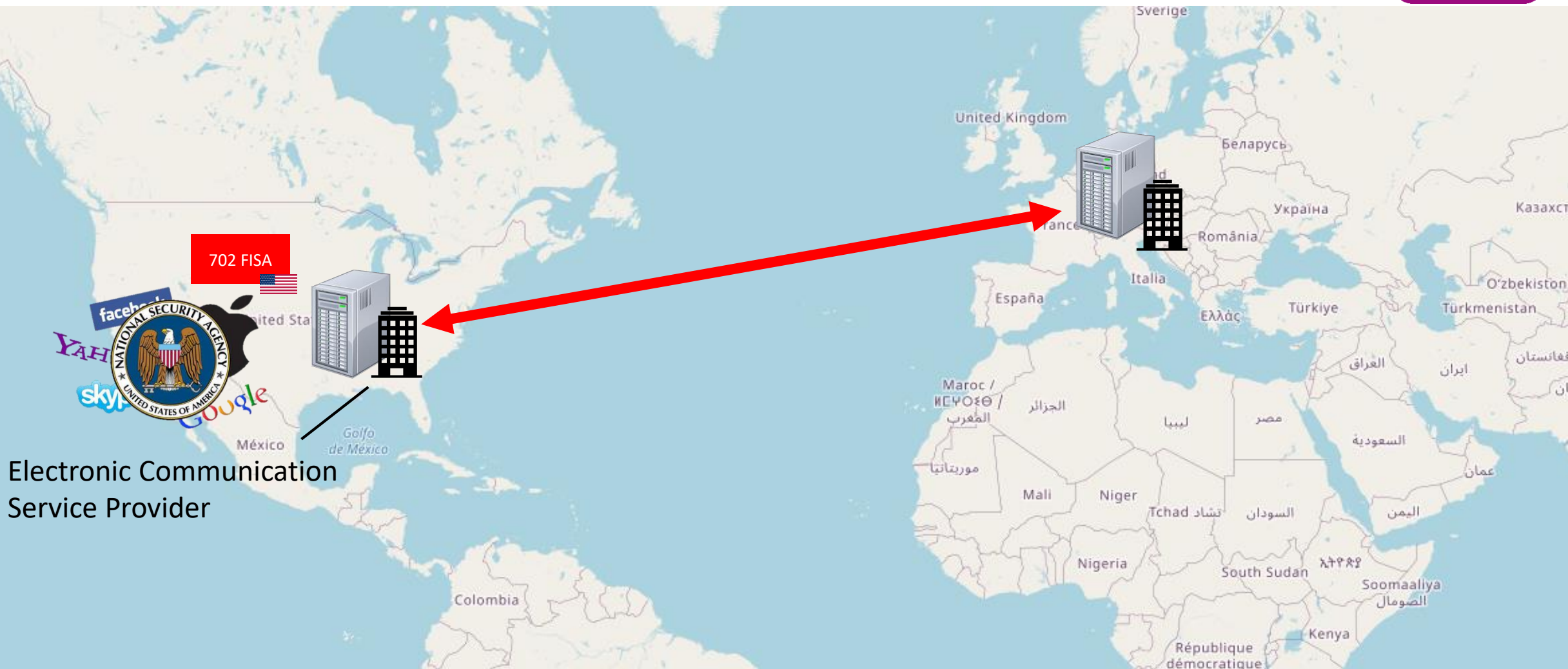


# TRANSFERS: NECESSARY TRANSFERS

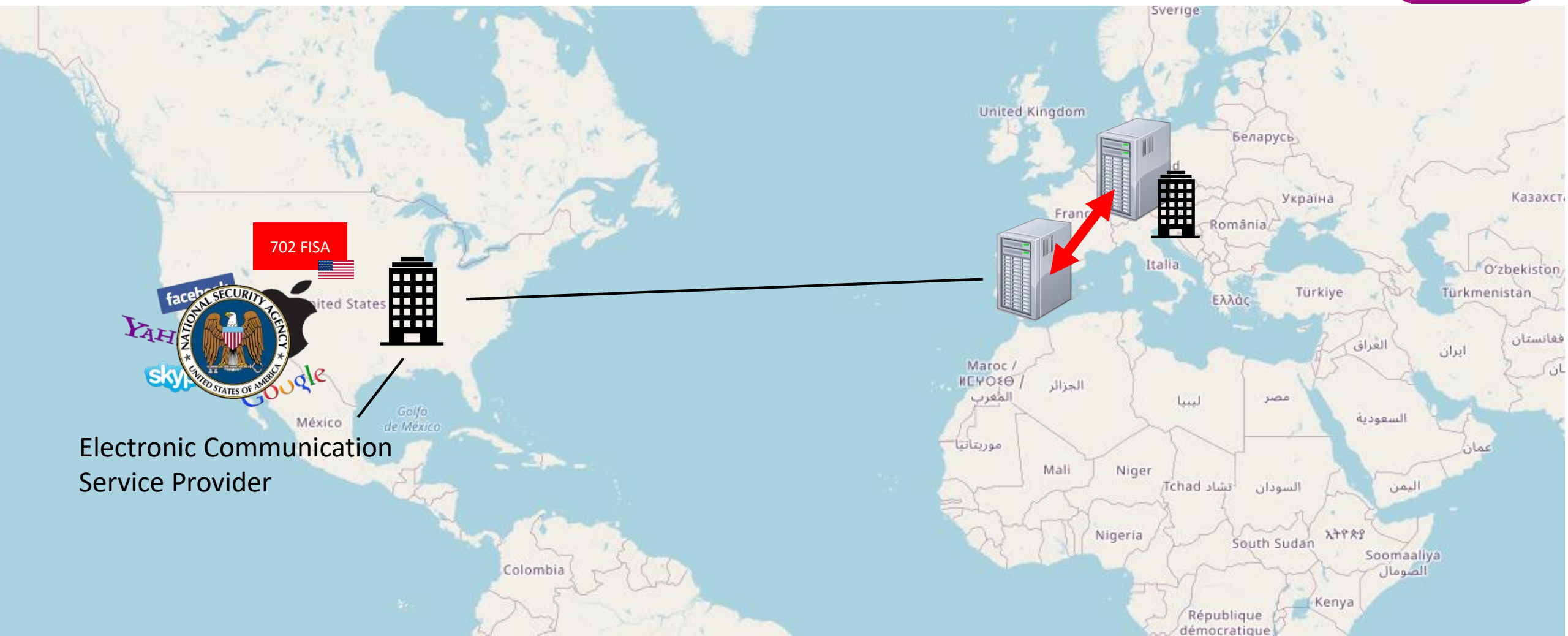


# TRANSFERS: “OUTSOURCING” (FISA) - USA

noyb



# TRANSFERS: “OUTSOURCING” (FISA) - EU

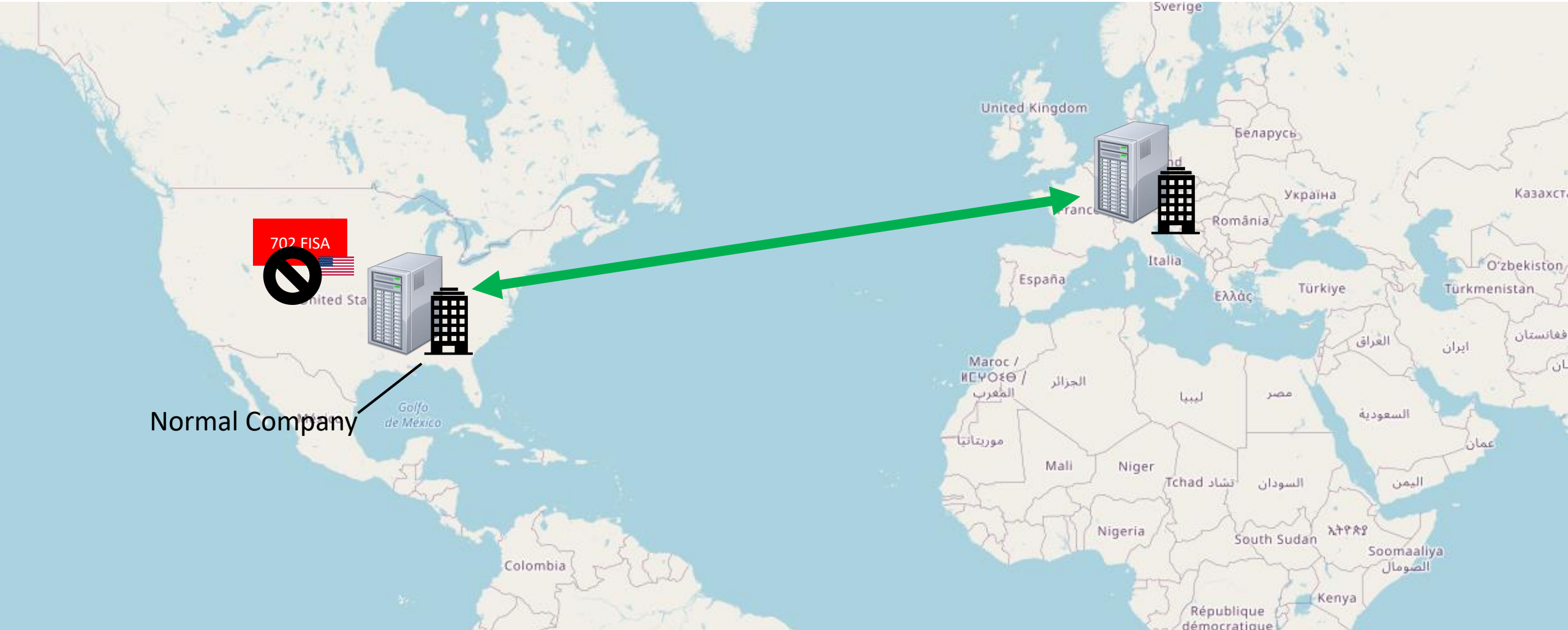


702 FISA



Electronic Communication Service Provider

# TRANSFERS: NON-FISA



**SOLUTION: „SUPPLEMENTARY MEASURES“**

# SUPPLEMENTARY MEASURES

## • Technical

- Encryption („Transit“)
- Encryption (Backups)
- „Zero Knowledge“



## • Contractual

- Disclosure
- Information
- „Resistance“



---

### Scenarios in which *no effective* measures could be found

---

87. The measures described below under certain scenarios would not be effective in ensuring an essentially equivalent level of protection for the data transferred to the third country. Therefore, they would not qualify as supplementary measures.

Use Case 6: Transfer to cloud services providers or other processors which require access to data in the clear

88. A data exporter uses a cloud service provider or other processor to have personal data processed according to its instructions in a third country.

If

1. a controller transfers data to a cloud service provider or other processor,
2. the cloud service provider or other processor needs access to the data in the clear in order to execute the task assigned, and
3. the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society,<sup>71</sup>

---

<sup>71</sup> See Articles 47 and 52 of the EU Charter of Fundamental Rights, Article 23.1 GDPR, and EDPB Recommendations on the European Essential Guarantees for Surveillance Measures.



#### Use Case 7: Remote access to data for business purposes

90. A data exporter makes personal data available to entities in a third country to be used for shared business purposes. A typical constellation may consist of a controller or processor established on the territory of a Member State transferring personal data to a controller or processor in a third country belonging to the same group of undertakings, or group of enterprises engaged in a joint economic activity. The data importer may, for example, use the data it receives to provide personnel services for the data exporter for which it needs human resources data, or to communicate with customers of the data exporter who live in the European Union by phone or email.

If

1. a data exporter transfers personal data to a data importer in a third country by making it available in a commonly used information system in a way that allows the importer direct access of data of its own choice, or by transferring it directly, individually or in bulk, through use of a communication service,
2. the importer uses the data in the clear for its own purposes,
3. the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society,

then the EDPB is incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights.

91. In the given scenarios, where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys.



Max Schrems     
@maxschrems

...

The #Microsoft "supplementary measures" on #SchremsII / #FISA702 in a 5 minute legal bullsh\*t analysis (powered by Microsoft PowerPoint).. 😊

(free to copy/used - especially for any legal department)

- First, we are committing that we will challenge every government request for public sector or enterprise customer data – from any government – where there is a lawful basis for doing so. This strong commitment goes beyond the proposed recommendations of the EDPB.
  - Second, we will provide monetary compensation to these customers' users if we disclose their data in response to a government request in violation of the EU's General Data Protection Regulation (GDPR). This commitment also exceeds the EDPB's recommendations. It shows Microsoft is confident that we will protect our public sector and enterprise customers' data and not expose it to inappropriate disclosure.
- We call these protections [Defending Your Data](#) and we will begin adding them to our contracts with public sector and enterprise customers immediately.
- Defending Your Data makes a substantial addition to our [foundational privacy promises](#), and builds on the strong protections we already offer customers.
- **We use strong encryption:** We encrypt customer data with a high standard of encryption both when it is in transit and at rest. Encryption is a critical point in the draft EDPB recommendations. We do not provide any government with our encryption keys or any other way to break our encryption.
  - **We stand up for customer rights:** We do not provide any government with direct, unfettered access to customer data. If a government demands customer data from us, it must follow applicable legal process. We will only comply with demands when we are clearly compelled to do so. Our first step is always to attempt to re-direct such orders to customers or to inform them, and we routinely deny or challenge orders when we believe they are not legal.
  - **We are transparent:** We have, for many years, published information about government demands for customer data. We sued the U.S. government over the ability to disclose more data about the national security orders we receive seeking customer data and reached a settlement enabling us to do so. As a result, twice a year, we [disclose](#) more detailed information about these national security orders across all our businesses (consumer, enterprise, and public sector), in addition to our regular [Law Enforcement Request Report](#).
  - **We have a track record of legal success.** We have more experience than any other company going to court to establish the limits of government surveillance orders, and we have even taken one case to the U.S. Supreme Court. Our efforts have provided customers with greater transparency and stronger protections. No commitment to challenge access orders can assure victory, but we feel good about our record of success to date.

- Duty under Article 6(1)(c) – if there is no duty to comply (illegal request) then you can't provide the data... Challenging it is the logical consequence - nothing new...
- Duty under Article 82 GDPR, but without all the limits (no class action, burden of proof on the user, etc) that Microsoft put into its contract and that would actually limit (!) data subjects' (third party) rights!
- Required under Article 32 GDPR - big News.
- Yeah, so Microsoft complies with FISA 702 which is the „legal process“.
- Yeah, so you even disclose that you provided the data of 28.500 to 29.998 accounts in 2019.
- Congrats, good job on SCA – but frankly overtured by the Cloud Act and irrelevant when this is about FISA 702.

**facebook**®





**CNIL.**  
COMMISSION NATIONALE  
INFORMATIQUE & LIBERTÉS

**dsb** Republik Österreich  
Datenschutz  
behörde



**EUROPEAN DATA PROTECTION SUPERVISOR**  
The EU's independent data protection authority



**AUTORITEIT  
PERSOONSGEGEVENS**



**PROPER SOLUTION: LEVEL THE PROTECTION**



# PROPOSED SOLUTION: EU-US „FRAMEWORK“



# ANNOUNCEMENT 03/2022

- **Executive Order to introduce „proportionate and necessary“ in US**
  - CJEU found FISA 702 not to be „proportionate and necessary“
  - EU or US meaning?
  - Legally binding effects?
- **„Data Protection Court“**
  - Not a court, but an executive body
  - Only review under APA
- **No changes on commercial data useage?**
  - Principles (from 2000) hardly in line with GDPR

# QUESTIONS & ANSWERS