

# NOYB: BACKGROUND

# NOYB



- European NGO in Vienna
- Strategic Litigation
- About 5.500 members
- Team:
  - Board: 3
  - Legal: 10
  - Tech: 3
  - PR: 2
  - Admin: 5



# TWO ENFORCEMENT TYPES

- **Standard Setting Cases**

- Unclear legal situation
- Different decisions
- Novel issues

- **Enforcement Cases**

- Clear legal situation
- Lack of compliance



# **EU-US DATA TRANSFERS: UPSIDES AND DOWNSIDES OF THE NEW FRAMEWORK**



# PART 1: RECAP



# **SURVEILLANCE: US SIDE OF THE STORY**



Government control starts between your ears when you tell yourself what your masters told you.

astors Cold

THOSE WHO SACRIFICE FREEDOM & SECURITY DESERVE NEITHER.

1984 IS NOW

Die NSA wusste schon vorher, was für ein Schild ich malen würde. Fuck #PRISM

Ich was nach YES WE SCAN

You are the first Afro PRESIDENT need to also be censored for the SYSTEM?



TOP SECRET//SI//ORCON//NOFORN



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

Two Types of Collection



## Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.  
(FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

You Should Use Both

## PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.

**+10 Years**

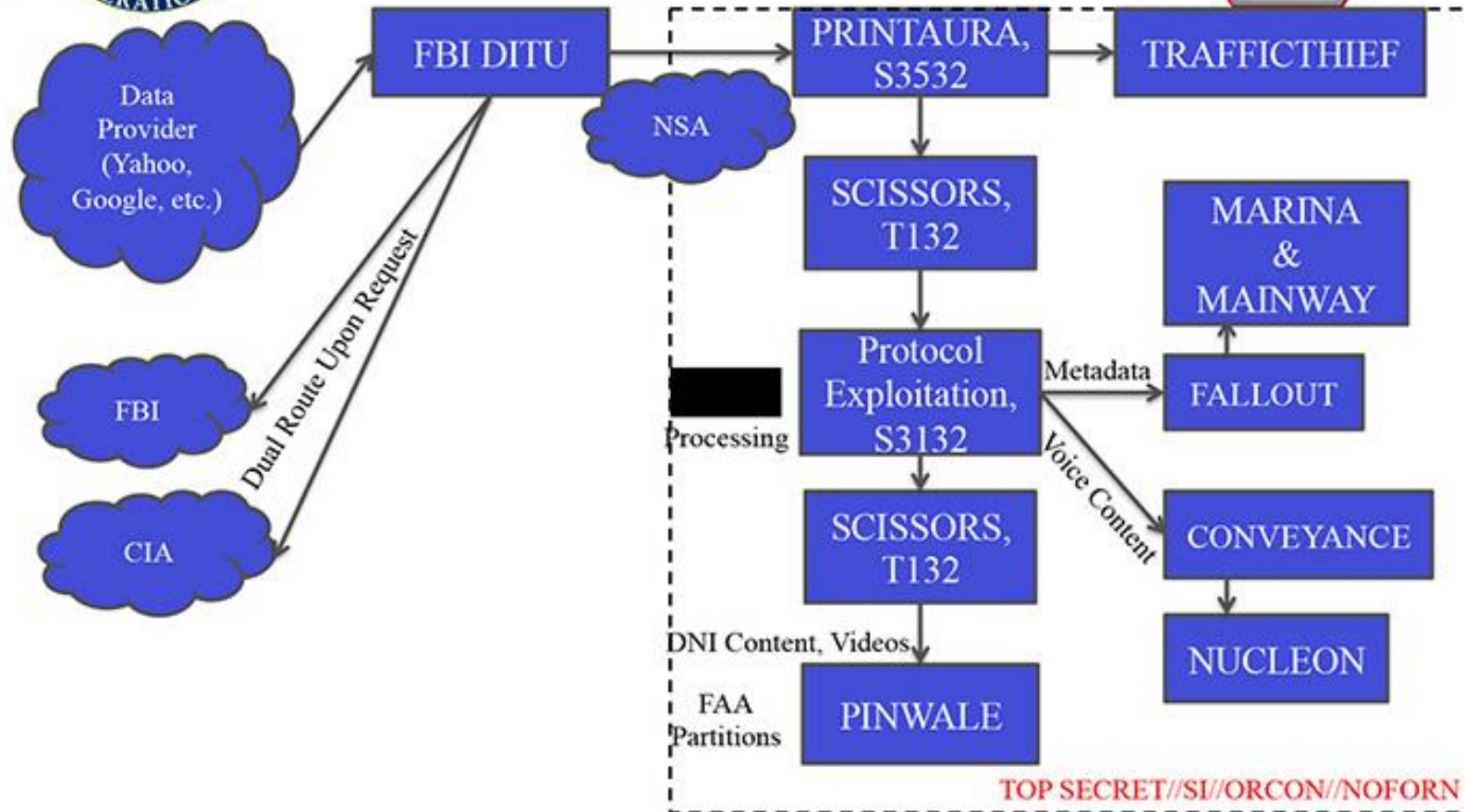




TOP SECRET//SI//ORCON//NOFORN



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





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

*Why Use Both: PRISM vs. Upstream*

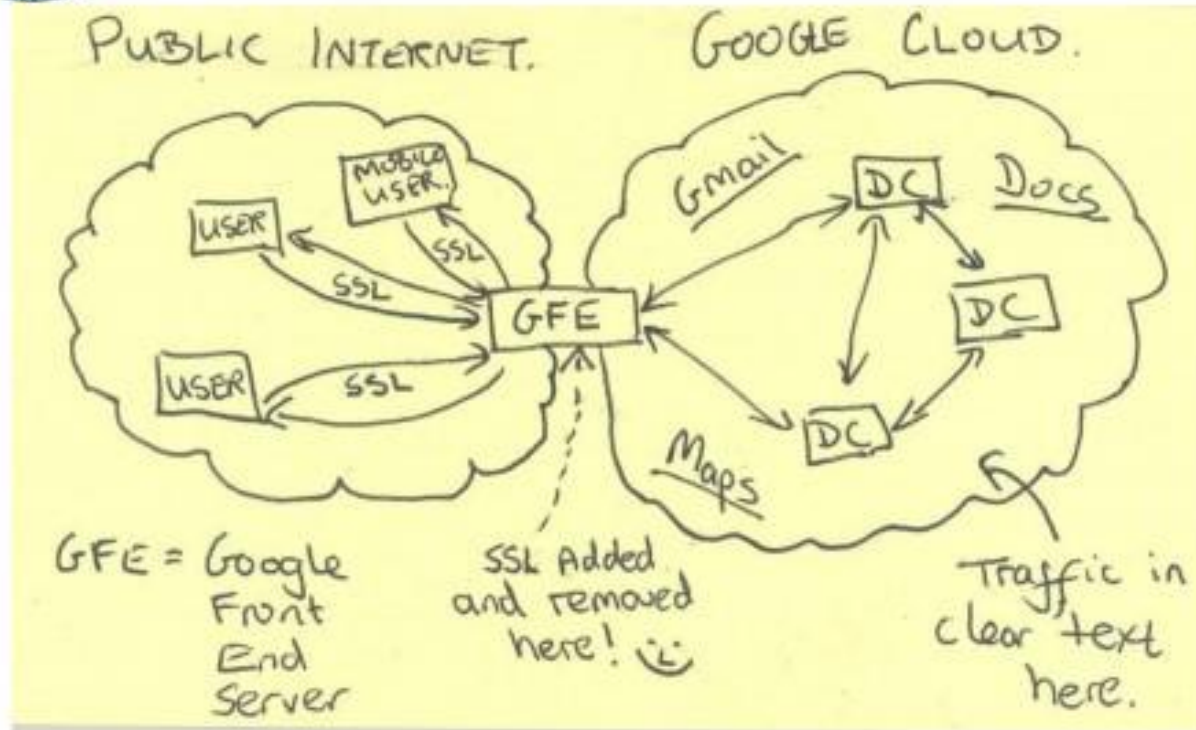


	PRISM	Upstream
DNI Selectors	9 U.S. based service providers ✓	Worldwide sources ✓
DNR Selectors	Coming soon ❌	Worldwide sources ✓
Access to Stored Communications (Search)	✓	❌
Real-Time Collection (Surveillance)	✓	✓
“Abouts” Collection	❌	✓
Voice Collection	✓ Voice over IP	✓
Direct Relationship with Comms Providers	❌ Only through FBI	✓





# Current Efforts - Google



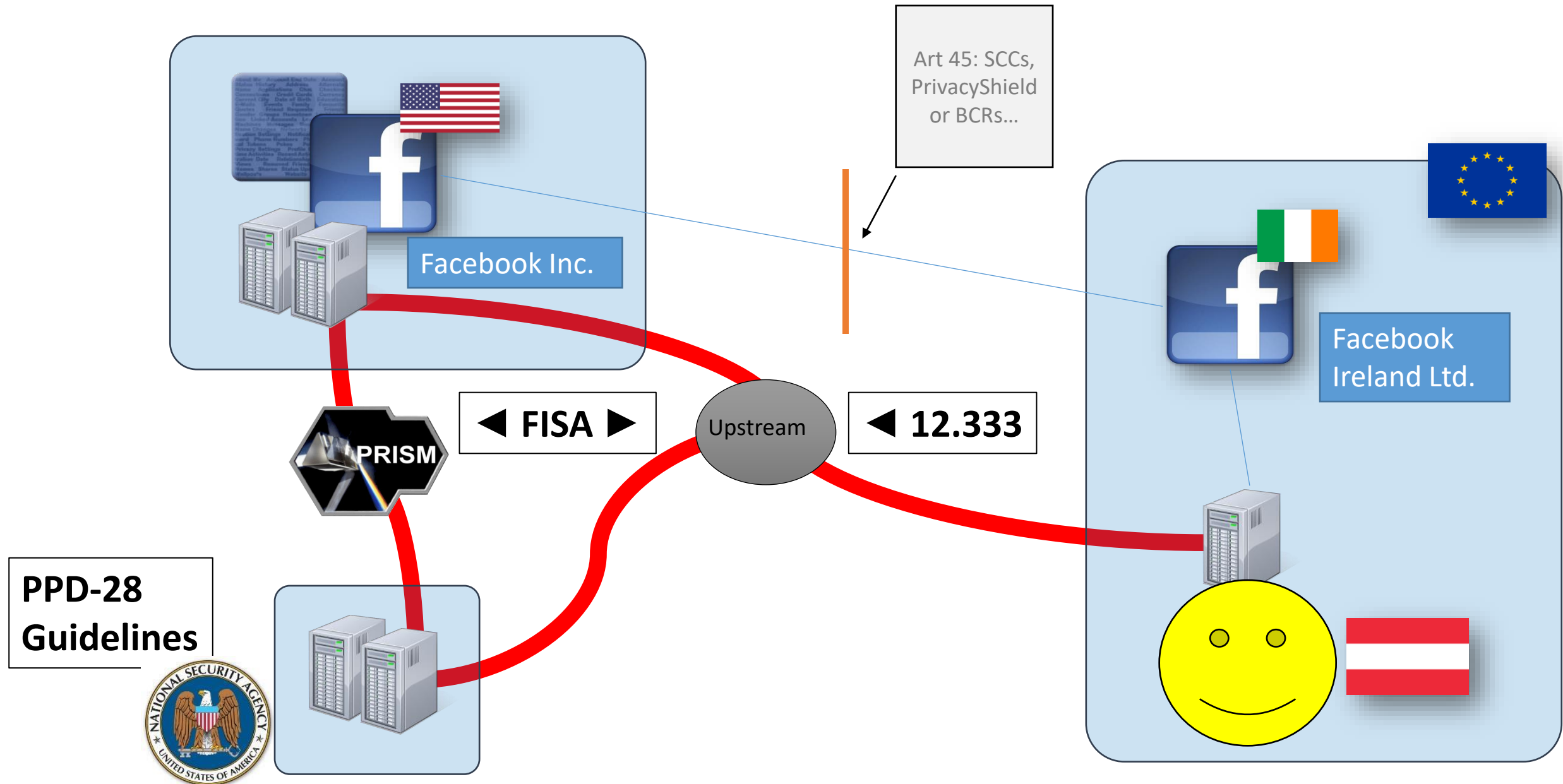
# FISA 702 (= 50 USC § 1881a)

- **Electronic Communication Service Provider**
- **“Foreign Intelligence Information”**
  - *“Information that relates to ... the conduct of the foreign affairs of the US.”*

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

**CLASSIFIED**





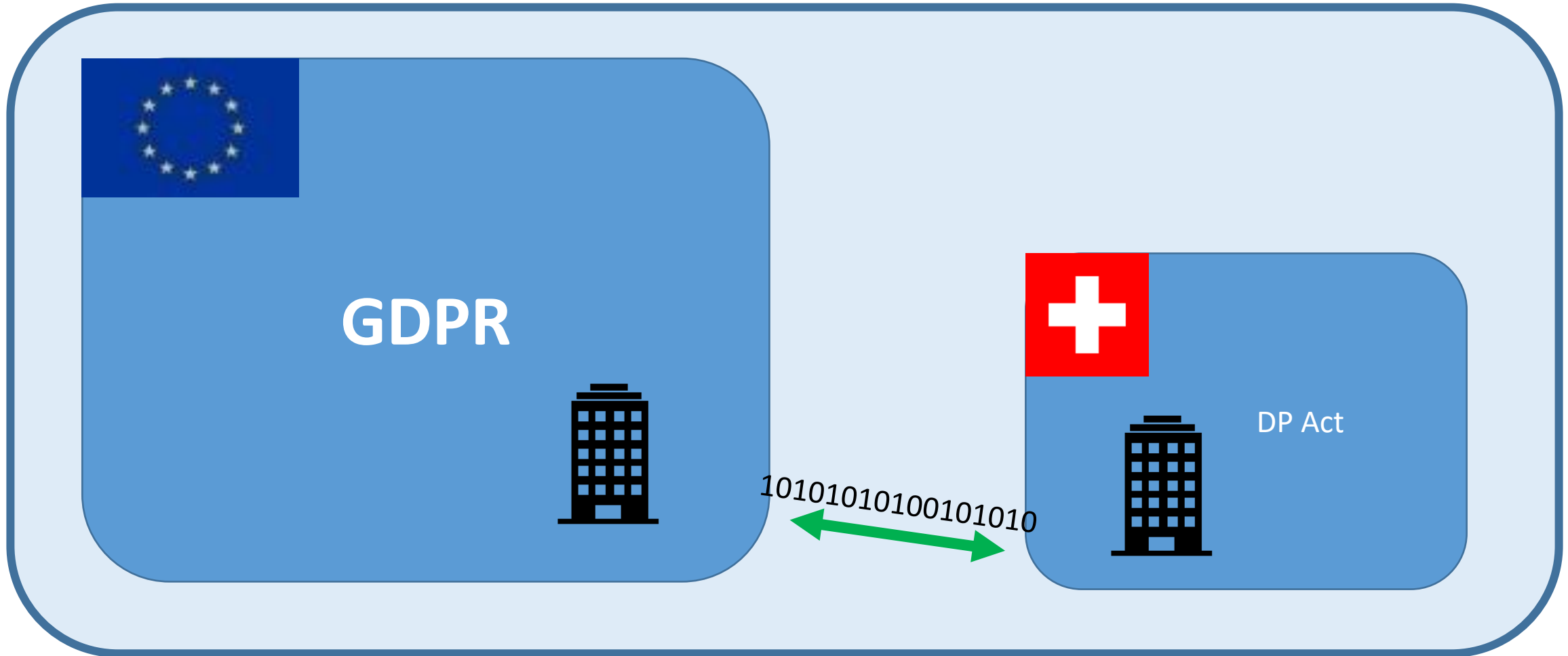


# **PRIVACY: EU SIDE OF THE STORY**

# DATA TRANSFERS

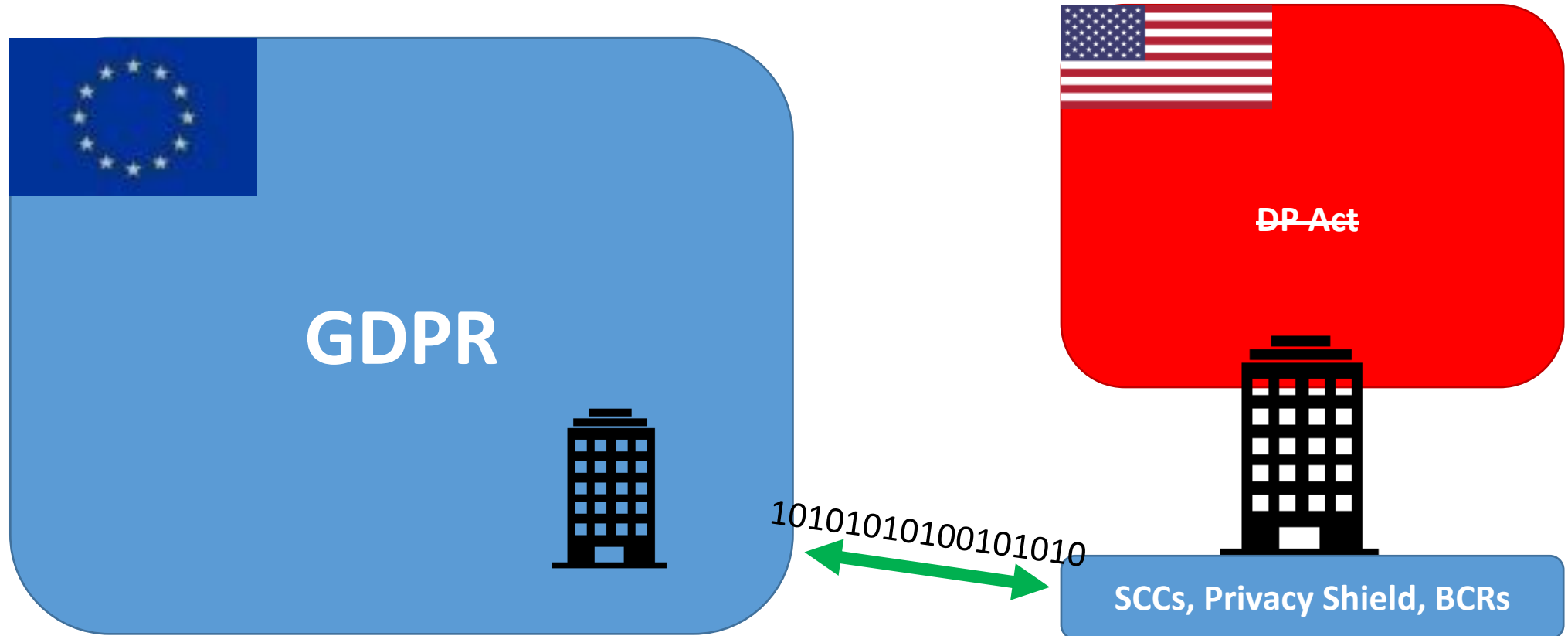
- **General Rule:** Export Prohibition on Personal Data
  - **Derogations:** “Necessary transfers”, non-structural (Art 49)
  - **Outsourcing:**
    - Adequacy (Art 45)
    - Standard Contractual Clause / Model Clauses (Art 46)
    - Binding Corporate Rules (Art 47)
- Expansion of GDPR rules in non-EU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

# PRIVACY “BUBBLE”: SWITZERLAND

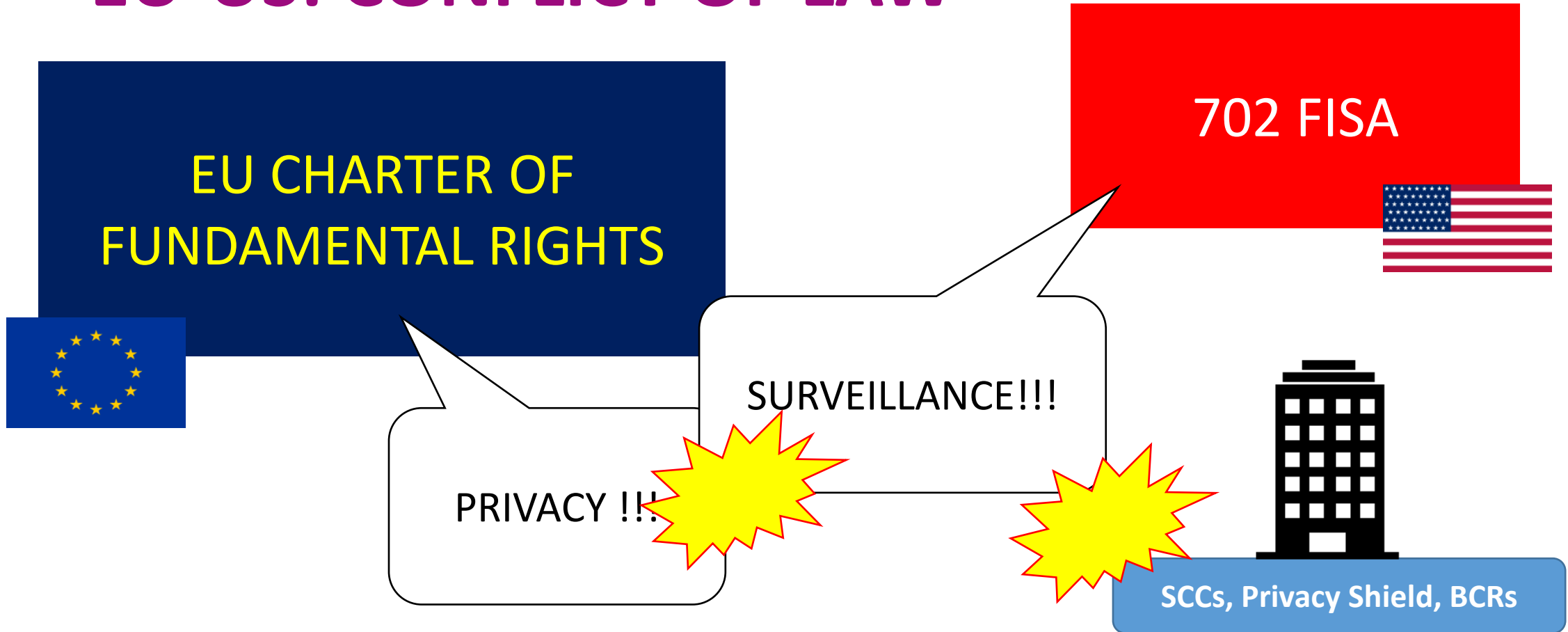




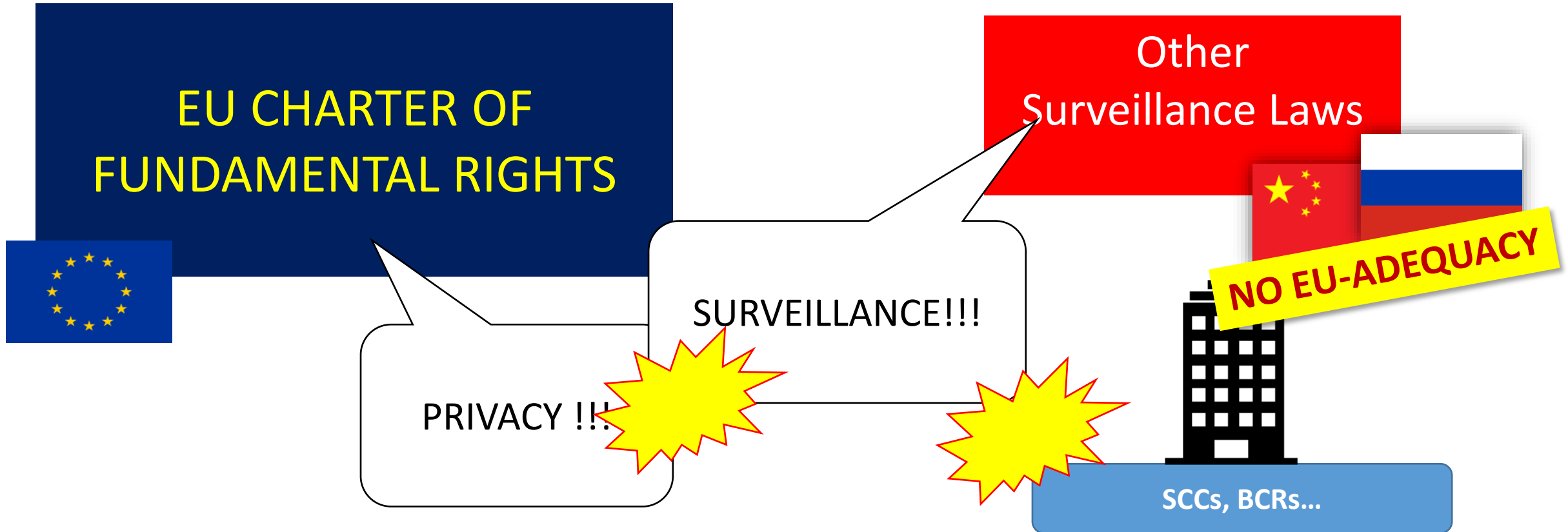
# PRIVACY “BUBBLE”: CONTRACTUAL



# EU-US: CONFLICT OF LAW



# EU-RUSSIA/CHINA: CONFLICT OF LAW?





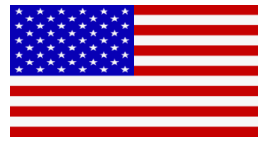
# PART 2: CJEU CASE LAW



# “ESSENCE”



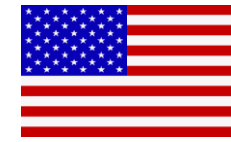
1. Legitimate aim for the measure
2. Measure suitable to achieve the aim
3. Measure must be necessary to achieve the aim (Less onerous way?)
4. Measure must be reasonable, considering the competing interests of different groups at hand



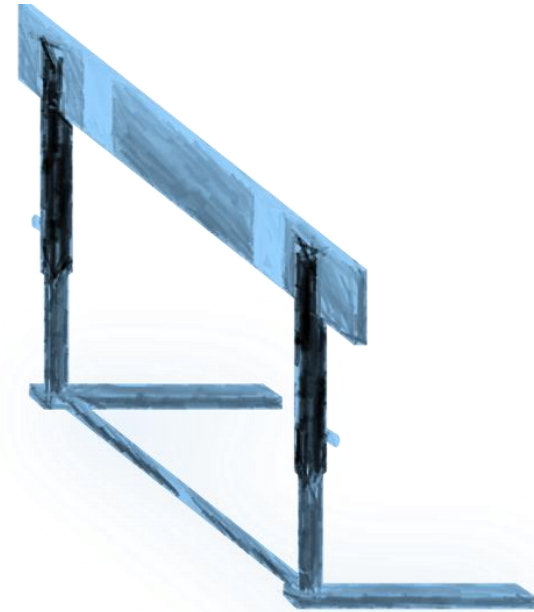
≈ **GDPR**



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



= **CFR**



CFR  
Art 7, 8 & 47



# **SAFE HARBOR & PRIVACY SHIELD: FOOL ME TWICE?**







***“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)*

# **OUTCOME: PRACTICAL CONSEQUENCES**

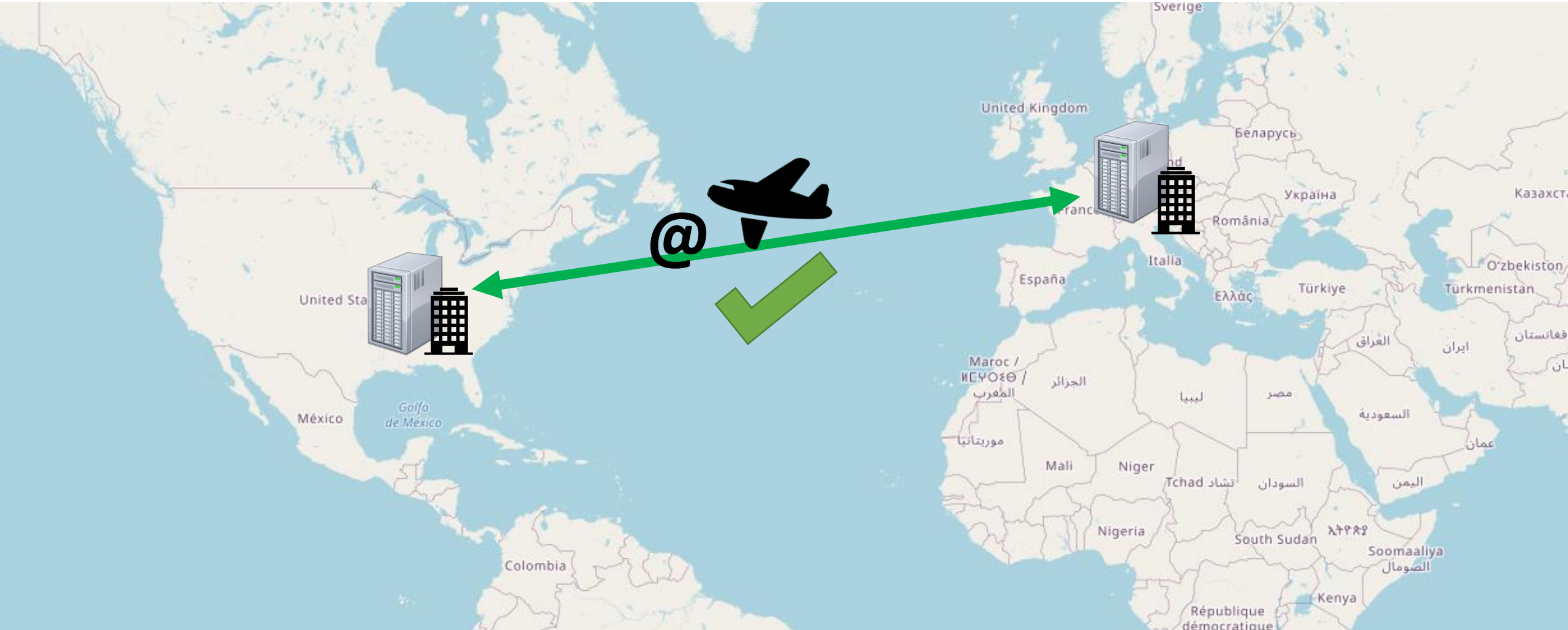
# DATA TRANSFERS

- **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

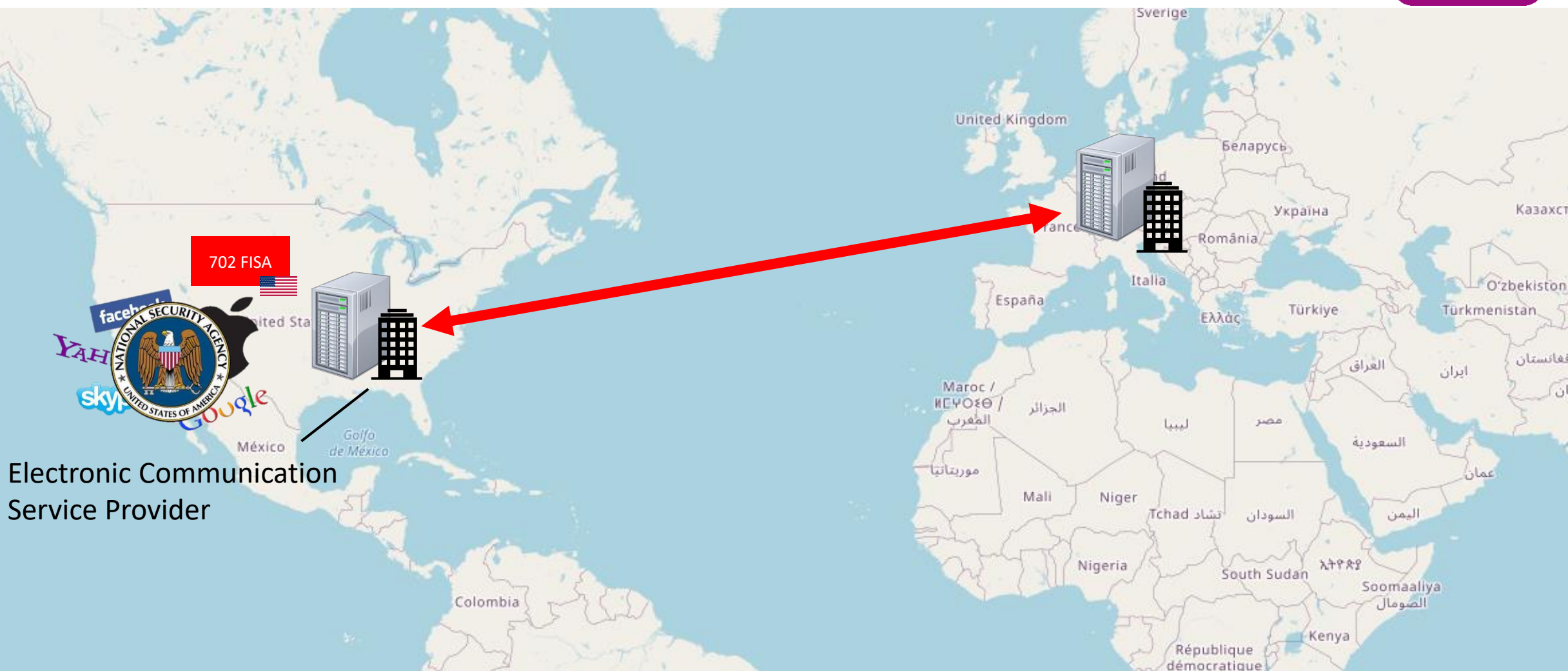


# TRANSFERS: NECESSARY TRANSFERS

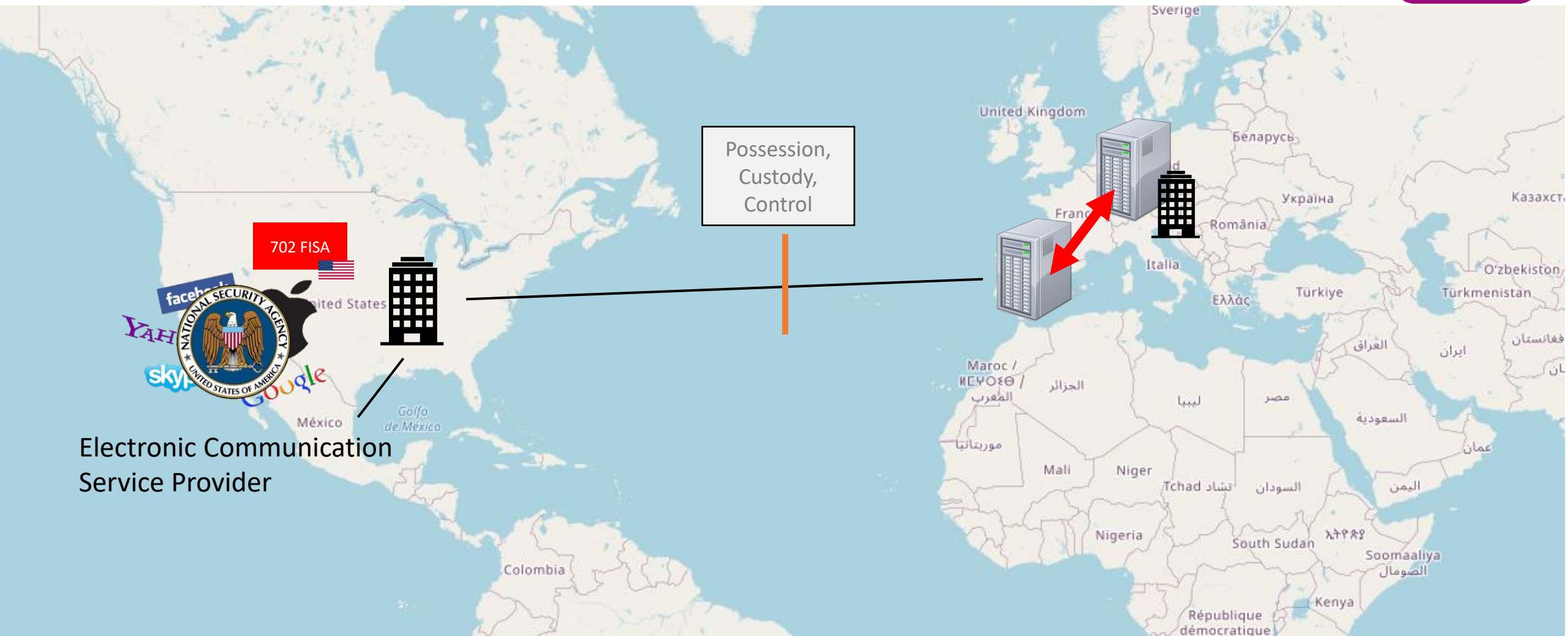


# TRANSFERS: “OUTSOURCING” (FISA) - USA

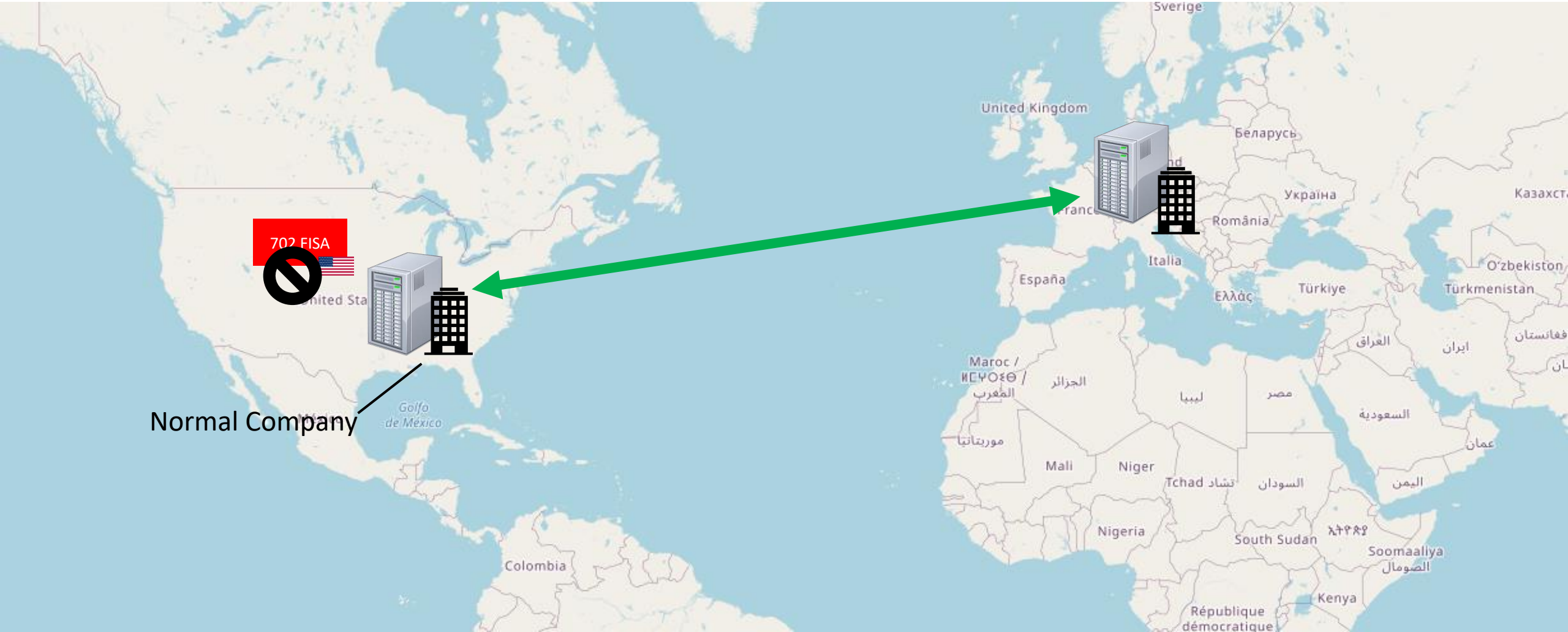
noyb



# TRANSFERS: “OUTSOURCING” (FISA) - EU



# TRANSFERS: NON-FISA





# ENFORCEMENT: 101 COMPLAINTS



Search

↓ Need more results? Try [internal pages search](#). [query syntax](#)

5230 web pages in 5.12 s.

URLs

CSV

CSV+snippets

Rank	Url	Snippets
2 465	<a href="http://www.panorama.com.al/">http://www.panorama.com.al/</a>	d = id; js.src = "//connect.facebook.com/en_US/sdk.js"; fjs.
2 710	<a href="https://www.inoreader.com/">https://www.inoreader.com/</a>	ocument,'script','//connect.facebook.com/en_US/fbevents.js')
8 195	<a href="https://www.jitunews.com/">https://www.jitunews.com/</a>	t,'script','https://connect.facebook.com/en_US/fbevents.js')
11 687	<a href="https://www.asb.co.nz/">https://www.asb.co.nz/</a>	s-prefetch" href="//connect.facebook.com/"> <link rel="dns-p
14 721	<a href="https://price.ua/ua">https://price.ua/ua</a>	ch" type="" href="//connect.facebook.com" /> <link rel="dns-
22 612	<a href="https://www.lovethispic.com/">https://www.lovethispic.com/</a>	= true; js.src = '//connect.facebook.com/en_US/sdk.js'; d.ge
23 604	<a href="https://www.bestprice.gr/">https://www.bestprice.gr/</a>	src 'unsafe-inline' connect.facebook.com www.google-analytic
31 409	<a href="https://www.mfat.govt.nz/">https://www.mfat.govt.nz/</a>	online.com https://connect.facebook.com; img-src 'self' *.t
33 125	<a href="https://www.southampton.ac.uk/">https://www.southampton.ac.uk/</a>	com use.typekit.net connect.facebook.com platform.twitter.co
34 166	<a href="https://sabaya.ae/">https://sabaya.ae/</a>	d = id; js.src = "//connect.facebook.com/en_US/sdk.js#xfbml=
44 125	<a href="https://1cak.com/">https://1cak.com/</a>	d = id; js.src = "//connect.facebook.com/en_US/sdk.js"; fjs.
45 866	<a href="https://alimero.ru/">https://alimero.ru/</a>	tch"> <link href="//connect.facebook.com" rel="dns-prefetch
47 153	<a href="https://www.cartabcc.it/Pagine/default.aspx">https://www.cartabcc.it/Pagine/default.aspx</a>	ript" src="https://connect.facebook.com/it_IT/all.js"></scr
52 870	<a href="https://sravni.ua/ua">https://sravni.ua/ua</a>	ch" type="" href="//connect.facebook.com" /> <link rel="dns-
56 091	<a href="https://ppm.powerplaymanager.com/en/">https://ppm.powerplaymanager.com/en/</a>	script src="https://connect.facebook.com/en_US/all.js"></scr
58 016	<a href="https://s1.biathlonmania.com/?lang=">https://s1.biathlonmania.com/?lang=</a>	script src="https://connect.facebook.com/en_US/all.js" defer
59 840	<a href="https://www.e-gulfbank.com/en/personal">https://www.e-gulfbank.com/en/personal</a>	script src="https://connect.facebook.com/en_US/sdk.js"></scr
61 701	<a href="https://www.wideopenpets.com/">https://www.wideopenpets.com/</a>	nect" href="https://connect.facebook.com" crossorigin><link

noyb's

# 101

US TRANSFER  
COMPLAINTS





# MAIN ARGUMENTS IN 101 CASES

1. Sorry, we removed it!
2. Supplementary Measures
3. „Risk Based Approach“

**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.

**facebook**®



CNIL.

COMMISSION NATIONALE  
INFORMATIQUE & LIBERTÉ



dsb

Republik Österreich

Datenschutz  
behörde



AUTORITEIT  
PERSOONSGEGEVENS



EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

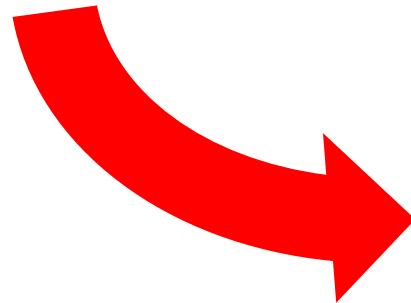




**SOLUTION: „RISK BASED APPROACH“**

# ACTUAL „RISK“ ELEMENTS IN THE GDPR

- Record of Processing (Article 30)
- Security (Article 32)
- Data Breaches (Article 33, 34)
- ...



*General Principle  
of the GDPR!*

**dsb**

Republik Österreich

Datenschutz  
behörde



# MAIN ARGUMENTS IN 101 CASES

noyb

1. Sorry, we removed it!
- ~~2. Supplementary Measures~~
- ~~3. „Risk Based Approach“~~





# **ENFORCEMENT: NEW CJEU CASE LAW**

# ENFORCEMENT

- **DPA: 101 Complaints**

- Slow procedures
- Mostly closed because of compliance
- **Fine on Meta: € 1.2 billion**

- **Tender / Requirments**

- **Case Law in Germany and France**

- **Non-Material Damages (C-300/21) + Collective Redress Directive**

- Example 1 Mio Data Subjects
- € 100 each
- **€ 100 Mio (+ legal costs)**

# **PART 3: TRANS-ATLANTIC DATA PRIVACY FRAMEWORK**



## PART 3: “TADPF”









# COMMERCIAL: “TADPF” PRINCIPLES

## II. PRINCIPLES

### 1. NOTICE

- a. An organization must inform individuals about:
  - i. its participation in the EU-U.S. DPF and provide a link to, or the web address for, the Data Privacy Framework List,
  - ii. the types of personal data collected and, where applicable, the U.S. entities or U.S. subsidiaries of the organization – also adhering to the Principles,
  - iii. its commitment to subject to the Principles all personal data received from the EU in reliance on the EU-U.S. DPF,
  - iv. the purposes for which it collects and uses personal information about them,
  - v. how to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints,
  - vi. the type or identity of third parties to which it discloses personal information, and the purposes for which it does so,
  - vii. the right of individuals to access their personal data,
  - viii. the choices and means the organization offers individuals for limiting the use and disclosure of their personal data,
  - ix. the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is: (1) the panel established by DPAs, (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States,
  - x. being subject to the investigatory and enforcement powers of the FTC, the DOT or any other U.S. authorized statutory body,
  - xi. the possibility, under certain conditions, for the individual to invoke binding arbitration,<sup>5</sup>
  - xii. the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and
  - xiii. its liability in cases of onward transfers to third parties.

<sup>5</sup> See, e.g., section (c) of the Recourse, Enforcement and Liability Principle

- b. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

### 2. CHOICE

- a. An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.
- b. By derogation to the previous paragraph, it is not necessary to provide choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. However, an organization shall always enter into a contract with the agent.
- c. For sensitive information (*i.e.*, personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), organizations must obtain affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice. In addition, an organization should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

### 3. ACCOUNTABILITY FOR ONWARD TRANSFER

- a. To transfer personal information to a third party acting as a controller, organizations must comply with the Notice and Choice Principles. Organizations must also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation. The contract shall provide that when such a determination is made the third party controller ceases processing or takes other reasonable and appropriate steps to remediate.
- b. To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii)

ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

#### 4. SECURITY

- a. Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

#### 5. DATA INTEGRITY AND PURPOSE LIMITATION

- a. Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing.<sup>6</sup> An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. An organization must adhere to the Principles for as long as it retains such information.
- b. Information may be retained in a form identifying or making identifiable<sup>7</sup> the individual only for as long as it serves a purpose of processing within the meaning of 5a. This obligation does not prevent organizations from processing personal information for longer periods for the time and to the

<sup>6</sup> Depending on the circumstances, examples of compatible processing purposes may include those that reasonably serve customer relations, compliance and legal considerations, auditing, security and fraud prevention, preserving or defending the organization's legal rights, or other purposes consistent with the expectations of a reasonable person given the context of the collection.

<sup>7</sup> In this context, if, given the means of identification reasonably likely to be used (considering, among other things, the costs of and the amount of time required for identification and the available technology at the time of the processing) and the form in which the data is retained, an individual could reasonably be identified by the organization, or a third party if it would have access to the data, then the individual is "identifiable."

extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis. In these cases, such processing shall be subject to the other Principles and provisions of the Framework. Organizations should take reasonable and appropriate measures in complying with this provision.

#### 6. ACCESS

- a. Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

#### 7. RECOURSE, ENFORCEMENT AND LIABILITY

- a. Effective privacy protection must include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum such mechanisms must include:
  - i. readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;
  - ii. follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of non-compliance; and
  - iii. obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.
- b. Organizations and their selected independent recourse mechanisms will respond promptly to inquiries and requests by the Department for information relating to the EU-U.S. DPF. All organizations must respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department. Organizations that have chosen to cooperate with DPAs, including organizations that process human resources data, must respond directly to



such authorities with regard to the investigation and resolution of complaints.

- c. Organizations are obligated to arbitrate claims and follow the terms as set forth in Annex I, provided that an individual has invoked binding arbitration by delivering notice to the organization at issue and following the procedures and subject to conditions set forth in Annex I.
- d. In the context of an onward transfer, a participating organization has responsibility for the processing of personal information it receives under the EU-U.S. DPF and subsequently transfers to a third party acting as an agent on its behalf. The participating organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.
- e. When an organization becomes subject to a FTC or court order based on non-compliance or an order from a U.S. statutory body (e.g., FTC or DOT) listed in the Principles or in a future annex to the Principles that is based on non-compliance, the organization shall make public any relevant EU-U.S. DPF-related sections of any compliance or assessment report submitted to the FTC court or U.S. statutory body, to the extent consistent with confidentiality requirements. The Department has established a dedicated point of contact for DPAs for any problems of compliance by participating organizations. The FTC and the DOT will give priority consideration to referrals of non-compliance with the Principles from the Department and EU Member State authorities, and will exchange information regarding referrals with the referring state authorities on a timely basis, subject to existing confidentiality restrictions.

# COMMERCIAL DATA USAGE



Consent  
(or other legal basis)

Necessary

Full Access



Opt-Out  
(only sharing, change of purpose)

Relevant

Limited Access



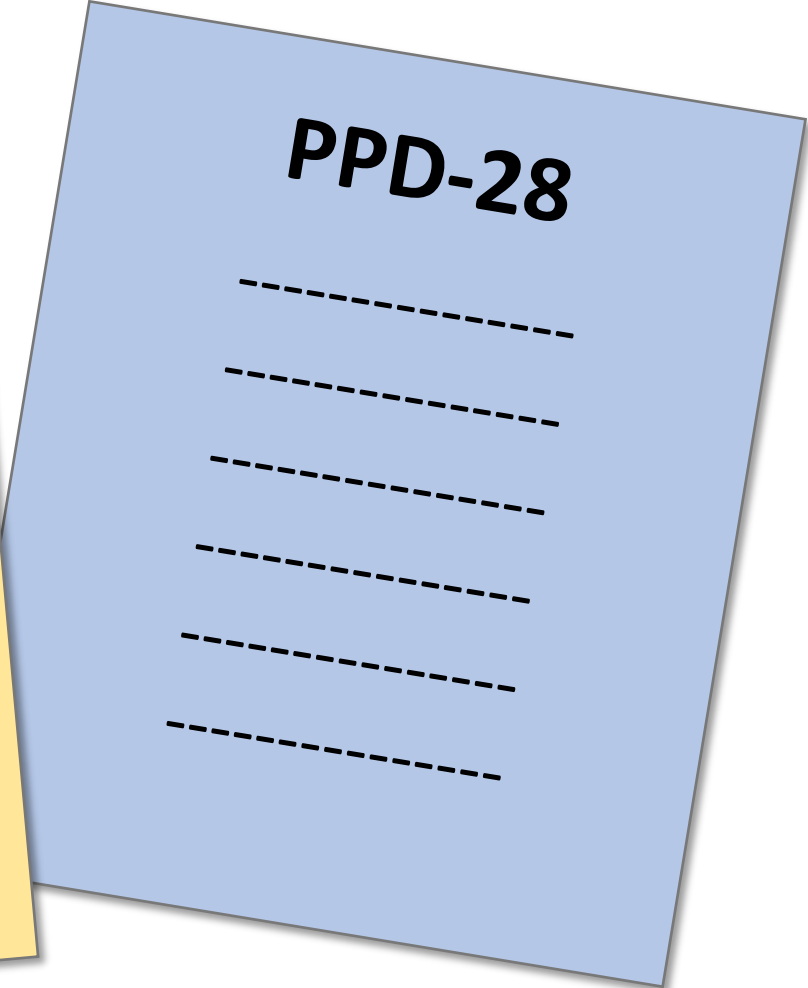
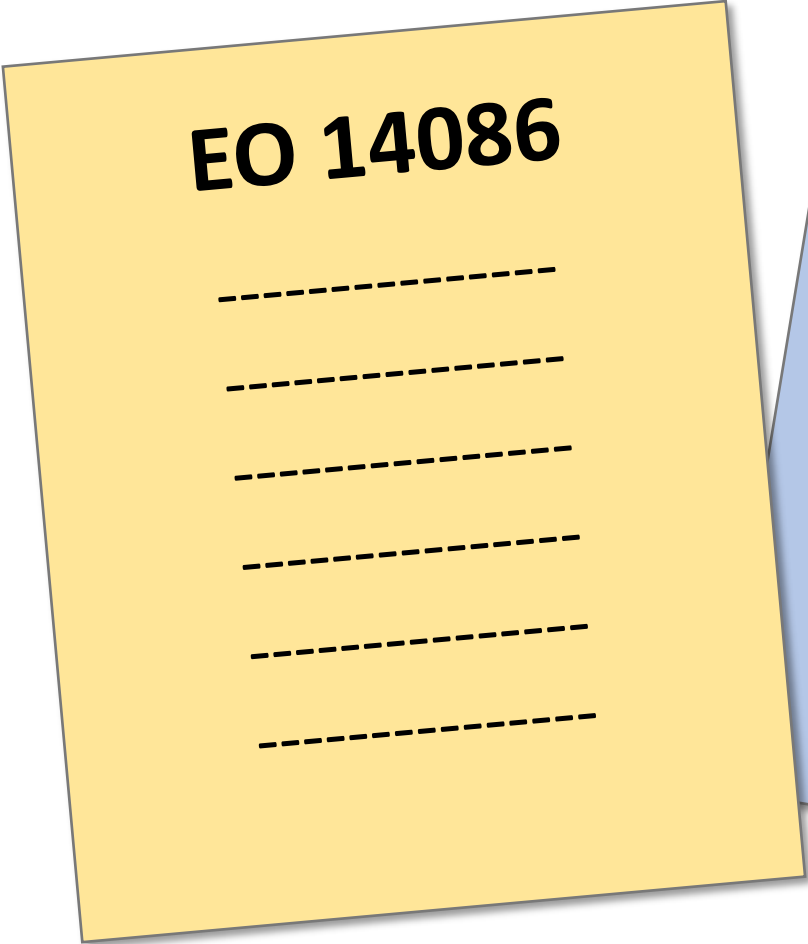


# **SURVEILLANCE: “NEW” EXECUTIVE ORDER**





# EO 14086 VS. PPD-28



# EO 14086 VS. PPD-28

- Biden EO 14086 has largely the same limitations as Obama PPD-28
- Slightly clearer language
- Some additional reasons for mass surveillance  
*(for example: health crisis and climate change)*
- „**Necessary**“ is now „**Necessary and Proportionate**“  
*(both were meant to comply with Articles 7, 8 and 52 CFR)*

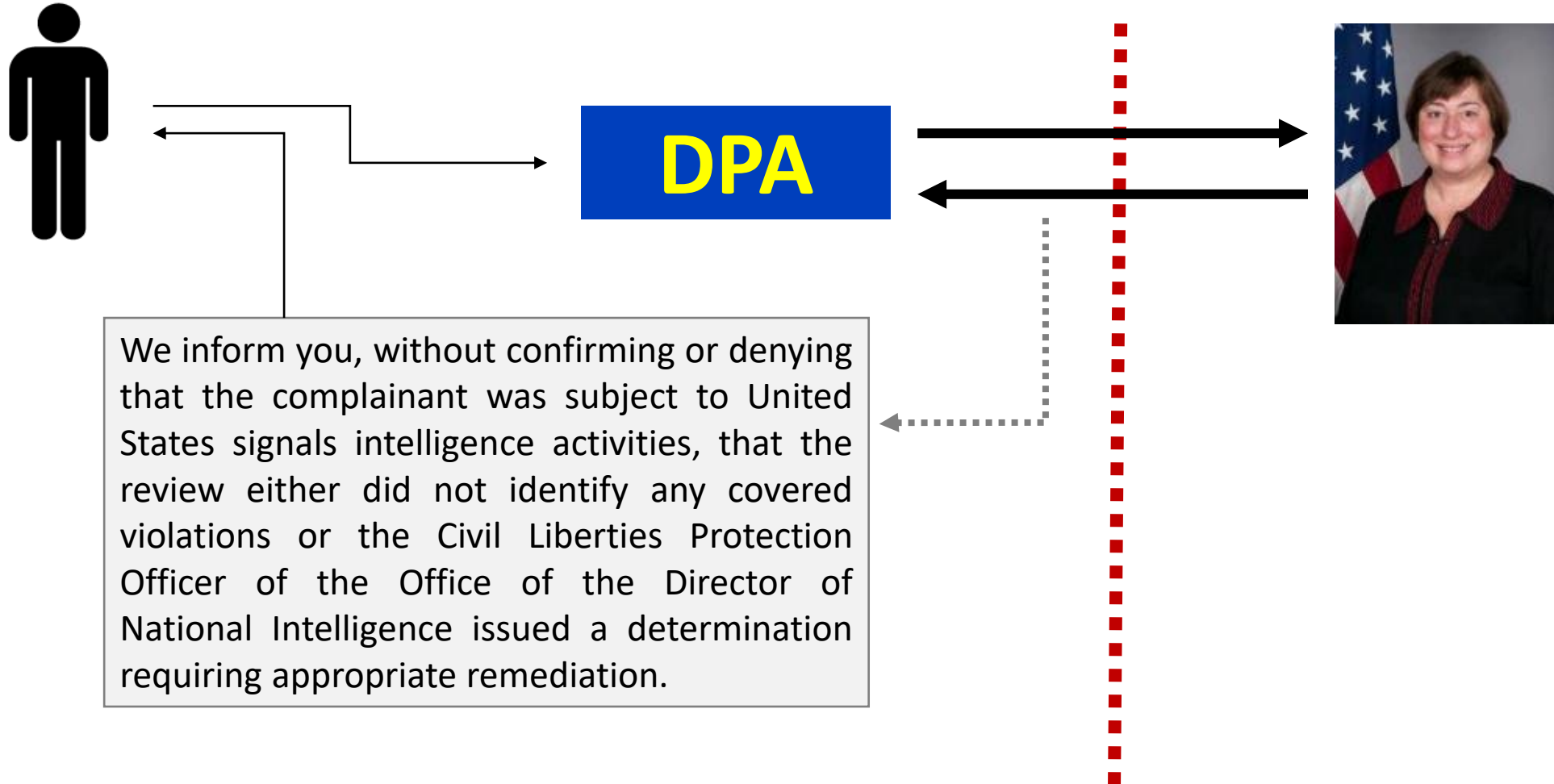
# PROPORTIONALITY IN EO?



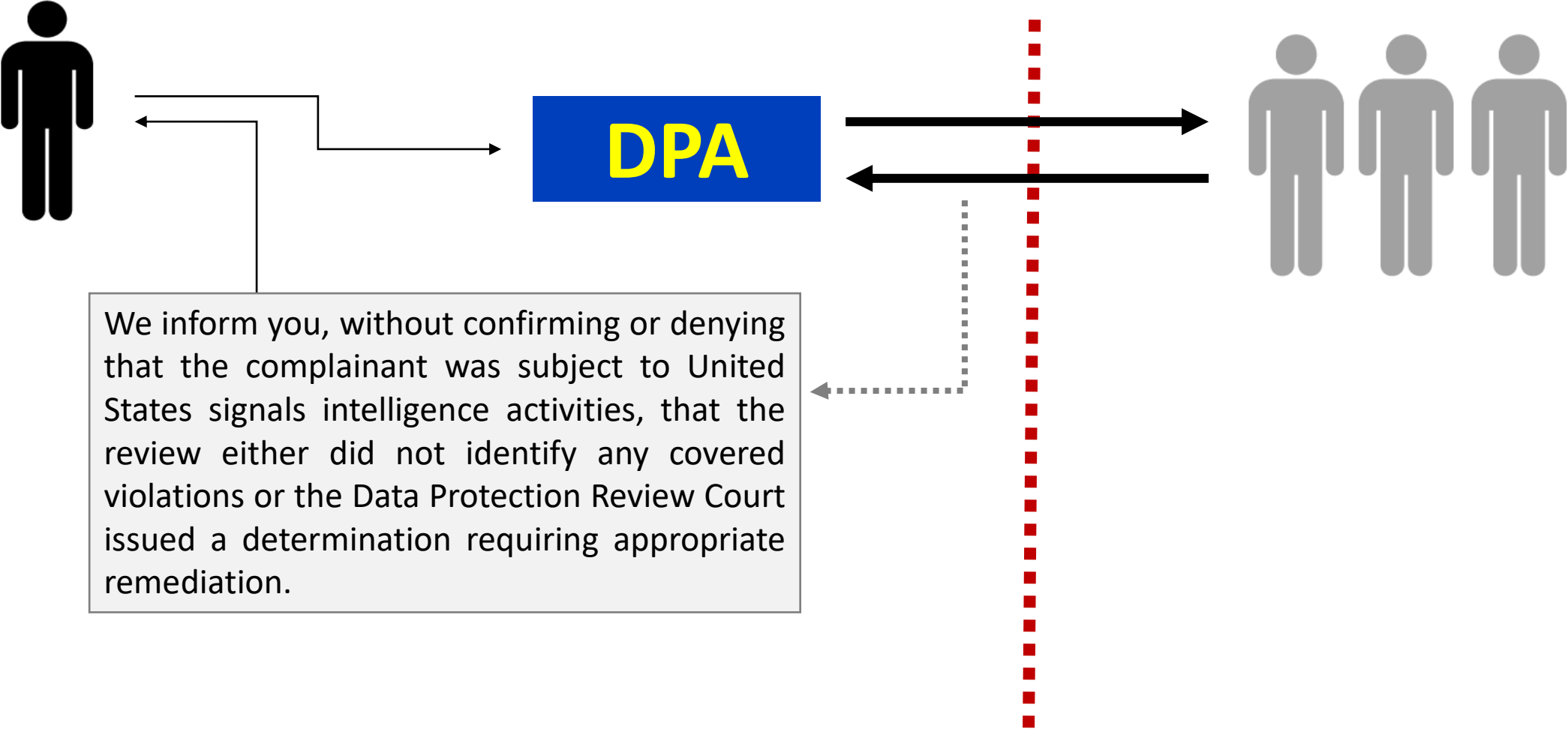
FISA



# OMBUDSPERSON BECOMES „CLPO“



# DATA PROTECTION „COURT“



We inform you, without confirming or denying that the complainant was subject to United States signals intelligence activities, that the review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation.

We inform you, without confirming or denying that you were subject to United States signals intelligence activities, that the review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation.



# DATA FROM 1995 TO 2023?

- EO only applies to data transferred from the EU to the US after July 2023
- Under the EO, EU companies would have to „retransfer“ all personal data to the US to get covered





# SHORT TERM: EU-US „SOLUTION“





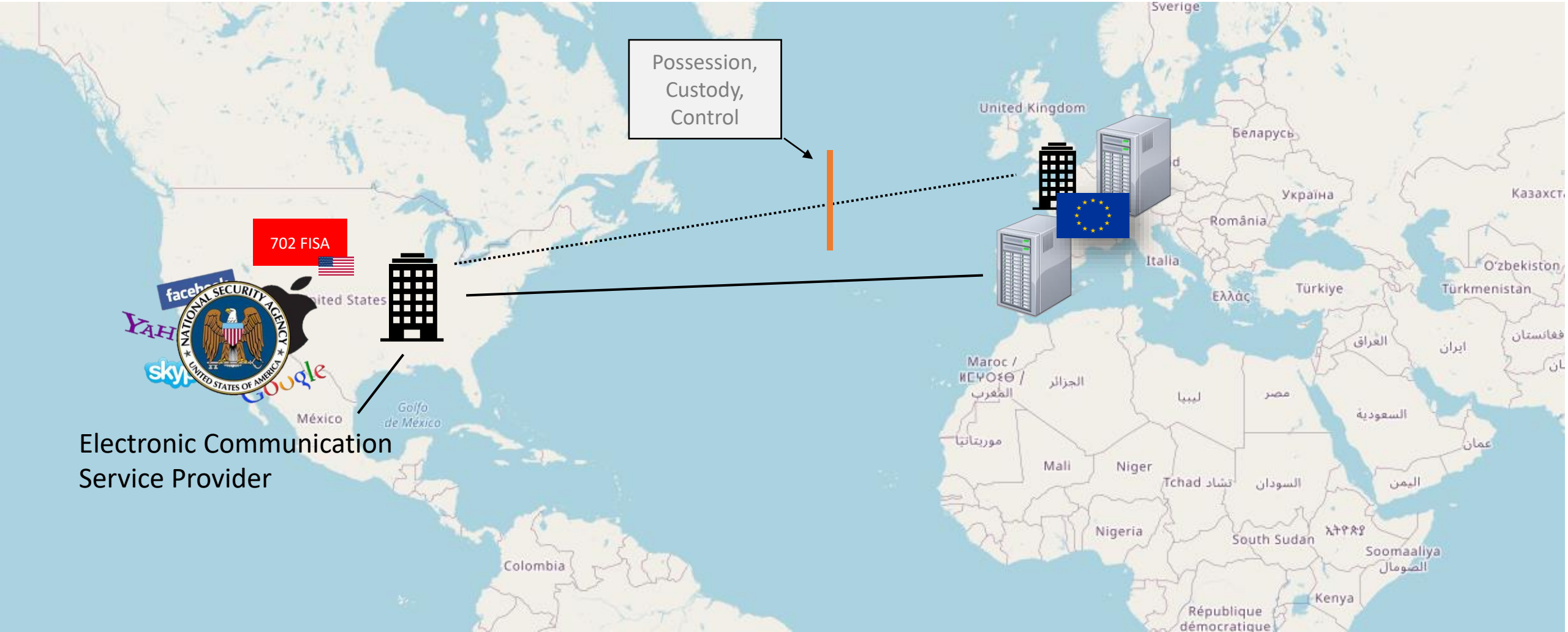


# LONG-TERM: OTHER SOLUTIONS





# SEGREGATION: EU ENTITY



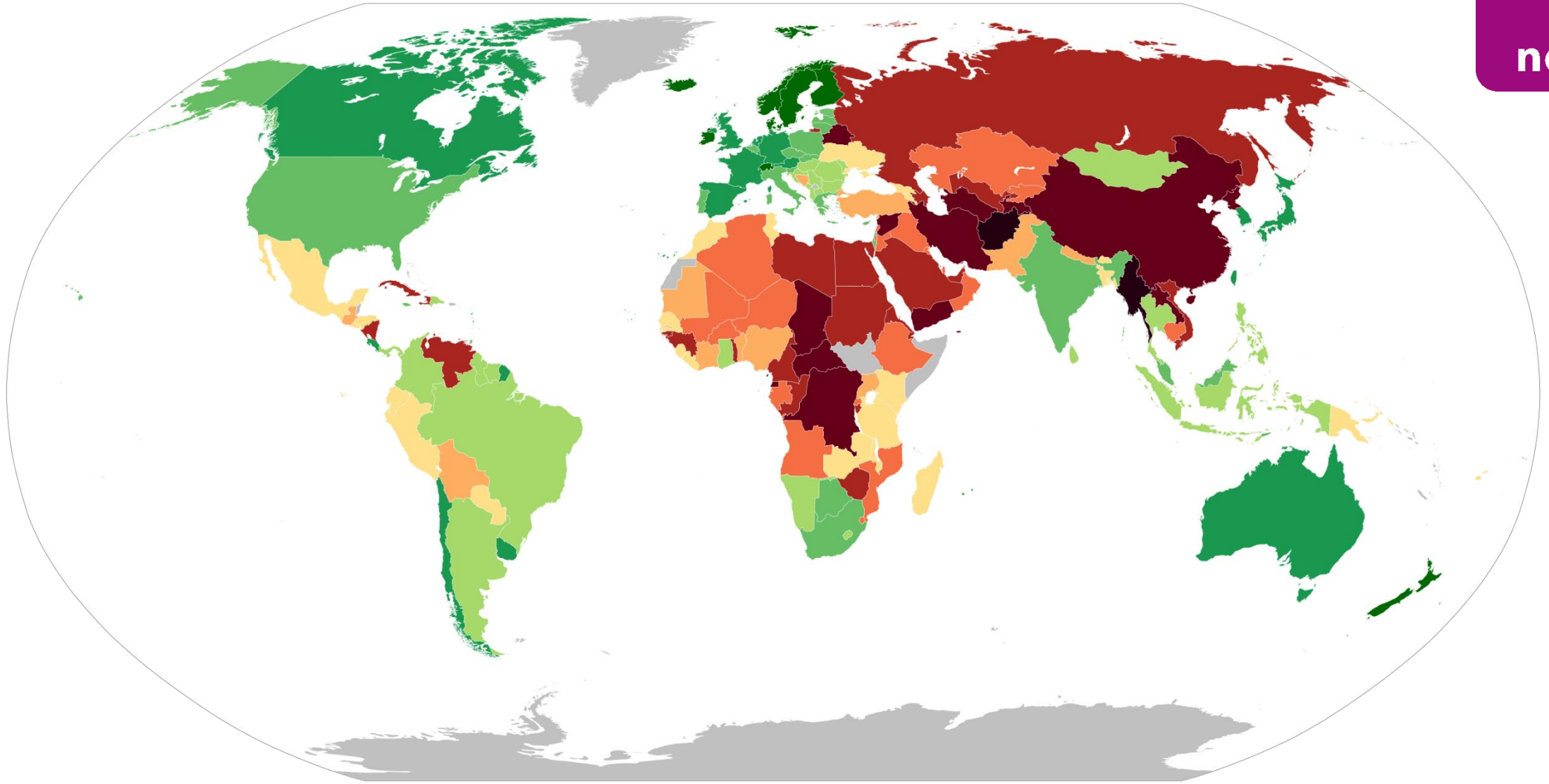
Electronic Communication Service Provider

Possession, Custody, Control



# **LONG-TERM: NON-DEMOCRATIC COUNTRIES**







**THANKS!**

