VISCHER

**FREQUENTLY ASKED QUESTIONS (FAQ)**

# ON THE RISK OF FOREIGN LAWFUL ACCESS AND THE STATISTICAL "ROSENTHAL" METHOD FOR ASSESSING IT

*By David Rosenthal*[1]

My statistical method of assessing and documenting foreign lawful access risks has been published in August 2020, and since then, various updates and new releases have been published – including a transfer impact assessment form for complying with the requirements under the Standard Contractual Clauses of the European Commission (**EU SCC**) and the European Court of Justice's "Schrems II" decision in August 2021, which again has been overcome for the time being with the European Commission's, United Kingdom's and Switzerland's recognition of the adequacy of the "Data Privacy Framework" im combination with the US EO 14086. Meanwhile new question have arisen in view of the uncertainties caused by the changes in the US since 2025 under the Trump administration.

In view of the overwhelming positive feedback to my method in Switzerland and abroad, I have decided to create this FAQ to respond to many of the questions I have been receiving or misunderstandings that I have noticed.

This FAQ is for those who want to ● understand how lawful access works (in particular under US law) ● use my method to assess it, ● coach and help others in using it, ● scrutinize or criticize my method, ● improve and further develop it, or ● review and understand assessments done by others.

If you have further questions, please let me know. I will update this FAQ from time to time, and you may freely share the FAQ (preferably by sharing the URL, so people get the latest version[2]).

A substantial part of the FAQ is devoted to providing information (including official sources) on how to deal with Section 702 FISA and other US laws in connection with foreign lawful access risk assessments. It appears that many people are struggling with this task and have difficulties finding the necessary information. I hope this FAQ can contribute to solving this issue.

I cover both the EU General Data Protection Regulation (**GDPR**) as well as the current and revised Swiss Data Protection Act (**Swiss DPA**), which is comparable to the GDPR when it comes to international transfers of data.

Please note that this FAQ is no legal advice but only for informational purposes and provided "as is". Get your own legal advice when dealing with these issues. Also, I am not making any risk assessments or political statements here; I

---

1 I thank Robin Weissenrieder for his support on Section 702, Jonas Baeriswyl, David Vasella, Rie Aleksandra Walle and Benedikt Meier for their comments and all the others that inspired me for this FAQ.

2 Permalink: https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf or https://vischerlnk.com/flarafaq.

simply provide a tool to do and document them – a tool that is today widely used in practice by many data law professionals.

The method has been implemented in two Excel files with multiple worksheets, all of which are available here for free in English (and partly in German):

- https://www.rosenthal.ch/downloads/Rosenthal_EU-SCC-TIA.xlsx
- https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx (or short: https://vischerlnk.com/flara)

See also my similarly extensive FAQ on the EU SCC, which is available here, but has not been updated for some time.

| Version | Most important changes |
|---|---|
| August 1, 2022 | First draft for public comment |
| October 23, 2022 | Q37 with comments on the Foreign Sovereign Immunities Act as raised in a legal opinion; introduced Q24a to discuss the effect of a "gag order" and Q29a to discuss the new EO 14086 ("Privacy Shield 2.0"); I added a prominent new supporter of my method to Q38 (the Swiss Federal Chancellery), another critic to Q39 and some further thoughts on how the "Schrems II" problem will be solved or go aways in the next years (Q44); updated links and archived them permanently (perma.cc) |
| May 5, 2025 | Updated the FAQ for covering the "multi-scenario" version of my method, and tried to also follow-up on other developments that have occurred since the last update, resulting in updates throughout the text (but no fundamental rewrite of the 2022 text). |

Questions and feedback: david.rosenthal@vischer.com

## A. GENERAL

### 1. What is the purpose of your method?

It is a tool that allows you to estimate your confidence that no foreign lawful access will occur in your cloud project or other cases of cross-border transfers of personal data by:

- Providing a structured approach to more objectively assess whether data transfers will be subject to a prohibited foreign lawful access and how effective the "supplementary measures" undertaken to prevent such access will be; without it, you have to either rely on their "gut feeling" or oversimplify the assessment;

- Providing a format to you to document and communicate the findings more efficiently and clearly; if filled out correctly, the reader immediately sees how the user arrived at its conclusion;
- Permitting you to apply both a rights- and risk-based approach in assessing foreign lawful access risks.

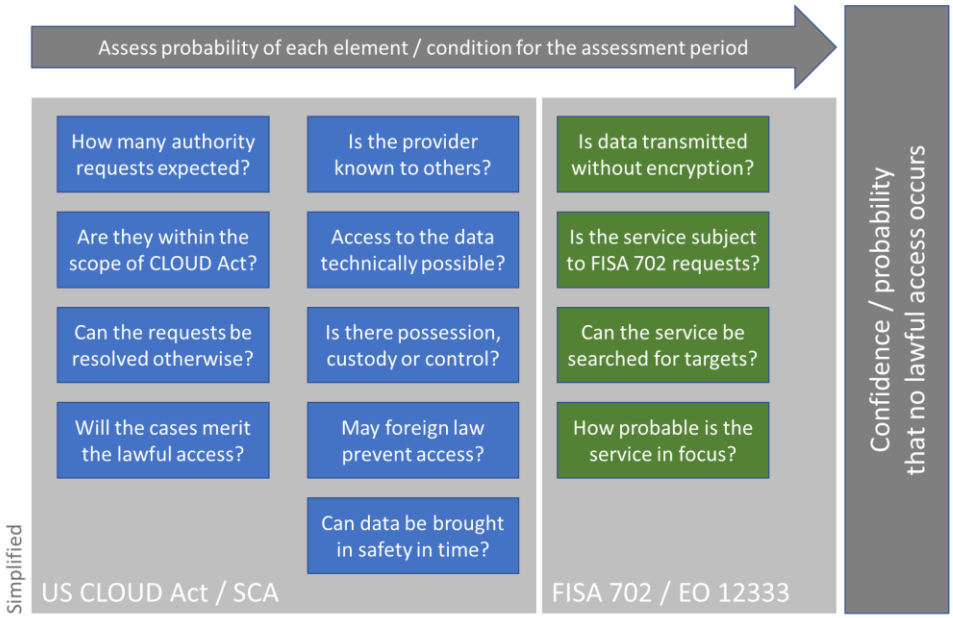
## 2. How does your assessment method work?

The method allows you to find out how well the protective measures you are taking will in your specific case prevent a prohibited foreign lawful access from happening and what the residual risk is given the circumstances (or, conversely, how confident you are that no lawful access will occur). It does so by splitting up a highly complex issue with many "variables" into smaller pieces that you will better understand and feel more comfortable and able to assess. Also, the method does not force you to be sure about your estimates; it can deal with different levels of confidence as to your assessments.

The method is built on the fact that in the US and every other country, local lawful access can only occur if certain legal, technical and practical conditions are fulfilled cumulatively. Once you understand them, you can find out whether they are fulfilled and what could be done to prevent them from being fulfilled.

When you do the assessment, each of these conditions is tested against the circumstances and how you plan to transfer and protect the data (see, for example, Q35). Your task is to estimate the chances with which each condition is fulfilled; based on this, an overall probability is calculated using commonly used statistical formulas (Q5).

This chart is a simplified overview of the process (for both transfer impact and professional and official secrecy assessments):



Some of these conditions are of legal nature and some are factual. Some require technical knowledge, some legal knowledge. This is why I recommend applying the method in a workshop with all stakeholders being present (e.g., IT, CISO, DPO, Legal, Compliance, Business, see also Q18 for group assessments). Professional guidance will help (in particular on more complicated issues such as foreign law).

This is not a huge exercise, but you should invest 2-3 hours for professional and official secrecy use cases and 1 hour for mere data protection cases. I and peers at other law firms have done many such workshops and the experience is always the same: After a workshop, stakeholders have a much better understanding of the risk. Understanding a risk is key to dealing with it appropriately.

In May 2025, the method has been expanded by a "multi-scenario" version to cover cases where the legal situation in the target country is very unstable. You can define four different scenarios on how the situation will develop during the covered period, e.g., how the separation of power or rule of law could change over time, you can assign each scenario a probability and perform the assessment for each scenario. You will get weighted average probability of a foreign lawful access to occur. Further, this multi-scenario-version also covers business continuity risks due to political uncertainties and other "outside" factors, i.e. circumstances that you have not already taken into account in your traditional business continuity risk assessments. The multi-scenario version was developed following requests on how to deal with the situation caused by the Trump administration in the US since 2025.

### 3. Is your method compatible with the requirements of EEA data protection authorities for transfers to third countries?

Yes, it is compatible.

It implements and permits you to implement the recommendations of the European Data Protection Board (**EDPB**) of June 18, 2021 on "supplementary measures"[3] and – contrary to what many believe – it can even be used for the "rights-based" approach promoted by some EU data protection authorities. It is also compatible with the approach proposed by the Swiss data protection authority,[4] which more or less reflects the EDPB recommendations (see also Q41).

---

[3] European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0 adopted on June 18, 2021 (https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en, archived at https://perma.cc/BCW5-MJ4B).

[4] See the "Guide to checking the admissibility of data transfers with reference to foreign countries (Art. 6 para. 2 letter a FADP)" of June 18, 2021, available in English at https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows.html (archived at https://perma.cc/RDM3-692Z)

The EDPB in essence recommends a six-step approach, which consists of (1) understanding the facts of the transfer, (2) verifying the transfer tool relied upon (e.g., the EU SCC), (3) assessing whether the law or practices in the country of the importer could subject the importer to problematic forms of foreign lawful access, (4) depending on the assessment, identify additional measures to prevent such foreign lawful access, (5) adopt such "supplementary measures", and (6) re-evaluate the situation in appropriate intervals.

My method covers the steps (3) and (4), and it allows the exporter (and importer) to properly document their assessment in line with the principle of accountability (Art. 5(2) GDPR). In addition, findings obtained through application of the method might also be useful in performing steps (5) and (6).

It addresses in particular the question whether public authorities of the country of the importer may seek access to the transferred data in a problematic manner (i.e. not compatible with EU requirements).

In the case of transfers to the US, the European Court of Justice (**CJEU**) in the "Schrems II" decision in July 2020 had found the two relevant problematic US laws to be Section 702 of the Foreign Intelligence Surveillance Act (**FISA**) and Executive Order (**EO**) 12333. My forms also provide instructions and information about public sources concerning the relevant laws and practices in the country at issue (in Q29 of this FAQ, I also provide detailed information about Section 702 FISA and EO 12333).

Meanwhile, the situation around transfers to the US has relaxed in view of the Executive Order 14086 of October 7, 2022, which ultimately, together with the "Data Privacy Framework", led to an adequacy decision by the European Commission in summer 2023 and thereafter also by the United Kingdom and Switzerland.[5] Hence, for transfers of personal data to the US the situation has relaxed since then, with a "pro-forma" transfer impact assessment (**TIA**) being sufficient even where transfers do to occur under the Data Privacy Framework (a sample is here). For other countries without an adequacy decision, the need for a TIA remains, even if in practice many exporters of personal data do not care in our experience (also, many European supervisory authorities de facto only cared and care about transfers to the US).

Of course, it remains the responsibility of the user to properly understand and assess the specific transfer at issue, but the method provides the necessary platform to do so.

According to the EDPB and the Standard Contractual Clauses of the European Commission (**EU SCC**), the key question that needs to be answered is whether the exporter and the importer have "no reason to

---

[5] See, e.g., https://www.vischer.com/en/knowledge/blog/swiss-us-dpf-how-to-transfer-data-to-the-us-with-and-without-it/.

believe that relevant and problematic legislation will be applied in practice" with regard to the transfer and importer at issue.[6] If they have no such reason to believe, they can proceed with the transfer. My method will provide the numbers that will help them to answer this question.

When assessing the transfer at issue in view of the applicable laws and practices in the country of the importer, my method (using the form "EU SCC Transfer Impact Assessment (TIA)") will provide you with two outputs:

- **Rights-based (or "zero-risk") approach:** The form will allow you to estimate the probability that the importer under the specific circumstances of the case could be required to produce transferred personal data to the government under the foreign access laws identified to be problematic. This is a purely legal analysis based on the country's laws and practices.

  The number reflects how confident the user is that the importer has legal arguments to successfully reject a problematic lawful access request (e.g., a request under Section 702 FISA in the case of transfers to the US[7]).

  The number will normally not be zero; no lawyer can be 100 percent sure that it will win a court case and no legal opinion will provide 100 percent certainty. This is not different here. This is no contradiction to the "rights-based" approach: It is based on the idea that Art. 46 GDPR only permits transfers if the importer is *not* subject to problematic lawful access law with regard to the data in question, regardless of whether the authorities have an actual interest in the data or not. The "rights-based" approach does not require that the exporter is and can be 100 percent sure that each and any judge would follow its legal analysis; as long as the exporter's particular case has not been tried in court, this is also not possible. The same is true in the EU or Switzerland, where there is no certainty how national security laws will be applied in each case (and whether they are always complied with). This is why referring to the "rights-based" approach as a "zero-risk" approach is also not entirely correct (see Q43).

  The "rights-based" approach also does not require that the non-applicability of the problematic law is the result of only one legal argument (e.g., the importer not being an Electronic Communication Service Provider [**ECSP**] in the US). It is fine if the non-applicability is the result of a combination of arguments, which it often is.

  Note that this number may not be available for countries with poor legal protections (e.g., China, Russia).

---

6 EDPB (footnote 3), para. 43.3, third bullet; Clause 14 EU SCC.

7 EO 12333 is usually not relevant because data in-transit is encrypted (Q29 at the end).

- **Risk-based approach:** For those who – like me – are convinced that Art. 46 GDPR provides for a "risk-based" approach (Q42), you can use the other numbers that my method produces. The overall probability also takes into account other factors that are relevant for determining whether a problematic foreign lawful access will occur during the assessment period. These other factors are expressly referred to in the recommendations of the EDPB, such as the documented practical experience of the importer with relevant prior instances of requests[8] (even if not based on law) and practices taking into account, for instances the purposes of the transfer, the type of entities involved or the sector in which the transfer occurs.[9] Therefore, and based on common-sense and a reasonable interpretation of the GDPR (and the Swiss DPA), relying on them is valid in my opinion.

  Some EU data protection authorities believe that, with regard to Section 702 FISA, it is not permitted to consider whether the exporter could be a target of the US intelligence authorities. This is wrong because it builds on a misunderstanding of how Section 702 works. If one takes a closer look at Section 702, it becomes clear that the question of whether the exporter could be a "target" is highly relevant under US law (Q29).

  In my view, there is no *numerus clausus* with regard to the aspects that can be taken into account in the assessment – all relevant circumstances may be considered in my view.

The *sequence* of the steps (3) and (4) in the EDPB recommendation is academic. In practice, these two steps go hand-in-hand or even have to be inversed. The reason is that most of the supplementary measures proposed by the EDPB cannot be implemented in practice with reasonable efforts or without defeating the purpose of the transfer. For instance, it is always easy and popular to propose the use of "encryption" to protect data following its transfer, but those who are familiar with such techniques know that there are hardly any solutions that provide full *technical* protection. If you encrypt everything and keep the key, most use cases in the cloud do not work anymore. I am sure that new technical developments and product offerings will change this over time, but currently most of the effective "supplementary measures" proposed by the EPDB do not work. And most of the "supplementary measures" actually implemented by cloud providers are ineffective – and the data protection authorities do not buy them (see, e.g., my comments on the first Google Analytics case in Austria).

What I usually recommend is to rely on technical and organizational measures that are designed to make it easier for the importer (or pro-

8 EDPB (footnote 3), para. 47.

9 EDPB (footnote 3), para. 33.

viders involved) to reject foreign lawful access requests on legal grounds. One such example are measures that allow the importer to argue that it has no "possession, custody or control" over the personal data at issue, for example by limiting day-to-day access to such data (Q35).

Unfortunately, only a few US-based providers (including Microsoft, Google and AWS) have started to offer such measures. In my experience, many of them have not yet realized the advantage and effectiveness of offering these kind of measures (for example, H., a popular US-based CRM SaaS provider, offers customers to limit day-to-day access by support staff, but not by other staff in the US and refuses to improve the protection of the data of its European customers).

In any event, my method permits the exporter (and importer) to assess and document the effect of such measures on the overall risk assessment. Hence, users will often first have to think of such measures and only then undertake an assessment of the combined transfer case.

4. **Why do many Swiss authorities refer to the US CLOUD Act as the main "issue" when moving to the cloud and not the laws that were relevant in the "Schrems II" decision and subsequent adequacy decision?**

Some consider the US CLOUD Act being more problematic and others do not know the difference or confuse them.

This table shows the key differences and scope of the provisions that are at issue:

| | Stored Communications Act & US CLOUD Act (re territoriality) | Section 702 FISA (inside US) EO 12333 (outside US) |
|---|---|---|
| Purpose | Investigating "serious crimes" | Protecting national security, investigating crimes (FBI) |
| Type of lawful access | One-time targeted access to specific customer data held by a US provider | Continuous search of a US provider for communications of targets |
| Affected by lawful access | Suspect of a crime, individuals involved in such crime | Targets of US intelligence community (approx. 200k) + people communicating with them |
| Compatibility with European law | ✓ Art. 18(1) Cybercrime Convention | ✗ ECJ 16.7.2020 C-311/18 "Schrems II" ✓ With EO 14086 implemented |
| Comparable provisions under Swiss law | Art. 265 Swiss Criminal Procedure Law (territoriality: e.g., DFC 143 IV 270) | Art. 39 et seqq. Swiss Intelligence Service Act ("signals intelligence") |
| To be assessed for transfers of personal data (Art. 16 Swiss DPA) | No | Yes (only pro-forma, for EU SCC transfers) No (for transfers under the EU-US/CH-US DPF) |
| To be assessed for transfers under professional or official secrecy | Yes | Yes |
| Which assessment form to use (if pro-forma is not sufficient)? | "Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities" | "EU SCC Transfer Impact Assessment (TIA)" (included also in the left form) |

The US CLOUD Act (and the Stored Communications Act, to which it relates) is a provision for US law enforcement authorities to investigate serious crimes. It is comparable to provisions in Swiss and many other

European laws that allows law enforcement to investigate serious crimes, and it is considered acceptable under the GDPR and the Swiss DPA (see Q31 for more details). Under the GDPR and Swiss DPA, the risk of the US CLOUD Act being applied does normally not have to be assessed. It is considered compatible with the GDPR and Swiss DPA, which has also been confirmed in the adequacy decisions under the GDPR and Swiss DPA in 2023 and 2024 for the US.[10]

Instead, it has to be assessed whether the data transferred could become subject to the US law provisions known as Section 702 FISA and EO 12333 (see Q3), which allow US intelligence authorities to conduct mass surveillance (see Q29 for more details). With the adequacy decisions concerning US law in 2023 and 2024, this is no longer an issue; transfers of personal data to the US are currently no particular issue from a data protection point of view.

The US CLOUD Act *is* relevant, though, for those who are subject to *professional or official secrecy* (e.g., data of banks, hospitals, medical doctors, law firms, the government). They have to assess the risk of *any* foreign lawful access, irrespective of whether it is compatible with the GDPR.

My method supports the assessment of both risks, depending on the type of the project (see Q12 on which one to use).

### 5. How is the probability of a foreign lawful access calculated?

The number is the result of a (rather simple) statistical calculation. It is based on the understanding that a prohibited lawful access can only happen if a number of conditions are fulfilled *cumulatively*.

This requires you (or your advisor) to understand how the local (foreign) law works. If you know that for a lawful access to happen in a particular country, say, *four* conditions must be fulfilled cumulatively, you have to test which of these four conditions are or could be fulfilled in your case. If you come to the conclusion that in view of your measures and the circumstances each of the conditions has only a 50:50 chance to be fulfilled, then the overall probability of a lawful access is 6.25 percent (0.5 x 0.5 x 0.5 x 0.5).[11]

I know that most lawyers (and data protection professionals) are not used to think this way (I did not either before I created the method), but this is simple statistics, a broadly accepted approach and was not

---

[10] See https://www.vischer.com/en/knowledge/blog/swiss-us-dpf-how-to-transfer-data-to-the-us-with-and-without-it/.

[11] Note that in the case of targeted lawful access types (e.g., US CLOUD Act), due to the nature of the lawful access, we also have to consider the expected number of cases in the assessment period.

invented by me. I only was the first to apply it to this particular problem (Q47).

Depending on the specific form you use, over a dozen factors are considered. This means that the "weight" of each individual factor is dramatically reduced. This, in turn, means that the method has a "built-in" tolerance for imprecise assessments: Whether you believe that a particular condition has a 30, 50 or 70 percent chance, does not make a big difference with regard to the overall result. You don't need to be sure about your assessment. It is sufficient if your judgement is reasonable and you will get a meaningful number (see Q2 and Q10). This is one of the advantages of the method (see Q7).

### 6. For which kind of cloud projects can we use your method? Does it work only for cloud projects?

You can use the method for any kind of cloud project.

The form "Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities" was designed for any kind of cloud project that requires the data held by the provider to remain confidential. This is why it is not only used to assess the foreign lawful access that is problematic from a data protection point of view (i.e. as determined under "Schrems II" and discussed in Clause 14 of the EU SCC), but *any kind* of foreign lawful access (e.g., under the US CLOUD Act).

It normally works with any cloud computing setup where the cloud provider itself or an affiliate or parent involved in the service are located abroad and could, therefore, become subject to foreign lawful access. If the provider and other parties involved are present in several countries you have to decide whether you want to cover all jurisdictions in the analysis (our clients often focus on the US).

You can also use the method in cases of intra-group outsourcings with or without the involvement of a commercial service provider. For example, we have applied the method in the case of an international insurance group that relies on M365 of Microsoft: We undertook a multi-country-analysis assessing both the lawful access risk on the part of Microsoft as well as the foreign system administrators of the group (Q11).

Last but not least, you can use the method in its current form or in amended manner to analyze other foreign lawful setups. For example, for a Swiss bank, we have used the method to evaluate the risk of a foreign lawful access if the bank permits its employees to remotely access the core banking system in Switzerland from their home offices in Germany and Austria, or for having call recordings temporarily processed outside Switzerland.

See also Q17 on the question whether to focus on the US or also assess other jurisdictions.

7. **What are the advantages and disadvantages of your method?**

Some of the advantages are:

- The structured approach that splits the problem in smaller pieces improves the quality of the prediction and makes it manageable;
- Users do not have to be sure about their assessments; they do not have to answer "yes" or "no", they can give a percentage figure indicating their confidence in one direction or another;
- Users can be imprecise when doing so; whether a particular condition is estimated to be fulfilled by a chance of 40, 50 or 60 percent is not relevant for the "big picture", which is what the method is all about;
- The method renders a clear result, as opposed to vague, generic and cautious statements usually found in legal opinions; it provides you with a clear statement on the confidence level of your assessment;
- The result and its calculation are fully transparent; it can be clearly seen which element contributed to the result in which manner and where the assessors where not sure about a factor of the overall assessment;
- The method has become a standard, supported by many and backed by various authorities (see Q38);
- The method favors the possibility of conducting an assessment with different stakeholders (even simultaneously) and thus obtaining a more controversial debate and often interdisciplinary input regarding the relevant aspects and questions (see Q18);
- The method is available for free;
- You can adapt the forms and create even new ones based on my method – designed to fit your own needs (Q45);
- You do not have to get my advice in using it; there are various of my peers who can support you;
- With the multi-scenario worksheets, you can even assess jurisdictions with a changing or uncertain legal landscape.

Some of the disadvantages of my method are:

- It requires a fair understanding of local law (but that's the case with every serious foreign lawful access assessment);
- It requires a fair understanding of the technical and organizational measures in place that may prevent foreign lawful access;
- If requires a fair understanding of how lawful access works (see, e.g., Q12, Q29 and Q31);
- The concept may not be easy to understand at first sight;

- It takes some time to diligently complete the assessment (in fact, for best results, do the assessment as part of a multi-stakeholder workshop);
- The forms used for the GDPR and Swiss DPA are country specific and available only for a limited number of jurisdictions; creating new ones involves costs (happy to help you, but I will want to make them publicly available for the rest of the community);
- The method acknowledges that every assessment of a legal or technical argument has uncertainties and that there is always a residual risk; this makes it much easier for people to attack it than a traditional legal opinion (where it may be less obvious if its authors are not 100 percent convinced that their opinion is correct);
- Some organizations have failed to convince data protection authorities about their assessments using the method (in my view due to a lack of understanding; see, e.g., Q39, Q26 and Q41);
- The method is best when used for pursuing a "risk-based" approach, which is several EU data protection authorities do not accept at the moment (but it can also be used for the "rights-based" approach, see Q3 and Q42).

## 8. Are there alternative methods for foreign lawful access risk assessments?

Yes, but most of are in my view either not fit for purpose or over the top.

I have seen largely the five following types of foreign lawful access risk assessments or "Transfer Impact Assessments" (**TIA**), as they are often referred to under the GDPR or Swiss DPA. But beware: Except for the last method, none of them will cover the US CLOUD Act (Q4); they usually only cover those foreign lawful access that is relevant under the GDPR or Swiss DPA:

- **Descriptive TIA:** The majority of the TIAs I have seen were mere descriptions of the lawful access laws in the country of the importer. In my view, these documents always were and are insufficient. They often are not even complete. Don't spend your money on such exercises, even if offered from well-known providers. In most cases, the descriptions do not even indicate whether the local laws are in compliance with the requirements of EU and Swiss law (e.g., the four basic guarantees). This is essential for an analysis under the GDPR (and Swiss DPA). I have created a freely available questionnaire that allows you to easily mandate a local counsel to provide you with exactly the information on local lawful access laws that you need – usually at a much lower cost (in my experience at around EUR 3'000).

- **Data Protection Authority TIA:** Following the "Schrems II" decision, the data protection authorities focused almost exclusively on transfers to the US and on the question whether the recipient of the data is an Electronic Communication Service Provider (**ECSP**) and, thus, subject to Section 702 FISA and EO 12333 (two problematic US laws that govern lawful access). If so, they claim that data may not be transferred in plain text because the recipient will have to turn it over to the US authorities. This was always wrong because there are various additional legal and other conditions that need to be fulfilled for a lawful access to occur (see Q29). For instance, in the US, the ECSP can only be ordered to turn over what is within its "possession, custody or control", which may often not be the case if customers take the right steps (Q36). Most data protection authorities, however, did not consider these additional conditions and were not interested in a serious assessment. A considerable number of EEA data protection authorities believed that any data transfer involving a US-based provider was illegal, even though this had no merit (see also Q42 and Q41 for the Swiss authority's view). Only over time they acknowledged in private discussions that they had been too extreme in their view. With the adequacy decisions in 2023 and 2024 the issue was off the table for them.
- **US Service Provider TIA:** Another class of foreign lawful access assessments, usually created by US-based service providers, provided (a) a description of local laws (e.g., Section 702 FISA), (b) they list all their technical and organizational measures, and (c) they declare that they have never or hardly ever received a problematic lawful access request, and if they were to receive one, they would exam them particularly carefully. It is obvious that these assessments are almost as useless as the first category. I never agreed with much what the Austrian data protection authority said on Google Analytics, but it was right to conclude that most of the technical and organizational measures apparently referred to by Google will not prevent lawful access. For example, the security of a data center is irrelevant when it comes to lawful access. What is relevant is whether the provider has specific measures in place that will allow it to push back on lawful access requests. Most US-based service providers have never understood this point, which is why they do never described or implement these measures in their TIAs. Again, I have created a free questionnaire to find out about these measures.
- **The Risk-Rating TIA:** The fourth type of lawful access assessments are more or less sophisticated tools offered by various law firms and consultants that are able to produce, in one way or another, a "lawful access risk factor" for each third country. For example, Australia is a lower risk than the US, but Russia and China is much higher. Users are usually asked to answer a number of

questions about the technical and organizational measures undertaken and the data at issue. The answers are used to up- or downwards adapt the risk rating. This results in a final assessment, for example green, amber, red or a risk rating number. These tools are efficient and produce good-looking results, but people should not expect them to withstand scrutiny. They are a kind of "fig leave" approach for low-risk international transfers, which makes perfect economic sense. I have also created a freely available form to perform such "lower risk" assessments more easily than with my original method (which is for a more in-depth analysis).

- **The "Rolls Royce" TIA:** The fifth type of lawful access assessment is the "full memo" provided by a local law firm in the country of the recipient analyzing in detail the use case against the background of the local lawful access laws. It is by far the most expensive approach, and I never really seen it in practice. If you read the European Data Protection Board's paper on supplementary measures following the Schrems II decision[12], this is what they obviously had in mind and expected to be created for every transfer, which is – with all due respect – entirely out of proportion.

If you have another approach used in practice that I should list here, please let me know. Since the establishment of this FAQ I received no such proposed dditions.

I am aware that my method, too, has disadvantages and weaknesses (I list some in Q7 below), but much to my surprise, it so far seems to be the most practicable solution in cases where people need a *serious* foreign lawful access risk assessment. I also never got a response with substance when I asked critical commentators to show me a better one or tell me how to improve the method as such; the main critical comment was that people who use it may have to repeat assessments from time to time, and that the Delphi method would result even better results when done anonymously (I agree with both suggestions). I am also not aware of my method ever having been challenged with substance. If you find any errors or ways to improve it, let me know.

There meanwhile even has been an independent legal opinion that concluded that there is no alternative that permits for a structured and systematic approach as does my method.[13]

---

12 See https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf, archived at https://perma.cc/BCW5-MJ4B.

13 XXXXX.

### 8a. In times of the Trump administration, does the method still work?

Yes, it does.

The method does not assume a particular legal system or reliability of a legal system in the country at issue. It can in principle be used to assess the risk of foreign lawful access in any country. Of course, in many setups, the strong rule of law and good separation of power are key elements for keeping the risk low, but the lack of such elements can be equally expressed when completing the Excel form. For instance, if there are no independent courts, then the government may be inclined not to follow certain restrictions that a cloud provider could rely on in defending the data of its clients.

What is special with regard to the developments under the Trump administration are that there is considerable uncertainty on how the legal situation will develop in the coming years. To cover this, we expanded the method by allowing users to assess the risk based on four different scenarios on what could happen in the next years. This allows them to take different possible developments into account in their risk assessment.[14]

## B. USING THE METHOD IN PRACTICE

### 9. Which assessment period shall we use?

In practice, most often a period of 3 or 5 years is used, but this depends on how stable you consider the circumstances underlying the assessment to be. Hence, where data is exported to a country that is not stable in terms of lawful access, shorter periods may be adequate.

The assessment period is relevant in three ways:

- If targeted lawful access scenarios are assessed (e.g., US CLOUD Act), it will serve as the basis for calculating the probability that a foreign authority will have an interest in gaining access to the data at issue. In a typical assessment scenario, this value will never be zero because the organizations can usually never with 100 percent certainty exclude that a foreign authority will want to get information from them. If they had one case in the last ten years, they may use this past experience as a basis and apply it to the assessment period looking forward (usually with a margin, see Q16). The forms will take care of the calculation.
- The assessment period has to be kept in mind when making the assessments, i.e. you have to consider the developments that are to happen during the assessment period. This can be a technical

[14] See https://www.vischer.com/en/knowledge/blog/how-to-deal-with-us-cloud-risks-in-times-of-trump/ for more comments on the situation in the US as of May 2025.

or organizational development (example: if you rely on the employees of your cloud provider not having day-to-day access to your data because this is written in the contract and this is how the provider is organized today, you should choose an assessment period during which you can expect this situation to remain stable), it can be a legal development (example: if you rely on a particular legal argument, ask yourself whether there are changes in law foreseeable that may force you to change your assessment) and it can be a change in other circumstances (example: the relevance of particular information for national security may increase or decrease).

- The assessment period is used to calculate the number of years used to express the probability in an alternate manner (see Q10). Hence, if the stated assessment period does not match the "horizon" of your assessment of the individual technical, legal and factual components then the number of years will not be correct (e.g., your period is defined to be a month, but your assessment is made with the next years in mind, the number of years will be much too low).

The foregoing leads to three conclusions:

- You need to carefully balance the assessment period. The shorter it is, the less meaningful the probability figure will be because it is a statistical value. The longer the assessment period is, the higher the margin of error will be because the circumstances forming the basis of the forecast may change over time.[15]
- You should redo the assessment when the circumstances you have relied on change but in any event before the assessment period ends. This also means that you should keep in sight the circumstances you have relied on, insofar this is practically possible.

If you have legal uncertainties, but nevertheless need to undertake an assessment for a several years, you may also consider using the multi-scenario version of the method, which allows you to do several separate assessments that deviate from your base assessment on the grounds that your basic assumptions may turn out to be wrong. You can define three alternative scenarios that you can give a probability, and repeat your assessment for these three scenarios. The Excel will calculate the weighted average.

---

15 Even over the period of a few years, there can be developments that increase the probability (more aggressive authorities, more cases, changes in law) and developments that decrease the probability (better protection, changes in law or behaviour of authorities).

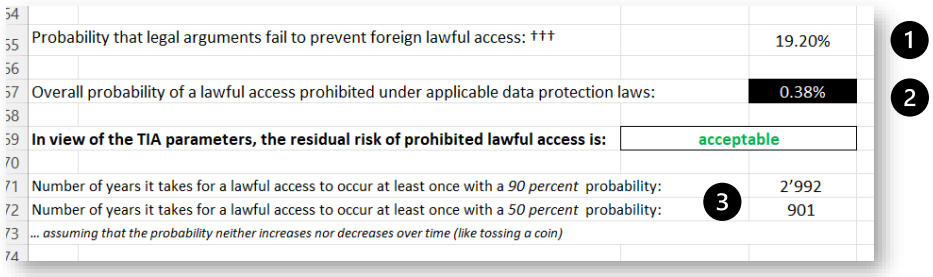
## 10. The method results in probability figures – what do they mean?

It tells you whether there is a realistic chance (or danger) or merely a theoretical possibility that a prohibited lawful access will happen during the assessment period if you do the transfer or project.

You can also think of it as the objective level of confidence that no lawful access will happen based on your assessment. In that case, you have to inverse the number, i.e. subtract the percentage from 100 (e.g., if the probability of a lawful access is 0.8 percent, then your confidence is 99.2 percent – you are 99.2 percent sure that no lawful access will happen during the assessment period).

This allows you to answer the key question whether you have "reason to believe" that such access will occur – depending on the approach you want to take. The number also indicates the effectiveness of the technical and organizational measures undertaken to prevent a foreign lawful access and the confidence you have in your assessment.

Depending on the form you use, you will get several probability figures to work with. This excerpt is from the form "EU SCC Transfer Impact Assessment (TIA)" for US law:




1. This the probability that the importer will fail to successfully challenge a request for production on legal grounds. It refers to how likely the importer will actually be required under local law to produce the data if requested. This is the number that is relevant for those who follow the "rights-based" (or "zero-risk") approach (which does not require this number to be zero, because it represents the user's confidence: Q3, Q43). You can also express this value inversely: In the above example, the assessor is about 80% sure that local law does not require the importer to permit a problematic lawful access.

2. This the probability that the importer will not have to produce the information during the assessment period. This is the number that is relevant for those who follow the "risk-based" approach. It does not only take into account the legal situation, but also practices in the importer's country, including past experience. Taking into account all factors, the assessor is 99.62 percent sure that there will be no problematic lawful access.

3 This the same probability but expressed in years, taking into account the assessment period. Since some people find percentage figures not intuitive, with the help of an actuarian of one of my clients, I have added a formula used in the insurance industry to calculate the probability in years. For instance, a probability of 1.25 percent over a period 5 years means that, statistically speaking, at least one lawful access is to happen with a 90 percent chance every 915 years assuming the probability were to remain the same.[16]

I do caution to read too much into this number; it is merely a method to express the probability in another form to help people better understanding the percentage value (which remains the key value). This is relevant because they have to decide whether they have "no reason to believe" that a problematic lawful access will occur during the assessment period. The "number of years" value has the advantage that it is only one number, as opposed to the percentage figure, which has to be read in conjunction with the assessment period. As intuitive and convincing the number of years may be, using it has certain limitations to consider:

- *First*, it should not be taken at face value. In the above example, the result does – of course – not mean that we are "safe" for the next 914 years. The number is an alternative method of expressing a probability, but it remains a purely statistical value. The number does *not* say if and when the case is to happen. Similar formulas are used for indicating the probability of natural disasters for the same reason, which is that many people prefer them over percentage values in combination with an assessment period. If a serious earthquake is estimated to happen only every 100 years, it doesn't mean that it can't happen tomorrow and another one year thereafter.
- *Second*, the number of years relies on the assumption that the chances of a lawful access neither increases nor decreases over the entire period time. It goes without saying that over 915 years the chances of a lawful access will in any event change. Even over the period of a few years, there can be developments that increase the probability (more aggressive authorities, more cases, changes in law) and developments that decrease the probability (better protection, changes in law or behaviour of authorities). This is why the assessment has to be repeated regularly (see Q9).

---

16 The more 5-year-periods you "add" in a sequence (or that pass by), the higher the probability of the event happening will be if the probability remains at 1.25%. After 1'831 years you will reach 99% and after 2'000 years (i.e. 400 5-year-periods x 1.25) you are at 100% (which still does not mean that the event has happened or has not already happened several times; it is merely the statistical probability that it has happened at least once in this period).

- *Third*, the calculation is, due to its very nature, directly related to the assessment period (so changing the assessment period will change the number of years). It is based on the assumption that the individual assessments of the legal and factual elements have actually been made in view of such assessment period. This is why the assessment period must be defined reasonably (see Q9).

The precise numbers are not relevant, as they are the result of a calculation (see Q5 and Q22). It's the magnitude that counts. A value in the range of 915 years will be understood by most people as an indication that they do not have to expect a prohibited lawful access to happen in the next five years for which you have made the assessment. In fact, it is much more likely that an earthquake will damage your house.[17]

If you want to better understand how the figure is calculated, see Q5.

If you think about translating a percentage figure into words, see Q20.

If you want to better understand what the European Data Protection Board recommends you determining in terms of problematic foreign lawful access, see Q3.

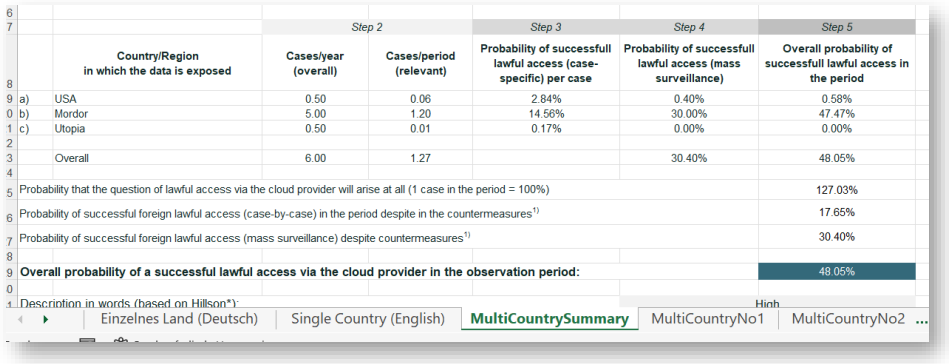
Some, such as the Danish data protection authority, apparently believe the figure indicates the remaining share of transfers that are subject to a prohibited lawful access. See Q26 why this is wrong. Others, including the Swiss data protection authority, found the figure to be too low case. See Q35 and Q27 on that point.

## 11. Can we use the form for different jurisdictions at the same time?

The form "Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities" provides for this possibility, although most focus on the US (Q17).

If you look at the template, there is a separate worksheet with for a multi-country-assessment (prepared for three distinct jurisdictions):

[17] In Switzerland, houses are built to withstand earthquakes that happen every 300-500 years; the assessment period is 50, not five years.



| | | Step 2 | | Step 3 | Step 4 | Step 5 |
|---|---|---|---|---|---|---|
| | Country/Region in which the data is exposed | Cases/year (overall) | Cases/period (relevant) | Probability of successfull lawful access (case-specific) per case | Probability of successfull lawful access (mass surveillance) | Overall probability of successfull lawful access in the period |
| a) | USA | 0.50 | 0.06 | 2.84% | 0.40% | 0.58% |
| b) | Mordor | 5.00 | 1.20 | 14.56% | 30.00% | 47.47% |
| c) | Utopia | 0.50 | 0.01 | 0.17% | 0.00% | 0.00% |
| | Overall | 6.00 | 1.27 | | 30.40% | 48.05% |
| Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%) | | | | | | 127.03% |
| Probability of successful foreign lawful access (case-by-case) in the period despite in the countermeasures[1)] | | | | | | 17.65% |
| Probability of successful foreign lawful access (mass surveillance) despite countermeasures[1)] | | | | | | 30.40% |
| **Overall probability of a successful lawful access via the cloud provider in the observation period:** | | | | | | 48.05% |
| Description in words (based on Hillson*): | | | | | | High |

Einzelnes Land (Deutsch) | Single Country (English) | MultiCountrySummary | MultiCountryNo1 | MultiCountryNo2 ...

As discussed in Q6, a typical use case could be an intra-group-outsourcing. Another use case could be a provider with access to customer data being present in several "risky" jurisdictions at the same time.

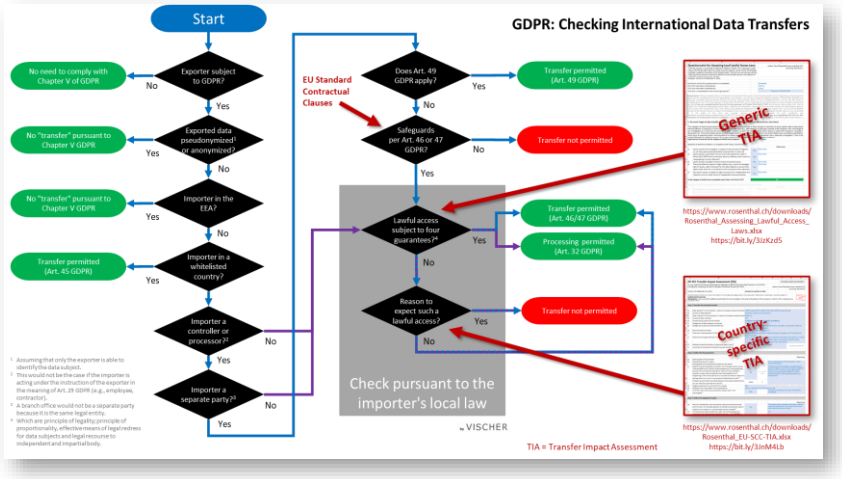
## 12. You offer different forms for assessing foreign lawful access. Which one should we use?

This will depend on the obligations you have to comply. There are basically two scenarios where you need to perform a Transfer Impact Assessment (**TIA**):

- **Compliance only with GDPR:** If you are subject to the GDPR (or Swiss DPA) you will have to comply with the "Schrems II" requirements for exports to countries without an adequate level of data protection, in particular if you use the EU Standard Contractual Clauses (**EU SCC**). Clause 14 of the EU SCC expressly refers to the parties performing such a TIA. But even if you do not use the EU SCC, it may be necessary to perform a TIA, for instance in connection with BCR or transfers under Art. 32 GDPR (e.g., to a foreign branch).

  For doing such a TIA, you need the form "EU SCC Transfer Impact Assessment (TIA)", which is currently available for the US, India, China and Russia. For other countries, I or somebody else would first need to create a country-specific version of the TIA because the analysis is different for every jurisdiction. Note that the form for the US is no longer necessary since the adequacy decision concerning the US in 2023 and 2024 (formally, a TIA is still required unless you export personal data under the Data Privacy Framework, but a "pro forma" TIA is sufficient; a sample is available here).

  However, before you actually do perform a country-specific TIA, please make sure whether you really need one. While this is clear for countries such as the India, China and Russia, it may not be clear for others. My TIA Toolbox contains more detailed instructions on how you find out whether you need to perform a TIA and which form you have to use:




If you find these forms too complicated and your case at hand is a lower risk case, you can also consider using the "Simplified TIA" contained in the same file. It is not country-specific and therefore requires you to assess the countries lawful access laws separately (for which the same file also contains a questionnaire for local counsel). It does *not* make use of my statistical method.

- **Compliance with professional or official secrecy:** Some transfers or projects involve data that is not only subject to the GDPR (or Swiss DPA), but also subject to professional or official secrecy.

  In Switzerland, this is the case, for instance, where banks, hospitals, law firms or public authorities move to the cloud with data about their "clients". These secrecy obligations (e.g., bank secrecy in the case of a Swiss bank) go far beyond the requirements of the GDPR, i.e. you do not only have to assess the risk of foreign lawful access pursuant to Section 702 FISA or EO 12333 (such as is an issue as per the "Schrems II" requirements). You also have to – in principle – make sure that there is not *any other kind* of foreign lawful access, even if it were acceptable under European standards (e.g. lawful access under the US CLOUD Act, which essentially mirrors Art. 18(1) of the Cybercrime Convention of the Council of Europe; similar provisions exist in all European countries).

  Hence, a Swiss bank does not only have to make sure that there is no lawful access by US authorities, but it also likewise has to ensure that there is no lawful access by any foreign authority, including those who are subject to the GDPR. For this you need to use the Excel with the name "Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities". That said, many will still focus on assessing only the lawful access risks from the US if they are using a US-based cloud service provider such as Microsoft, Google or AWS (see Q17).

Note that the aforementioned requirements for those who are subject to professional and official secrecy obligations are legally speaking too absolute. I make them to be on the "safe side". Depending on the type of professional or official secrecy and the specific circumstances of the case, foreign lawful access may not always be considered a violation of the secrecy obligation at issue. For example, the level of protection against foreign lawful access required for client-identifying data of a Swiss bank may be higher than in the case of data held by a medical doctor. In such cases, data subject expectations, data subject protections under foreign law, waivers, the purpose of the secrecy obligation and other factors have to be considered, too.[18] Yet, in my experience, most organizations do not want to undertake such a detailed legal analysis, which is why they assume that *no* foreign lawful access shall be considered permitted.

See also Q29 at the end on how to complete the Excels with regard to mass surveillance.

### 13. Do we have to fill out a TIA form for every single transfer?

No. You can combine an analysis for several transfers if their share the same "risk profile", i.e. if the importer is the same or of the same kind, if the measures to protect the personal data and all other aspects relevant for assessing the lawful access risk are also more or less the same. This is particularly often the case in intra-group transfers or if several affiliates of a group use the same service provider in the same technical and organizational setup.

See also Q21 at the end for an example where two separate assessments have been made for one transfer and why.

### 14. Which "residual risk" of foreign lawful access is acceptable?

There is no generally accepted position.

In my view, the "no reason to believe" test under the GDPR and Swiss DPA (see Q3) means "highly unlikely" if translated to words, but not "impossible". Some would consider a probability of 10 percent to be a reasonable maximum number for such standard. This was also more or less the decision of the Canton of Zurich when it decided to use my method as a standard for all cloud projects; it requires 100 or more years till the probability of at least one access rises to 90% (Q38).

---

[18] For more details, see David Rosenthal, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter 10. August 2020 (only available in German) (https://www.rosenthal.ch/downloads/Rosenthal-CloudLawfulAccess.pdf, https://www.rosenthal.ch/downloads/Rosenthal-CloudLawfulAccess-Anhang.pdf, archived at https://perma.cc/HF65-X8UY and https://perma.cc/J35T-QSWT).

According to a proposal made by Hillson (see Q20), any value below 5 percent will fall in the lowest probability category ("Very low"), any value between 5 and 10 percent will still have to be considered "Low". Hillson's research shows that a probability of 90 percent or more is considered almost certain or even definite, which I believe is probably a correct conclusion for most people. This would support the 10 percent threshold because a 10 percent residual risk means that you are 90 percent certain that the event will not occur. That said, everybody has to make their own conclusion as to what how the number is to be translated in view of the "no reason to believe" test.

Under Swiss professional and official secrecy law, I would consider diligence requiring that all technical and organizational measures are taken that will result in a foreign lawful access risk being highly unlikely. While this does not exclude that a breach may occur, it is legally also not required to achieve a "zero risk" status (which conclusion is shared by public prosecutors, see Q38). If a party has taken the steps to prevent an unauthorized access that a diligent party would do, this is generally considered sufficient (however, see the discussion in Q42).

The form "EU SCC Transfer Impact Assessment (TIA)" will tell its user whether the transfer is acceptable or not. This is not based on my judgement but based on the threshold defined by the user in Step 2:

| | | | | | |
|---|---|---|---|---|---|
| 28 | | Ending date of the assessment based on the above: | 01.03.2027 | | situation. |
| 29 | c) | Determining the acceptable residual risk of foreign lawful access: If the probability of a lawful access happening in the assessment period is so low that the chances of it are still only at 50:50 if another *xx* years were to pass by, then the probability of it happening in the initial period is so low that we have no reason to believe that it will occur in such period. What should *xx* be?[4)] | 30 | (= in total 35 years) | *We believe that if the probability of a prohibited lawful access to happen is so low that even after an additional 30 years in a row the chance of a prohibited lawful access occurring is still only at 50:50, it is of mere theoretical nature in a five year period which we are looking at here.* |
| 30 | | Required minimum probability that *no problematic lawful access* occurs during the assessment period for us to have "no reason to believe" that it will actually occur during the period (you can either manually enter a value or leave it calculated based on the above figure):[5)] | 90.57% | 30 | |
| 31 | d) | Target jurisdiction for which the TIA is made: | USA | | (if there are additional jurisdictions, perform a separate TIA) |

This process is not very intuitively, but I – so far – have not found a better solution. Line 30 provides the threshold, or the level of confidence, that must be achieved to conclude that the user has no reason to believe that a problematic lawful access will occur (see the EDPB recommendations discussed in Q3). In the above example, the 90.57 percent is calculated on the basis of the 30 years entered in the field above. It is the number of years that has to pass following the assessment period before the probability of a lawful access will have risen to 50:50.

If a user prefers to directly enter a percentage number, it can do so in line 30. If a user believes the 30/35 years is too low, it can enter a higher number, for example 95. This would mean that the user would find a risk acceptable only if it is so low that even after 100 years without any lawful access, the chances of one occurring is still only at 50:50. The number 95 would increase the confidence level to 96.59 percent.

### 15. How do we find out how often a cloud or Internet service provider is confronted with lawful access request?

First consult what is commonly referred to as a "transparency" report. These are publicly available reports in which providers publish statistics about the number and type of lawful access requests they have been getting on a yearly or half-yearly basis.

Martin Steiger maintains a list of links to the transparency reports of Swiss and various global providers. Another global overview is provided by AccessNow. It reports that since Google as the first company published a transparency report in 2010, some 90 companies are doing this today. You can also search the Internet for "transparency report" plus the name of the company to find it.

These reports cover different types of lawful access. In my experience, they are often of limited value because they do not provide detailed information and do not separate the categories of requests in a manner that is usable for conducting an effective transfer impact assessment. If I am evaluating a US provider for a Swiss business customer, I am not interested in learning how many requests the provider has received from US law enforcement if I am not told how many of those requests actually concerned Swiss business customers. Maybe all of the requests concerned US customers, which were consumers and which concerned a different service than the one I am considering for my client. Hence, these requests are irrelevant for my case and may even create a wrong impression. It is also necessary to distinguish the type of lawful access (e.g., FISA, Stored Communications Act/US CLOUD Act) to understand their relevance and how to consider them.

If you are not satisfied with the transparency report, then ask the provider directly. Many will give you more detailed or specific information, even though some will only do so under a Non-Disclosure Agreement. It is true that they cannot tell you about whether they have been asked under Section 702 FISA to search for a particular target, but they can tell you, for instance, that they have *not* yet received any Section 702 directive, which is a precondition to do a Section 702 search (Q29). They can also tell you, as Microsoft did in 2021, that they never received a lawful access request to disclose data of a EU public sector client, to give an example. Google has made a similar statement with regard to Google Analytics, when this was an issue in a specific case.

### 16. How do we find out how much a foreign authority is interested in our data and when is this relevant?

This question is primarily relevant when assessing the risk of *targeted lawful access* (see Q28 for a description), for example under the Stored Communications Act / US CLOUD Act. When you perform "only" a Transfer Impact Assessment under the GDPR or Swiss DPA, which is

about *mass-surveillance* as opposed to targeted lawful access, the question is less relevant (see below).

**Targeted Lawful Access**

Assessing the risk of a *targeted* lawful access consists of two elements:

- You need to understand whether it would be possible for an authority in the jurisdiction to force your provider (or other type of importer, e.g., a local affiliate) to produce the data. This assessment is done by evaluating the technical and legal requirements that have to be fulfilled for such a lawful access to be "successful" (from the authority's point of view).
- You need to forecast how often the authority will try to pursue such lawful access against the provider with regard to your data. This second element is crucial because if you and your data is of no interest to the relevant foreign authorities or if they have other, easier means to obtain your data, why should they try the burdensome way of compelling your provider? The answer and practical experience is that they will not – thus reducing the risk of a foreign lawful access by way of your provider.

In my form "Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities" (but also some country-versions of my Transfer Impact Assessments for EU SCC purposes) you are therefore asked to forecast the number of cases per year in which a foreign authority will try to legally obtain data from you.

It is not necessary to *know* how often this will happen (nobody can). For risk management purposes, it is sufficient to make a diligent, reasoned estimate. I cannot give a "one size fits all" response to how to do such a forecast. Yet, most organizations do have past experience they can rely on. This is because if a foreign authority wants to obtain data from a company, the authority will usually contact the company and try to obtain it from the company directly, which is why the company will learn about it. If a foreign authority wants to obtain evidence for investigating a crime without providing the Swiss company advance warning, it will usually use judicial (or administrative) assistance. The Swiss authorities will then contact the company or even conduct a dawn raid. Either way, the company will sooner or later find out about the request. In Switzerland, 95% of the judicial assistance requests in criminal matters from the US are granted.[19] Hence, a company usually knows how often a foreign authority tried to legally obtain data.

Here is the example of a Swiss bank:

---

[19] This is based on information we have been able to obtain from the Federal Office of Justice in early 2022.

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | Year | Requests | US | Ireland | Crimes | Crimes US |
| 2 | 2021 | 4 | 0 | 0 | 1 | 0 |
| 3 | 2020 | 2 | 1 | 0 | 0 | 0 |
| 4 | 2019 | 5 | 1 | 0 | 2 | 0 |
| 5 | 2018 | 5 | 2 | 0 | 0 | 0 |
| 6 | 2017 | 6 | 2 | 0 | 2 | 0 |
| 7 | 2016 | 6 | 2 | 0 | 0 | 0 |
| 8 | 2015 | 4 | 2 | 0 | 1 | 0 |
| 9 | 2014 | 2 | 1 | 0 | 1 | 0 |
| 10 | 2013 | 1 | 1 | 0 | 0 | 0 |
| 11 | 2011 | 1 | 0 | 0 | 1 | 0 |
| 12 | **Summary** | **36** | **12** | **0** | **8** | **0** |
| 13 | **Per year** | **3.6** | **1.2** | **0** | **0.8** | **0** |
| 14 | | | | | | |

As one can see, over the past 10 years, the bank received 36 requests for information from foreign authorities, 12 of which came from the US, zero from Ireland (which was included because the provider contract party was Microsoft Ireland) and none of the US cases was about a criminal matter (as opposed to civil, regulatory, tax matters). It should be noted that many of the requests involved the US-Swiss-tax dispute, which was considered over and a "one-time"-matter. In the risk assessment, the bank concluded that a forecast of 0.7 cases per year would be adequate for the next five years. This number seems very high in view of their past experience, however, the bank wanted to take a cautious or conservative approach to the forecast. Also, it wanted to include a safety margin to take into account (i) tax cases that would as well be considered "serious crime" cases (i.e. permit a lawful access under the US CLOUD Act / Stored Communications Act) and (ii) cases where a US authority tried to obtain information from the bank, but the bank never learned of this in the past. These thoughts can be documented in the Excel in one way or another to allow a reader to understand how the figure was achieved.

With this kind of past experience, it is usually possible to make a reasonably solid forecast for risk management purpose. The forecast is often much higher than what has to be reasonably expected, but most users prefer to be cautious.

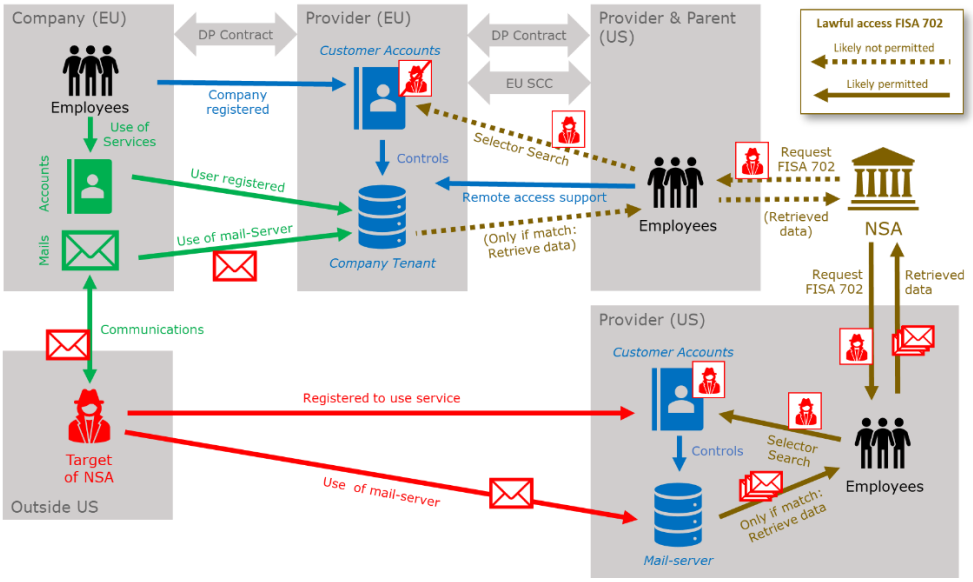
There are, of course, more aspects to consider. For example, you can consider whether the foreign authorities would have an interest in a particular set of data (e.g., accounting records, but not emails). If they are likely interested in accounting data, this could mean that moving emails to the cloud will not result in any increased lawful access risk. This, however, may not be true: The authorities may not know what data a company has stored in the cloud. Hence, even if a company does not store accounting data in the cloud, a foreign authority may still want to lawfully access the company's cloud instance.

**Mass-Surveillance**

In the case of mass-surveillance it is of less interest whether the foreign authorities are interested in the data of a particular company. The

reason is that in the case of mass-surveillance, by definition, all data of a particular kind is searched for relevant communications (e.g., all traffic that flows across an Internet backbone). This aspect is also constantly emphasized by data protection authorities.

However, it is not entirely correct. The reason is that depending on the type of mass-surveillance law, a provider that is compelled to perform mass-surveillance will not have to search each and any customer content but only selected sets of data it has about its customers. Under Section 702 FISA, which is the main problematic piece of law when transferring data to the US, providers are required to search their customer database for identifiers of specific individuals or companies that are targeted by the NSA. They do not have to search each and any set of data they have. If a customer is not a target, no data will be collected and provided to the NSA. The following chart illustrates the process (which is discussed in much more detail in Q29):




Therefore, it has to be considered whether a customer is likely a target and whether the kind of customer accounts and services offered by a provider is likely of interest to the NSA. For example, free email services and social media platforms are of interest, whereas services offering website analytics or CRM services are likely not.

### 17. Shall we focus on the US when assessing foreign lawful access in the cloud or also take into account other countries?

Most will focus on the US in my experience. The reason is that most cloud projects are based on the cloud services of Microsoft, AWS or Google, which all are US-based hyperscalers.

Theoretically, you should consider doing an assessment for each foreign country from which the provider (or your own staff and colleagues at other group entities) can access your data in plain text. Hence, if you are relying on Microsoft in Europe, you will normally have a con-

tract with Microsoft Ireland Operations Ltd., which means that access is at least possible also from Ireland. That said, most will consider the risk of foreign lawful access from Ireland to be negligible and do not further consider it.

I may note that the Public Prosecutor's Office of the Canton of Basel-Stadt in Switzerland following a request of the Cantonal data protection authority in a pilot project involving two public hospitals in Basel, Switzerland, found that it was acceptable to limit the foreign lawful access analysis to the US in a case involving Microsoft (see Q38). In fact, all data protection authorities with which I had discussed this issue so far agreed.

In other projects we have already done assessments for other countries, such as Germany, Austria or India – in each case because there was day-to-day access to data at issue from these countries. We have also done assessments for Luxemburg, Sweden and the United Kingdom, to give some examples. Notably, they are all very similar in their outcome, as most legal systems provide for similar lawful access rules that will cause a foreign lawful access to be more likely or less likely, depending on the setup. For examples:

- Some countries restrict their authorities in accessing or requesting data that is stored in other countries (i.e. no cross-border access);
- Some countries do not permit their authorities in accessing or requesting data in other countries if this violates criminal law of these other countries (e.g., professional secrecy laws);
- Some countries only permit their authorities to seize data that is actually stored "at rest" on a computer system, but not data that is processed merely in process or stored only temporarily.

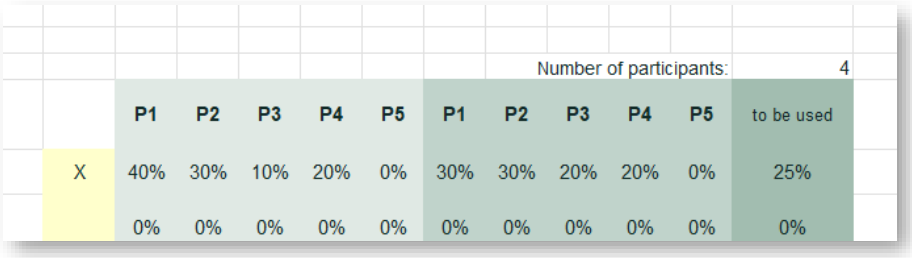
We do expect the issue of foreign lawful access to become a more prominent topic, though, once the e-evidence regulations will be in place within the EU, making cross-border lawful access requests much easier.

### 18. How do group assessments using the Delphi method work?

To begin with, I strongly encourage doing foreign lawful access risk assessments in a group setting. This significantly increases the quality of the assessment and its acceptance among the stakeholders. This is why I have built in support for group assessments in the form of the "Delphi" method.

The "Delphi" method is a widely used technique that will help you get better assessments in a group setting. I have implemented support for it in various of my forms and have used it myself in many workshops with success.

It requires a facilitator and a panel of assessors (my implementation supports up to five of them). The method works as follows:



| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | Number of participants: | 4 |
| | | P1 | P2 | P3 | P4 | P5 | P1 | P2 | P3 | P4 | P5 | to be used |
| | X | 40% | 30% | 10% | 20% | 0% | 30% | 30% | 20% | 20% | 0% | 25% |
| | | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% |

1. Enter the number of participants in the relevant field.
2. For every value in the form that requires an assessment, a row in the "Delphi" section has already been prepared for the group assessment.
3. Mark the yellow field with an "x". This will hide the sample text and prevent the participants from being influenced by the sample text.
4. Have each participant think of an appropriate value for the assessment at issue.
5. Ask each participant for their value and put it into the first columns (P1-P5). In the above example of four participants these values are 40%, 30%, 10% and 20%. The participants should at this stage neither explain nor discuss their own assessment.
6. Once completed, discuss the values; you may remove the X. You can ask each participant to explain why they arrived at the value that they have given to you.
7. Once the discussion is over, have each participant again think of an appropriate value and put their value in the second section for each participant (P1-P5). In the above example you can see how the values have slightly changed following the discussion. They are now 30%, 30%, 20% and 20% – the discussion convinced some of the participants to amend their final vote.
8. The last column will provide you with the average number. You can use it for completing your assessment. The average will be calculated on the number of participants entered into at the top of the section.

My experience in using the Delphi method is very positive for a number of reasons. *First*, asking each participant to provide a number without discussing it will ensure that the participants do not really influence each other in the first round. This will avoid unnecessary "noise". *Second*, it will cause people to discuss the assessment more controversially, which improves its overall quality. This will often result in different figures in the second round. *Third*, the method allows different stakeholders to participate and enter into an interdisciplinary dialogue with

each other, which will help all participants to better understand the problem. *Fourth*, the assessments are of better quality and have a broader support base.

18a. **We cannot do a full workshop for every application. Isn't there a faster way to do an assessment?**

Yes, there is. I have developed a "light" version of the basic foreign lawful access risk assessment method that can be completed within five minutes. It is based on asking eight questions to identify standard provider situations that permit standard assessments. This can help an organization to handle large amounts of use cases. Contact me if you are interested in it.

## C. STRUGGLING WITH THE METHOD

19. **What are the most common misconceptions about your method?**

| Some believe my method … | In reality … |
|---|---|
| … only works for when relying on the risk-based approach | … my method "works" for both the "rights-based" (or "zero-risk") and the "risk-based" approach, as it implements both (Q3) |
| … uses statistical calculations to create the impression that lawful access is predictable | … it is a standard approach for risk assessments to determine the probability; the calculation allows us to determine the combined effect of the arguments why we believe we can prevent a lawful access; it reflects how confident we are (Q23) |
| … renders numbers that are too precise to be true | … it is not an accurate prediction but an accurate statistic calculation; what counts is the magnitude (Q22); also, the method produces results based on the user's own assessment of the legal and other arguments and calculates their "combined" effect – this is all (and it is entirely agnostic) |
| … renders numbers that are too low given that a US-based provider has access to the data | … this is what many people believe who only rely on their "gut feeling" – those who have completed it successfully think differently about it; the method itself is neutral and agnostic of any legal or factual argument (Q35, Q27) |
| … will tell them how many transfers or sets of data will be subject to lawful access | … the amount of transfers or data is irrelevant and doesn't affect the probability; if it is 1%, it doesn't mean that 1% of transfers or data will be lawfully accessed abroad (Q26) |
| … is conceptually wrong or has flaws | … my method is public since 2020 but so far I have not received any substantiated report of any flaw in its design or approach (Q8) |
| … has been dismissed by data protection and other authorities | … no authority having seriously reviewed it has dismissed it; quite the opposite is true, as it has received substantial support in both the private and public sector (Q39, Q38) |
| … is too complicated for day-to-day use | … this may be true for people not familiar with it, which is why I am offering also a "simplified" TIA for more clear-cut cases |
| … is not supported by authorities | … many authorities have adopted the method (Q38), but there are some data protection authorities that do not want to permit data transfers to |

| | |
|---|---|
| | the US *at all*, which means that there is no point in assessing the risk of a foreign lawful access, because there is hardly any use case where can be zero (Q39, Q41) |
| … produces no meaningful number | … if you have difficulties with imaging what a particular residual risk means, subtract it from 100 and you will get an objectively calculated confidence level that no lawful access will occur in the assessment period based on your own assessment of the legal and other arguments – show me a better method (Q10) |
| … tries to calculate something that cannot be calculated due to its nature | … the method does what every insurance does when assessing a risk; the calculation is merely used to combine the various pieces of the assessment you will be making when using my method – this is simple statistics |
| … doesn't work: If a US provider has access to data, it will have to produce it upon request | … US providers do not have to produce data it they have no legal and no day-to-day control of it, which they often do not have (Q35) |

## 20. Can a risk assessment consist of only one probability figure?

The risk assessment using my method is detailed and structured and it provides ample reasoning for every step. It consists of much more than a number. However, the number that results at the end is essential: It tells you how confident you are that no problematic lawful access will occur when combining your assessment of all the individual technical, legal and other arguments.

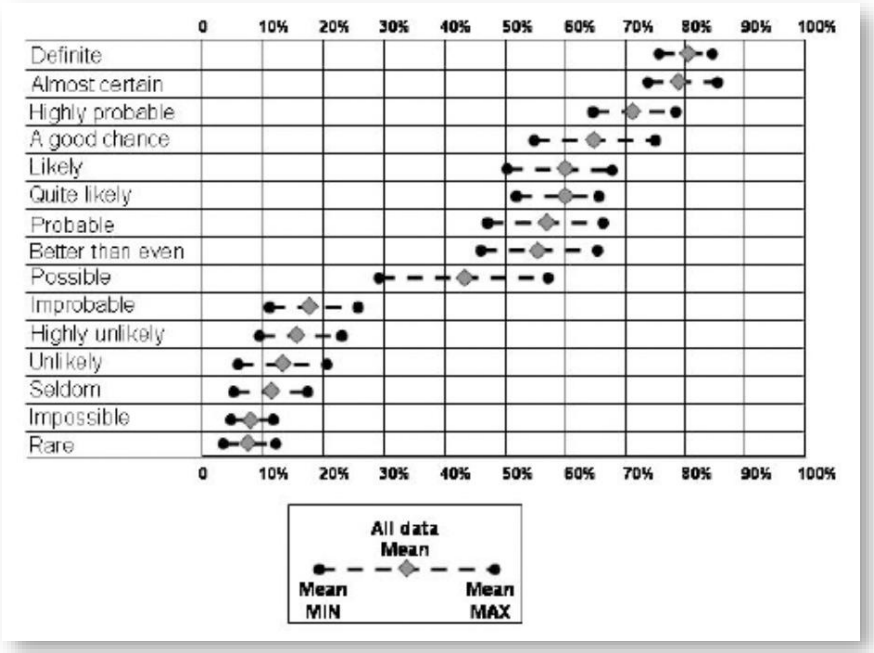
It is the same a lawyer does when providing you with a legal opinion, except that you will probably not find anybody telling you exactly how confident they are that their opinion will prevail in court. In fact, if you ask them, their confidence will usually be even lower than 90 percent, simply because they know that there is no certainty in life and how other lawyers apply the law. Lawyers are trained to use words to "hide" such uncertainty, but it always exists. Hence, if a lawyer tells you that you have a 90 percent chance winning a case, will you go for it?

In my experience, many assessments of properly prepared cloud cases result in a much high confidence that no problematic lawful access occurs. They are around 98 or 99 percent. The reason for such confidence is that the approach my assessment method is much more objective than that traditional lawyer assessments.

BTW: Determining the confidence or probability that no problematic lawful access will happen is also what EU data protection authorities require ("no reason to believe", see Q3).

People who are skeptical about expressing risk or probability by using a number should consider the alternatives. They are not better. Look

at the analysis of David Hillson as to how probabilities are expressed using words:[20]




If you look at the bottom end of the above table, you will find some people claiming an event to be "impossible" where others would consider it only "rare". As opposed to that, anything above 90 percent seems to be certain.

Hillson finds: *"Despite the evident importance of the probability dimension, subjective natural language terms are often used to describe probability, leading to a number of problems. However, even where the words are apparently well defined and in common use, individuals translate probability-related terms into percentage values or ranges unreliably, with a range of possible meanings, and with no consensus (as reported previously by Theil, 2002). For example, when someone says a risk is 'unlikely to occur', this can be interpreted to mean anything from around 5% probability through to a 20% chance of happening. One person might expect a 'likely' risk to occur with 50% probability, while another might take this to mean almost 70%."*

For this reason, I believe it is better to rely on percentage values. They add transparency (because you can see how you get there) and they remove the ambiguity of natural language.

If words shall nevertheless be used, Hillson based on various risk standards recommends the following model, which I have also implemented in one of the forms:

---

[20] David Hillson, Describing probability: the limitations of natural language. Paper presented at PMI Global Congress 2005—EMEA, Edinburgh, Scotland. Newtown Square, PA: Project Management Institute, 2005 (https://www.pmi.org/learning/library/describing-probability-limitations-natural-language-7556, archived at https://perma.cc/QJ5U-SV4N).

| Scale | Range |
|---|---|
| Very high | >50% |
| High | 26-50% |
| Medium | 11-25% |
| Low | 5-10% |
| Very low | <5% |

21. **Why is the probability of a foreign lawful access occurring assessed, but not the severity of the consequences?**

In a traditional risk assessment, both aspects are assessed. The risk is the combination of the two (severity x probability = risk). Even if the severity of damages is high, the risk can be low provided the probability is low.

In fact, the Dutch government, who also uses my method in their risk assessments of cloud service providers (Q38), have also included the severity of damages as another factor.

I have on purpose not done so. Unlike other risk scenarios, the legal requirements for cross-border transfers are different. The GDPR, the Swiss DPA and professional and official secrecy obligations under Swiss law (which is the origin of my method, Q47) provide that no lawful access shall occur *at all*, whether the data is particularly sensitive or not or whether it represents a special category of personal data. This is why my method focusses on probability, not severity. It *does* take into account the nature of the data when determining the probability, for instance how often a foreign authority would be interested in invoking the US CLOUD Act / Stored Communications Act in undertaking a lawful access (Q16).

In practice, if you have different risk profiles for different sets of data, you will perform two or more separate foreign lawful risk assessments. This is, for example, what we have done for the government of the Canton of Zurich (Switzerland), where we distinguished between data collected with government powers (e.g., data of the tax or police data) and other data (e.g., HR data). In our view, unlike in a classical data protection analysis, this is the proper distinction in cases of a foreign lawful access under the US CLOUD Act taking into consideration the purpose for which such an access would happen.

22. **How can the number be so precise and accurate?**

The number is not an accurate prediction, it is an accurate statistical calculation (see Q5). This is often confused.

The more factors you use to build it, the more granularity and fractions you will get in the resulting number. I could have included a formula to round the result or permit fewer input values (e.g., 0/25/50/75/100), but I decided to leave the input and calculated value as they are for

reasons of flexibility and transparency. If you don't like precise numbers but prefer a range, feel free to change the form (see Q45).

The Swiss data protection authority got confused about the apparent accuracy of the number (Q41). Do not fall in that trap. It is the magnitude that counts and how you get to the number, i.e. which legal and other arguments and measures you have considered in performing the assessment. The number merely represents the statistical-mathematical conclusion, much like an election prognosis that consists of an apparently very accurate number but can have a large margin of error.[21]

If you are still not convinced, ask yourself: Does it make a difference for the inhabitants of a city if an earthquake is to happen every 425 or 378 years? Probably not. Would you ask yourself why the probability is exactly 378 years? Probably not. You will probably have no reason to believe that an earthquake will happen during the rest of your life. In the present case we assess risks for the next few years only, usually not for periods of 10, 50 or 100 years. This forces us to reassess the situation regularly, which is good.

### 23. Can the risk of foreign lawful access be calculated after all?

Yes, it can. Every risk can be assessed in some way or another. My approach consists of splitting up the assessment in small pieces, which helps to avoid "noise", makes it easier for you and increases the overall quality (see Q24). The calculation is merely the mathematical method of combining these pieces to form an overall probability figure.

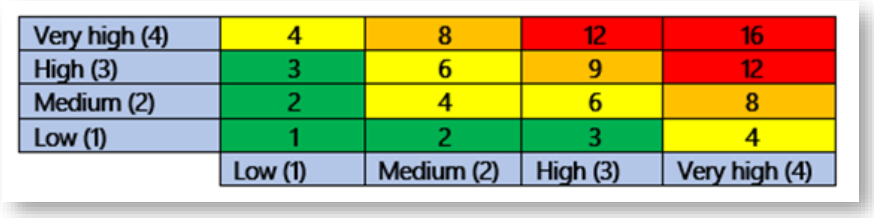
This is not about predicting when and how a foreign lawful access will actually happen. In essence, the number tells you how confident you are about the arguments and facts that will prevent a lawful access from happening. The statistical calculations are only used to *combine* these elements and come up with a "summary" of your estimates. This is no magic.

The concept of determining the probability of something happening is well accepted and state-of-the-art: Every insurance relies on it, the government does so when deciding on measures to protect us and companies use it when making investments decisions. Please also see Q24 on why we can assess the probability of something that has not yet happened.

Estimating probabilities are also the basis of assessing data security risks (in fact, the risk of a foreign lawful access *is* also a data security risk). These assessments are usually less sophisticated than the one I have chosen for my method. This is a typical risk matrix that experts use when assessing data security risks:

---

[21] Of course, the type of "prediction" based on an exit poll is an entirely different exercise than a lawful risk assessment. This is only to explain why the precision should not be misunderstood.



| | | | | |
|---|---|---|---|---|
| Very high (4) | 4 | 8 | 12 | 16 |
| High (3) | 3 | 6 | 9 | 12 |
| Medium (2) | 2 | 4 | 6 | 8 |
| Low (1) | 1 | 2 | 3 | 4 |
| | Low (1) | Medium (2) | High (3) | Very high (4) |

The chart is taken from an article "5 steps to an effective ISO 27001 risk assessment"[22] and is quite common. The risk assessment consists of creating a list of potential risk scenarios (e.g., a hacker being able to break in a system in a particular way). The expert will then briefly consider each such scenario and, based on an educated guess, rate (i) the probability and (ii) severity of damage that could be caused if the risk scenario materialize (in the above example on a scale from 1 to 4). Sometimes additional factors such as the "harm to reputation" or "detectability" are added, but even in these cases, these risk assessments for individual risks are often made quick and without much reasoning. This procedure is state-of-the-art and well accepted.

In the case of my method, I force people to "dive" a bit deeper because the "foreign lawful access" phenomenon is a problem that most are not yet used to and have difficulties in fully getting their hands around. By splitting up the problem in many smaller pieces they can more easily assess (see Q2), I will also help them to reduce the margin of error and increase the overall quality of their assessments (see Q24).

### 24. How can we assess the risk of something if we don't know whether and when it will happen?

This is the challenge of every risk assessment. Still, probability calculations are a recognized and accepted method for assessing and describing risks (see also Q23 for examples, including for data security risk assessments).

For example, normal buildings in Switzerland should be built to survive an earthquake that will happen with a 10 percent probability at the location of the building within its expected lifespan (e.g., 50 years). Specialists calculate the probability of a particular earthquake occurring for every region, even though none of them can tell you when and whether it will happen during the lifespan of the building. Will this stop anybody from relying on these calculations and build a house in Switzerland? No, because we have no reasonable alternative.

Please also consider the following:

---

22 https://www.itgovernance.eu/blog/en/what-is-an-iso-27001-risk-assessment-and-how-should-you-report-on-it, archived at https://perma.cc/S5T8-FGCD.

- My method uses various techniques that have been proven to increase the quality of professional predictions.[23] They include strictly following a defined structure when making the prediction, splitting up the problem in manageable pieces, mechanically connecting them and providing for group assessments (Q18).
- Most people have difficulty in assessing foreign lawful access risks because they lack experience with it. In reality, it is usually easier to assess than assessing the probability of an *unlawful* access to occur (be it by cybercriminals or be it by foreign governments). The reason: For lawful access, we both have past experience and we know the rules that authorities have to follow. This is why it is referred to as *lawful* access. While our experience may not be with cloud services, the underlying concepts of foreign lawful access are often not new – not even in the case of the US CLOUD Act.[24] For example, I have many years been dealing with US authorities trying to lawfully access data located in Switzerland; in all cases we managed them to give up such plans on the basis of certain provisions of Swiss law.[25] We can make use of these provisions if we ensure that data is stored at-rest in Switzerland, even if it remains accessible from the US. This will greatly reduce the risk of foreign lawful access. While we cannot be sure that the argument will work in every case, we have sufficient experience to conclude that the chances of success are very high, and my method supports this.

For both reasons, the calculation of the probability of a foreign lawful access using my method will often be much more solid than conventional information security risk assessments (which are often done based on educated guesses by experts, but without the measures to avoid noise and bias, Q23). That said, the quality of each assessment depends on those who make it. As usual, the principle "garbage in, garbage out" applies – as with any other method for risk assessments.

In case that the legal situation is evolving in the target country, you may consider the "multi-scenario" version for a more solid assessment, as you can have a mix of several assessments for different scenarios. This allows you to take such evolving situation into account, at least to a certain extent.

---

23 For those interested in the topic, read Cass R. Sunstein, Daniel Kahneman, Oliver Sibony, Noise: A Flaw in Human Judgement, 2021.

24 With regard to the right of US authorities to force US providers to provide access to customer data even located abroad, the US CLOUD Act merely reconfirmed a long-standing US court practice. Lawmakers felt the need to do so because one US court in a decision of Microsoft had attempted to change such practice. See, for example, https://www.hoganlovells.com/en/publications/demystifying-the-us-cloud-act, archived at https://perma.cc/X4G4-8D5Y.

25 Such as Art. 271 Swiss Criminal Code.

24a. **Does it make a difference if a cloud provider receives a gag order, i.e. is not allowed to talk about a lawful access?**

No, this is not relevant. In fact, it is to be assumed that most service providers will receive a "gag order" prohibiting them to inform their customer that a law enforcement authority has asked customer content to be produced to the authorities. This is also standard practice in Switzerland, and probably most countries in the world.

Yet, the fact that the provider is not permitted to alert the customer does not mean that such lawful access does not need to comply with the rules. In order to ensure that it does, it is, therefore, essential that the customer has agreed with the provider that the provider will legally challenge any lawful access request to the extent possible – even if the customer may not be informed about it. This way, even with the customer not knowing, the provider will make sure that the customer's data is defended against any lawful access to the extent possible.

I note that gag orders are usually limited in time, i.e. customers will sooner or later learn of the effort of an authority to access customer data.

25. **Some Swiss data protection authorities argue that it is not possible to assess the probability of a lawful access!**

Footnote 11 in the most recent guideline on "cloud-specific risks and measures" of *Privatim*, the association of Swiss data protection authorities, states the following (translated): [26]

> *"If authorities can access data without informing the responsible public body, the probability of occurrence cannot be assessed (because it cannot be verified), so that the main focus is on the extent of the damage, where the quality of the data is particularly important (sensitive personal data)."*

This is conceptually and factually wrong:

- Lawful access can be verified. Many providers publish transparency reports on their past experience with foreign lawful access, others make public statements that they have never received lawful access requests for a particular service or group of customers, there are court decisions and statistics from authorities.
- The probability of lawful access *can* be determined because lawful access (at least in countries such as the US) is subject to clear rules and legal and technical preconditions, which can be assessed (see also Q24). It *can* be determined how probable it is that in a specific technical and organizational setup these rules

[26] Version 3 of Februar 2, 2022 (http://www.privatim.ch/wp-content/uploads/2022/02/privatim_Cloud-Merkblatt_v3_0_20220203_def._DE-1.pdf, archived at https://perma.cc/MSE3-ZA8B).

permit the authorities to access customer data. Since most providers are forced to challenge access requests, these rules will most likely be complied with, whether the provider is permitted to talk or not ("gag order"). This is exactly what my method assesses. It is probably easier to determine the probability of a foreign lawful access being successful than whether a cybercriminal will be successful in stealing data from a computer system.

- Whether personal data is "sensitive" personal data (e.g., health data) or not is irrelevant in the context of foreign lawful access scenario. What counts are the negative effects of such lawful access to the data subject. In the case of the US CLOUD Act, the negative effect does not depend on whether the data is sensitive or not, it depends on whether and how come the data is relevant for the criminal prosecution and can be used against the data subject as evidence of a crime.

A similar view has been published by David Vasella in his blog.[27] Likewise, the Canton of Zurich has on purpose not distinguished between normal and "sensitive" personal data in its risk assessment, but whether the data at issue has been collected using government powers or not.[28]

Note: Q33 discusses on whether we can rely on foreign authorities complying with the law.

### 26. Doesn't the calculated probability increase the more transfers we make or the more data we process?

No, it does not.

Some believe that the probability calculated indicates the share of transfers that will be subject foreign lawful access. If the probability of a foreign lawful access is 2%, they argue that it will take 50 transfers to reach 100%, meaning that one out of 50 transfers will statistically be subject to foreign lawful access (2 x 50 = 100).

This is wrong. The probability of lawful access does not depend on the number of transfers (nor on the volume of data transferred).[29] The reason is different depending on the type of lawful access (see Q28 for an overview of these types):

- **Targeted Access:** In the case of targeted access (such as under the US CLOUD Act) the probability of a foreign lawful access will increase or decrease depending on whether the data at issue is

---

27 https://datenrecht.ch/privatim-merkblatt-cloud-spezifische-risiken-und-massnahmen-neue-fassung-und-kritische-anmerkungen/ archived at https://perma.cc/BY98-V44D.

28 https://www.zh.ch/bin/zhweb/publish/regierungsratsbeschluss-unterlagen./2022/542/RRB-2022-0542.pdf, archived at https://perma.cc/Y4K8-ZCDN.

29 Apparently, the Danish data protection authority fell into this "trap" with its decision of July 2022 (Case 2020-431-0061).

relevant for investigational proceedings of a particular kind because the lawful access is always triggered by a specific investigation (e.g., a US authority investigates a serious crime and believes that a particular US cloud provider has evidence relevant to such crime). Accordingly, the probability that the customer data of a Swiss school becoming the target of a lawful access under the US CLOUD Act is considerably lower than the customer data of a Swiss bank. Therefore, my method takes into account the number of cases in which a foreign authority will be interested in accessing the data of the particular customer of the provider (regardless of the channel through which it would access it) (see Q16). Whether this customer undertakes one transfer or 100 transfers does not make a difference; the chances of the data being accessed will not increase just because there are more transfers to the US. Nor will it increase with an increased volume of data.[30] Likewise, the probability will not increase just because the same provider has 10'000 other customers or only 100.

- **Mass-surveillance:** Here, the probability does not increase or decrease because it is not assessed on the basis of the number or transfers or volume of data. Rather, it is calculated on the basis of other factors such as the type of customers of a provider (e.g., a school, a municipality, a retailer, a bank), the type of the service (e.g., HR management, CRM, social media) and relevant circumstances of the transfer (e.g., whether the customer directly contracts with a US-based provider or instead uses its European subsidiary, whether it uses in-transit encryption or not). If one customer assesses a probability of 1 percent, this applies to all customers with the same "risk profile". It indicates how probable it is that this kind of customer of the provider using this kind of service in the specific manner at issue will be subject to lawful access, not this particular customer. Whether the provider has 5 or 5'000 customers does not make a difference. The reason is that providers are not asked to perform mass-surveillance randomly (e.g., pick one e-mail out of every 1'000), they perform it systematically. They either scan *every* communication or they scan none. If they scan every communication, the next question is whether you or your communications is on the search list or not. If you are on the list, then *all* your communication (with that service) will be collected, otherwise none will be collected. When you do a risk assessment, you try to assess the probability with regard to both aspects.

---

30 Of course, an increased volume of data will increase the chance that the provider will be able to find the piece of information that the authority is looking for. This aspect, however, is already covered in the assessment itself (when evaluating the technical ability not search the data). In addition to this, it is always assumed that the in case of a targeted lawful access of customer data that the customer data does include the information sought. The method assesses the probability that it can be located.

The probability of a lawful access to occur can increase from a statistical point of view and in reality depending on other factors. See Q9 and Q10 for more.

### 27. How can the probability be so low even in cases where the US provider technically could access my data in plain text?

Check at the specific assessment to find out why. Every assessment is different. Look at the factors that contributed to the overall result to understand the assessment and look at the reasoning that has been given. The method neither guarantees low numbers nor was it designed to produce low numbers.

Low numbers are typically the result of effective countermeasures (or "supplemental measures", as the European Data Protection Board refers to them, see Q3).

Contrary to common belief, it is *not* sufficient under US law to assess whether a US-based provider is an "Electronic Communications Service Provider" and, thus, in principle is subject to Section 702 FISA. This is the beginning, not the end of the analysis. There are additional conditions that need to be fulfilled for such provider being required to hand over customer data to the US intelligence authorities (for Section 702, see Q29, for "possession, custody or control" see Q35 and Q36, and for "international comity" see Q37). Whether these additional conditions are fulfilled largely depends on the measures undertaken.

My method allows the assessment of *all* such measures and circumstances (see Q2).

## D. QUESTIONS ABOUT FOREIGN LAWFUL ACCESS

### 28. What forms of foreign lawful access do exist and are covered by the method?

The law of every country provides for different forms of lawful access. Some jurisdictions have a wider variety of access types than others, and some jurisdictions give their authorities broad powers with their laws being very vague (e.g., China, Russia) while others more precisely regulate what their authorities can do (e.g., the US).

The four basic types are:

- **One-time targeted access:** This access type is used when an authority is investigating a particular case and wants to access specific information or documents of a particular target. This can involve intercepting certain phone and Internet connections, but also seizing data on a computer or documents during a search. This type of lawful access is a usually one-time event, triggered by a specific investigation. Of course, in the case of the intercep-

tion of a phone line, it will span over a certain period of time, but it will involve only the defined phone "number".

The Stored Communications Act (**SCA**) and the US CLOUD Act (which clarified the territorial reach of the SCA) falls in this category: It permits US authorities investigating a serious crime to require a US cloud provider to turn over specifically defined data of a customer for investigating the case, and provider has to comply irrespective of whether the data is stored in or outside the US – provided the data is in "possession, custody or control" of the provider (see Q31). This corresponds to Art. 18(1) of the Cybercrime Convention of the European Council. Swiss prosecutors can do the same, including requiring providers to produce data that is stored outside of Switzerland. The SCA and US CLOUD Act only have to be considered for the purposes of professional and official secrecy, but not for simple cross-border data transfers under the GDPR or the Swiss DPA (Q31). This is also why "Schrems II" assessments do not address the risk of data access under the SCA and US CLOUD Act; these laws are not considered "problematic" from a GDPR point of view because all EU countries have similar laws.

- **Signals intelligence:** This access type involves national intelligence authorities systematically and on ongoing basis intercepting telecommunications in the hope of running into communications relevant for national security purposes. Data is typically accessed "in-transit".

  Section 702 FISA and Executive Order (EO) 12333 are the provisions of US law that authorize the NSA to perform signals intelligence by tapping into Internet backbone traffic, phone networks, etc. inside and outside the US. In the US, this is also referred to as "upstream" surveillance. For cloud projects and international data transfers, signals intelligence is usually not an issue of practical relevance as it can be prevented by encrypting data transfers in-transit, which – at least in Europe – is standard practice and provides solid protection. See Q29 for more details on Section 702 FISA and EO 12333. Many European countries, including Switzerland, also undertake signals intelligence.

- **At-rest mass-surveillance:** This access type involves intelligence authorities systematically collecting communications and other data from customer accounts operated by communication providers in their territory. This type of lawful access is usually a continuous surveillance.

  Section 702 FISA is the provision of US law that permits the NSA to require US communication providers under certain conditions to search their customer accounts for certain identifiers of targets (e.g., email addresses, phone numbers and other identifiers) and

have the hits turned over to the authority. This mass surveillance typically occurs with data "at-rest" and is referred to as "downstream" surveillance in the US (see Q29 for a detailed explanation on how Section 702 FISA works). As with signals intelligence, this is not a targeted lawful access, but rather a fishing expedition: The authority hopes that at least some of the accounts belong to the targets (e.g., terrorist suspects) they are looking for. The contents and metadata of these accounts are then reviewed for relevance for national security purposes (e.g., terrorism, weapons proliferation).

- **Self-declaration:** Some countries require providers to self-report information about their customers that could be of relevance for national security (e.g., China). This is a form of indirect lawful access, which is why it is often overlooked in practice.

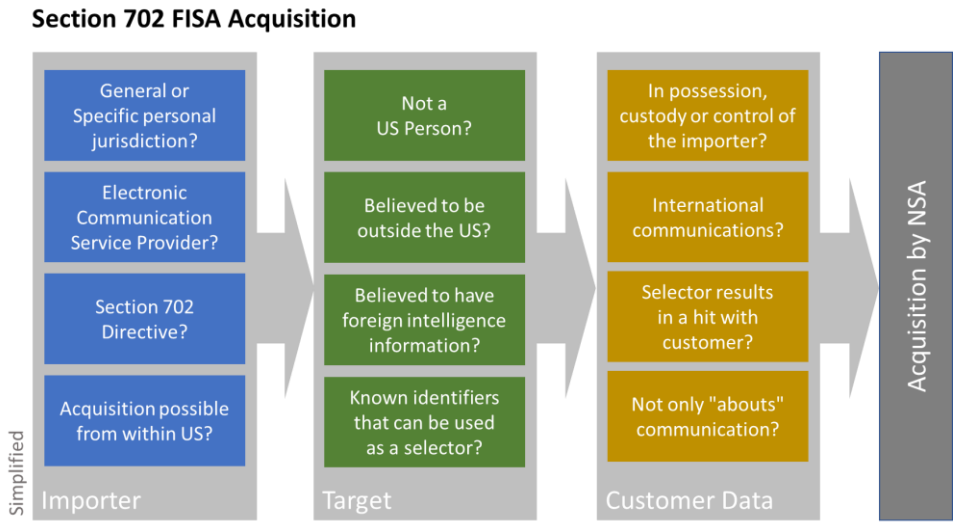
I have created various assessment forms to deal with different types of lawful access because not all forms of lawful access are relevant in all cases and countries (see Q12 and Q6).

Also, the probability of a targeted access happening must be calculated in a different manner than at-rest mass-surveillance because of the nature of the lawful access.

For instance, the probability that a particular implementation of a service of a cloud provider is subject to mass-surveillance, remains the same for each and any customer of a particular service, whether one or hundred customers use such service or whether they use it once or all the time during the assessment period (see Q26 on why the probability does not increase).

### 29. How does lawful access under Section 702 FISA and EO 12333 work and what limitations apply pursuant to US law?

In practice, it is primarily Section 702 FISA that is relevant for the present purposes, which is why I will discuss Section 702 first. EO 12333 is discussed at the end of this answer, as well as further instructions as how to assess the probability of these forms of lawful access to apply.




Please note that I will in the following only discuss those aspects of Section 702 FISA and EO 12333 that are relevant for assessing the risk of foreign lawful access.

### Section 702 FISA

The Foreign Intelligence Surveillance Act of 1978 (**FISA**) is a US law that permits certain US authorities to gather and use foreign intelligence information.[31] It also provides for the Foreign Intelligence Surveillance Court (**FISC**) to, alongside other institutions, oversee such activities. FISA concerns electronic surveillance, but also physical searches, pen registers and trap and trace devices, the collection of business records and various forms of collection concerning persons located outside the US.

In its "Schrems II" decision of July 16, 2020, the European Court of Justice (**CJEU**)[32] focused on what is known as "Section 702", which permits the Attorney General and the Director of National Intelligence (usually not a court[33,34]) to authorize the targeting of non-US persons who are reasonably believe to be located outside the US to acquire foreign intelligence information. The legal basis is in 50 U.S.C. § 1881a.

---

31 An official backgrounder with an easy to read overview is available under https://www.intelligence.gov/assets/documents/702%20Documents/statistical-transparency-report/2022_IC_Annual_Statistical_Transparency_Report_cy2021.pdf, archived at https://perma.cc/BL9X-2D7W.

32 Facebook Ireland / Schrems, C-311/18, para. 184 (https://curia.europa.eu/juris/liste.jsf?num=C-311/18).

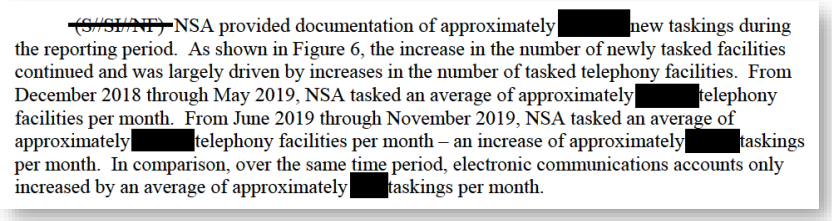
33 Some exceptions may apply, e.g., 50 U.S.C. § 1881b, § 1881c.

34 This is one of the problematic aspects of Section 702. In essence, the FISC only reviews the procedures (e.g., targeting procedures by the NSA and FBI) and compliance violations (e.g., illegal queries or targeting). See, for example, https://www.intel.gov/ic-on-the-record-database/results/1057-release-of-documents-related-to-the-2020-fisa-section-702-certifications archived at https://perma.cc/4FKM-999A. See also Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, July 2014, p. 26 et seqq. (https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf, archived at https://perma.cc/S7LU-2NRY).

For the purposes of Section 702, a US person can be an individual or a corporation.[35] The CJEU found Section 702 not to be in line with EU law requirements, in particular due to a lack of judicial oversight, data subject redress and proportionality.[36]

In order to understand why Section 702 may be a problem from a European point of view and where it affects cloud projects and other transfers to the US (and where not), it is necessary to understand how the US government gathers information under it. The following information is based on official information released by the US government in redacted form:

- Collections under Section 702 are a kind of a "fishing expedition" where the US government asks telephone, email and other electronic communication service providers (**ECSP**) located in the US to search their transmissions, phone records and customer accounts for those communications of people and companies they are looking for. Any hits are to be produced to the government.
- The names and even the number of ECSP involved in the exercise are not published by the US government. What is known from its statistics is that the number is increasing, although mainly due to additional traditional phone companies being added:[37]



~~(S//SI//NF)~~ NSA provided documentation of approximately [redacted] new taskings during the reporting period. As shown in Figure 6, the increase in the number of newly tasked facilities continued and was largely driven by increases in the number of tasked telephony facilities. From December 2018 through May 2019, NSA tasked an average of approximately [redacted] telephony facilities per month. From June 2019 through November 2019, NSA tasked an average of approximately [redacted] telephony facilities per month – an increase of approximately [redacted] taskings per month. In comparison, over the same time period, electronic communications accounts only increased by an average of approximately [redacted] taskings per month.

Because several providers have published their own "transparency" reports indicating that they have received FISA orders in the past, NOYB.eu has published the list of the following providers they allege have received FISA orders: AT&T, Amazon, Apple, Cloudflare, Dropbox, Facebook, Google, Microsoft, Verizon Media (former Oath & Yahoo), Verizon.[38]

---

35 As defined by Title I of FISA, a U.S. person is "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in [50 U.S.C. §§ 1801(a)(1), (2), or (3)]." See 50 U.S.C. § 1801(i).

36 CJEU Decision of July 16, 2020, Facebook Ireland / Schrems, C-311/18, para. 178 et seqq. (https://curia.europa.eu/juris/liste.jsf?num=C-311/18).

37 See 23rd Joint Assessment of Section 702 Compliance of the Office of the DNI, September 2021, p. 22 (https://www.intel.gov/assets/documents/702%20Documents/declassified/23rd_Joint_Assessment_of_FISA_for_Public_Release.pdf, archived at https://perma.cc/34EZ-GK2R).

38 https://noyb.eu/en/next-steps-eu-companies-faqs, archived at https://perma.cc/8L27-AW2A.

- The definition of ECSP is rather broad: It includes telecom carriers, email providers, cloud service providers, internet service providers and "any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored" (50.U.S.C. § 1881(b)(4)).[39] The definition is so broad that it even includes companies providing email services to their own employees, which, however, is neither how Section 702 was intended nor is applied. For the purposes of Section 702 an ECSP is a company providing communication services *to others*.[40] Furthermore, based on the targeting limitations (see below), ECSP can only be compelled to collect data under Section 702 insofar they enable communications outside the US.[41]
- The US government authorities involved and entitled to request the collection of information and query are the National Security Agency (**NSA**), the Federal Bureau of Investigation (**FBI**), the Central Intelligence Agency (**CIA**) and the National Counterterrorism Center (**NCTC**). The actual collection from the ECSP is performed by the NSA, who then provides the other authorities with access to the acquired "raw" data.[42] Such access is referred to as "querying".
- Here, I only discuss the *acquisition* of data by the US government. It would already be a violation of EEA/Swiss data protection law as well as professional or official secrecy obligations if an acquisition of personal or secret data were to take place, regardless of the US government's measures that further limit the use of such information.[43] Such subsequent querying and use of data by the NSA, FBI, CIA and NCTC only makes things "worse" from a privacy/secrecy point of view. Hence, cloud projects and other transfers are only permitted if there is no reason to believe that

---

39 Stephen I. Vladeck, Expert Opinion on the Current State of U.S. Surveillance Law and Authorities, November 15, 2021, p. 3, with further references (https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf, archived at https://perma.cc/3XPA-Q9B4).

40 Alan Charles Raul, Schrems II Concerns Regarding U.S. National Security Surveillance Do not Apply to Most Companies Transferring Personal Data to the U.S. Under Standard Contractual Clauses, December 23, 2020 (revised), p. 7 et seqq. (https://datamatters.sidley.com/wp-content/uploads/2020/12/Raul-Schrems-II-Concerns-Regarding-U.S.-National-Security-Surveillance-Do-Not-Apply-REVISED-12.23.20.pdf, archived at https://perma.cc/LH8P-YSWD, with a shorter version available at https://www.lawfareblog.com/why-schrems-ii-might-not-be-problem-eu-us-data-transfers, archived at https://perma.cc/L5Y5-2P9T); Vladeck (footnote 39), p. 4 et seq., which takes a more theoretical approach.

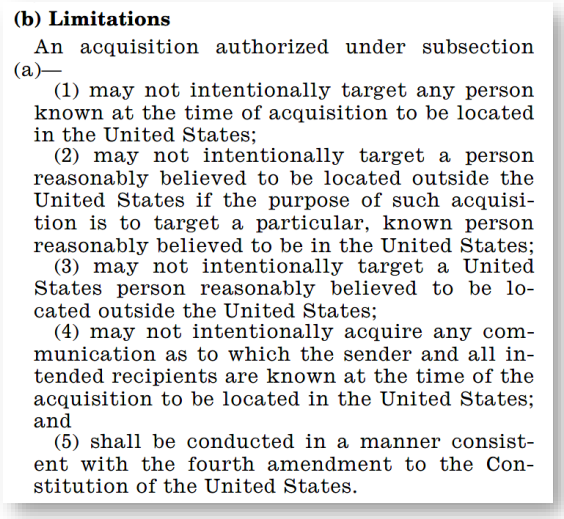
41 Ibid.

42 FISC November 2020 Opinion, p. 14 (https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_FISC%20Cert%20Opinion_10.19.2020.pdf, archived at https://perma.cc/EW5J-MFBS).

43 It is subject to special procedures, including procedures to "minimize" the collected information prior to its further use by the US government. Each authority has its own such procedures. For 2020, they are available here: https://www.intel.gov/ic-on-the-record-database/results/1057-release-of-documents-related-to-the-2020-fisa-section-702-certifications, archived at https://perma.cc/4FKM-999A.

an acquisition (or collection) of data takes place by the US government in the first place.

- Under Section 702, the US government does not collect each and any Internet traffic or account data that is transmitted or otherwise processed by ECSP, i.e. there is no "bulk" acquisition. It rather requires the participating ECSP to search for information related to specific persons, commonly referred to as the "targets".
- These targets can be individuals or companies of national security interest to the US government. The NSA procedures require that any decision to target a particular person shows that it is "expected to possess, receive, and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory authorized for targeting", which has to be supported by a "particularized and fact-based" assessment.[44]
- More importantly, under Section 702, the targets may only be (i) non-US persons[45] (ii) who are reasonably believed to be located outside the US. Specifically, 50 U.S.C. § 1881a provides:



**(b) Limitations**

An acquisition authorized under subsection (a)—

(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;

(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and

(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

To comply with this requirement, each US authority follows its own "targeting" procedures.[46]

- In 2020, there were some 232'432 targets under Section 702.[47]

---

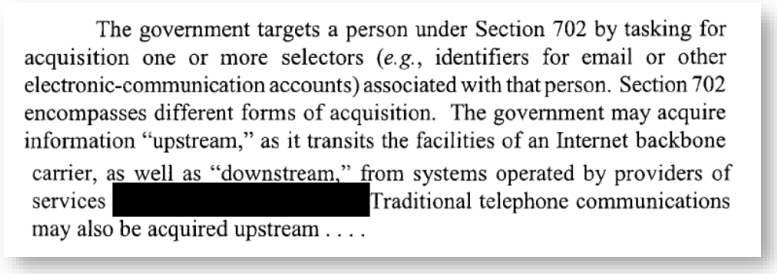
44 NSA 2020 § 702 Targeting Procedures court stamped October 19, 2020, p. 4 (https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_NSA%20Targeting%20Procedures_10.19.2020.pdf, archived at https://perma.cc/V793-7Z4P).

45 With limited exceptions for those considered to be an agent or employee of a foreign power (59 U.S.C. §1881b, §1881c).

46 The 2020 targeting procedures (NSA, FBI) are available here: https://www.intel.gov/ic-on-the-record-database/results/1057-release-of-documents-related-to-the-2020-fisa-section-702-certifications, archived at https://perma.cc/4FKM-999A.

47 Office of the DNI, Annual Intelligence Community Transparency Report for Calendar Year 2021, April 2022, p. 4, https://intelligence.gov/assets/documents/702%20Documents/statistical-transparency-

- For each such target, the US government determines one or several "selectors", which are phone numbers, email addresses and other identifiers "used" by the targets in their communications or for their accounts.[48] Terms like "bomb" or "terror attack" or names likes "Osama Bin Laden" cannot be selectors because they do not relate to a target or are not an identifier that can be used to identify communications to or from such target (or their accounts). These selectors are given to the ECSP, which will then use them to search the relevant data under their possession, custody or control[49], which can be either (i) the traffic they transmit for customers across their networks (known as "upstream" surveillance) or (ii) customer data at-rest (e.g., email accounts of customers, known as "downstream" surveillance). In each case, the purpose of the search is to identify the target's calls, other transmissions or accounts and collect the (raw) contents of communication (including metadata, which is often also referred to as "non-content"):[50]



The government targets a person under Section 702 by tasking for acquisition one or more selectors (*e.g.*, identifiers for email or other electronic-communication accounts) associated with that person. Section 702 encompasses different forms of acquisition. The government may acquire information "upstream," as it transits the facilities of an Internet backbone carrier, as well as "downstream," from systems operated by providers of services [redacted] Traditional telephone communications may also be acquired upstream . . . .

- The "contents" of communication may both be the actual content (e.g., what people say in a call or include in an email) but also metadata of such communication (e.g., caller or called ID, email sender, recipient and date/time, IP addresses); the term includes "any information concerning the substance, purport, or meaning of that communication."[51]
- Since the selectors with which an ECSP is tasked by the NSA are limited to communications identifiers, it only has to search for communications or accounts that would use such terms *as identi-*

---

report/2022_IC_Annual_Statistical_Transparency_Report_cy2021.pdf, archived at https://perma.cc/BL9X-2D7W.

48 Office of the DNI, Annual Intelligence Community Transparency Report for Calendar Year 2021, April 2022, p. 13 and p. 17, https://intelligence.gov/assets/documents/702%20Documents/statistical-transparency-report/2022_IC_Annual_Statistical_Transparency_Report_cy2021.pdf, archived at https://perma.cc/BL9X-2D7W.

49 See below, including footnote 54.

50 FISC November 2020 Opinion, p. 7 et seq. (https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_FISC%20Cert%20Opinion_10.19.2020.pdf, archived at https://perma.cc/EW5J-MFBS).

51 Stephen I. Vladeck, Expert Opinion on the Current State of U.S. Surveillance Law and Authorities, November 15, 2021, p. 2, with further references (https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf, archived at https://perma.cc/3XPA-Q9B4).

*fiers*. Although the wording of Section 702 is pretty vague and, at least on the face of it, permits broader search tasks, this is not how Section 702 is applied in practice according to the documented procedures and oversight documents. For instance, the ECSP does not have to search actual contents of non-target communications for hits (see the discussion below concerning "about" communications).

- The raw communication contents of a target so identified in the communications transmitted or stored by the ECSP and subsequently collected by the ECSP are then provided to the NSA for further processing, use and dissemination to other authorities. As opposed to the ECSP, the NSA and the other authorities may search the actual contents of the communications of a target that has been collected. I do not further discuss this here for the reasons explained above.
- An ECSP is required to provide the government "all information, facilities, or assistance" necessary to accomplish the acquisition of communications of a target.[52] Yet, there seems to be a consensus that an ECSP is neither required to build "backdoors" into its systems nor to disclose its (own) decryption keys.[53] This is only half of the truth, though: If the ECSP itself has access to a target's contents of communications in plain text, there is no need to turn over a decryption key in the first place (it will simply provide the government with the contents in a decrypted form). This leads to real question as to whether the ECSP can "access" the target's contents in plaint text and what steps the ECSP has to do to accomplish so. The test applied in national security contexts as well as in civil and criminal procedure law is usually whether the information sought is in the ECSP's "possession, custody or control".[54] If customer data is in the possession, custody or control of an ECSP only in encrypted form, it has to be produced only in that particular form. This also applies to decryption keys: If a target retains decryption keys in a key vault to which the ECSP could theoretically gain access but is not considered having possession, custody or control of it, then the ECSP will not have to turn it over by "hacking" into the key vault or otherwise gaining such access.
- A good way to get comfort that a US-based provider has in the past not been required to produce information under Section 702

---

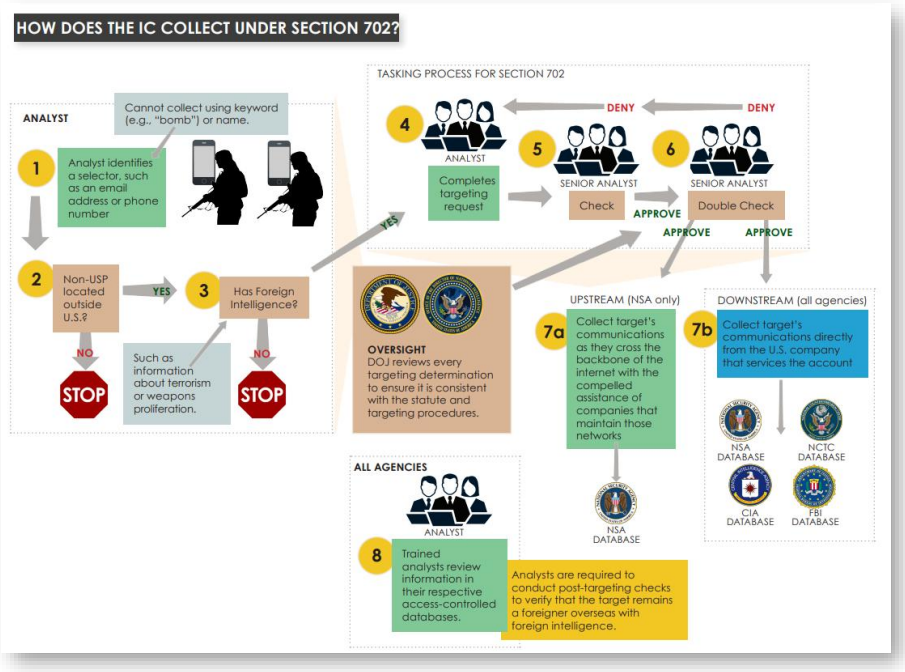
52 50 U.S.C. §1881a(i)(1)(A).

53 For instance, Microsoft, in its Data Protection Addendum of September 2021, expressly states that it will not provide any third party "platform encryption keys used to secure Processed Data or the ability to break such encryption".

54 See Q35 for a discussion of what "possession, custody or control" means. For case law, see, e.g., Fed.R.Civ.P. 34 and 45(a); Fed.R.Crim.P. 17; Flame S.A. v, Industrial Carriers, Inc., 39 F. Supp. 3d 752, 759 (E.D. Va 2014); Asset Value Fund, Ltd. v. The Care Group, Inc., No. 97 Civ. 1487, 1997 WL 706320, at *9 (S.D.N.Y. Nov.12, 1997).

is to get confirmation that it has *not* yet received "Section 702 directive".[55] ECSP are not prohibited from saying so. A Section 702 directive is a legal precondition for being "tasked" to search traffic or accounts for certain selectors. Usually, if the NSA foresees that a particular ECSP could be relevant for searching for particular targets, it will send the ECSP such a directive. Many cloud providers, including at least one major hyperscaler, claim not yet having received one. The other possibility to get a better understanding of whether a particular provider is involved in Section 702 collections is to study the provider's "transparency" reports.[56] These reports can be misleading, though: They usually do not distinguish between different types of services and they often make no clear statements about how often the provider has been tasked with searching for certain targets ("0-499"). For example, it is well possible that a particular ECSP has been regularly tasked for searching accounts of consumer customers, but never accounts of corporate customers. See also Q15 regarding transparency reports and how to find them.

In the following chart, the US government summarizes the overall collection process under Section 702:[57]




55 Privacy and Civil Liberties Oversight Board (footnote 33), p. 32 et seqq., p. 46.

56 See also the list of providers that have provided reports referring to FISA according to NOYB.eu: https://noyb.eu/en/next-steps-eu-companies-faqs, archived at https://perma.cc/8L27-AW2A.

57 See https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf (archived at https://perma.cc/8XGM-6EZT), p. 4, from the Office of the Director of National Intelligence.

The foregoing makes clear why this kind of gathering of intelligence information is referred to as "mass surveillance": While the US government under Section 702 does not acquire bulk traffic or account data of ECSP, it asks the ECSP to search such bulk traffic and account data for the information it is looking for. This means that personal data of anybody communicating over the network or using the online services at issue can become subject to this form of lawful access. This is different in the case of targeted lawful access, such as under the US CLOUD Act and Stored Communications Act, where a law enforcement authority will specifically request from a provider the account information of one particular customer; other customers or accounts are not affected.

Note that most or all European countries perform mass surveillance in one form or another, at least with regard to foreign communications. The issue with Section 702 is that it does not provide some guarantees to data subjects that corresponding provisions in EEA/Swiss law do. For example, the US government considers the "Fourth Amendment" protections referred to in 50 U.S.C. § 1881a not protecting the privacy of non-US persons outside the US.[58] Note that improvements of such protections are under discussion, some forms of legal redress is already available[59] and the 2014 Presidential Policy Directive (PPD-28)[60] directs US intelligence authorities to respect the privacy rights of foreign citizens (which the CJEU in "Schrems II" did not consider sufficient because it was a mere executive order).

In order to assess the relevance for a particular cloud project or other transfer of data to the US, it is necessary to look more closely to the practices of the NSA in requiring ECSP to search and collect data for the governments acquisition under Section 702.

To begin with, the following three statements in the documents released by the NSA provide more insight:

- The NSA holds that "[a]cquisitions conducted under these procedures will not intentionally acquire communications that contain a reference to, but are not to or from, a person targeted in accordance with these procedures."[61] This is also provided for by 50 U.S.C. §1881b(b)(5).

---

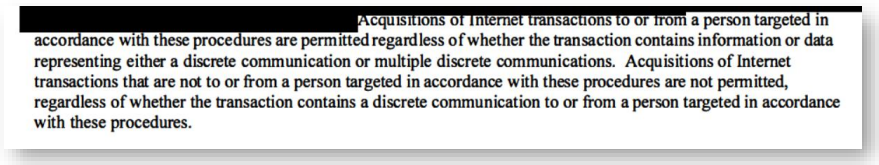
58 See FISC November 2020 Opinion, p. 32, with further references (https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_FISC%20Cert%20Opinion_10.19.2020.pdf, archived at https://perma.cc/EW5J-MFBS).

59 Vladeck (footnote 39), p. 17.

60 https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities, archived at https://perma.cc/NV2G-WNCG.

61 NSA 2020 § 702 Targeting Procedures court stamped October 19, 2020, p. 2 (https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_NSA%20Targeting%20Procedures_10.19.2020.pdf, archived at https://perma.cc/V793-7Z4P).

- When NSA proposes to direct surveillance at a target, "it does so because NSA has already learned something about the target or the facility or facilities the target uses to communicate."[62]
- In a footnote, the NSA clarifies that "[a]cquisitions of Internet transactions to or from a person targeted in accordance with these procedures are permitted regardless of whether the transaction contains information or data representing either a discrete communication or multiple discrete communications.[63] Acquisitions of Internet transactions that are not to or from a person targeted in accordance with these procedures are not permitted, regardless of whether the transaction contains a discrete communication to or from a person targeted in accordance with these procedures."[64]


[redacted] Acquisitions of Internet transactions to or from a person targeted in accordance with these procedures are permitted regardless of whether the transaction contains information or data representing either a discrete communication or multiple discrete communications. Acquisitions of Internet transactions that are not to or from a person targeted in accordance with these procedures are not permitted, regardless of whether the transaction contains a discrete communication to or from a person targeted in accordance with these procedures.

The term "Internet transactions" refers to any communication over the Internet (as it would be collected in-transit) whether as an email or supposedly in any other form (e.g., video streams, voice-over-IP-phone calls, application data transmissions).[65]

This shows that in practice, ECSP are not required to search *nested* Internet communications (also referred to as "abouts" communications[66]), as long as such communication does not belong to the account of a target. Hence, if a party in Europe (that is no target) transfers data to a party in the US (that cannot be a target because it is a US person) and such communication happens to include communications or other content about the target, then such communication will not intentionally be acquired according to the rules (and, thus, does not have to be searched for).

---

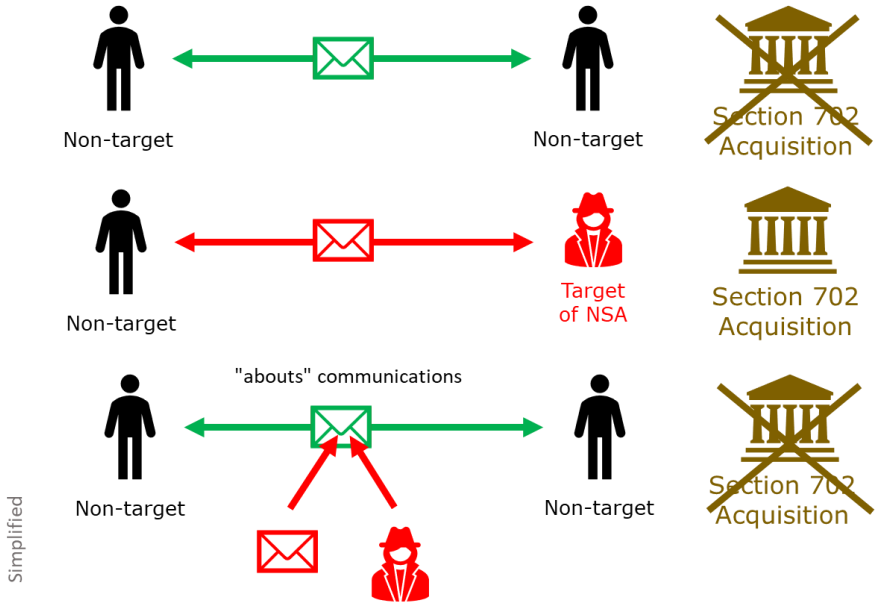
62 Ibid.

63 This relates to a communication that consists of several discrete communications that is sent over the Internet in "one package"; in such case, the entire communication will be collected, if one of the discrete communications is to or from a target.

64 Ibid., footnote 1.

65 Ibid.

66 50 USC § 1881a(m)(4)(B)(i) ("The term 'abouts communication' means a communication that contains a reference to, but is not to or from, a target of an acquisition authorized […]").




This was not always the case. In 2014, the Privacy and Civil Liberties Oversight Board (**PCLOB**)[67] issued a report that criticized the NSA for collecting "abouts" communications and recommended reviewing the technical possibilities to exclude such communications from collection;[68] this was implemented.[69] The topic of "abouts" communications has repeatedly been the topic of discussions.[70]

The NSA does not disclose the type of communications that is searched for (except for radio signals, emails and phone calls) nor the type of ECSP required to apply the selectors. However, in view of the nature of the selectors (which always have to be associated with a target) and the aforementioned statements (referring to a communication, i.e. an exchange of information between a sender and a recipient) acquisitions under Section 702 are about information that can either be linked to (i) a known account maintained by the ECSP for sending or storing communications[71] (identified by an account identifier) or (ii) to a known sender or recipient of a transmission of data (a phone number, an IP address, email address, a messenger address). This significantly reduces the reach of Section 702 in practice – most corporate applications (HR, CRM, ERP, etc.) will be out of scope.

Based on the available statistics, while it is not clear whether the quantity of information obtained through Section 702 has actually increased, it is noteworthy that the increase in ECSP involved is mainly because of an increased interest in telephony services, not electronic

67 https://www.pclob.gov/Oversight.

68 Privacy and Civil Liberties Oversight Board (footnote 33), p. 143.

69 https://documents.pclob.gov/prod/Documents/OversightReport/b1accb9f-0469-46f1-b660-b66acfbc601a/Recommendations_Assessment_Report_20160205.pdf, archived at https://perma.cc/9BKR-D3GQ.

70 See, e.g., https://www.law.cornell.edu/uscode/text/50/1881a at the end.

71 E.g., an email, messenger or conferencing service.

communications accounts (see above). This is no surprise, though: Due to the increasing use of effective end-to-end encryption, surveillance of Internet and other electronic communications is becoming increasingly difficult. In-transit encryption, which successfully prevents signals intelligence on Internet backbones, is already standard in the western world, which is why the intelligence community focuses on communications to and from areas of the world where encryption is regulated or even prohibited. Communications through phone calls is less affected. It can be assumed that a large number of the selectors in use are phone numbers (as opposed to Internet addresses and identifiers).

There is a further element to be considered in the case of US-based cloud providers and data transfers to the US, which is the prohibition to intentionally target US persons.[72] In fact, in practice, the US government has to show that a particular target is "reasonably believed" to be a non-US person (referred to as the "foreignness determination").[73] Section 702 also prohibits targeting any communication where the sender and recipient (whether or not being a US person) is in the US. Yet, the statutory limitations of Section 702 acquisitions (see above) only prohibit *targeting* communications of a US person or domestic communications, but they do not prohibit acquiring it incidentally. This can happen because the US person is a participant in communications of a target or because a target's communications is about the US person.

Based on this, an initial set of conclusions can be drawn:

- **Use Case 1:** If a US company receives an Internet transmission (email, call, data transfer, remote access connection, etc.) from a company or individual in Europe and stores it using the system of an ECSP (e.g., its own US-based cloud provider), then such data will not be collected at-rest: Any selectors would not apply because the ECSP is not providing any service to the sender and has, thus, no matching account. The ECSP would also not be required to disclose the contents at-rest of the account of the recipient (i.e. the US company), because it would not match a selector (assuming that the NSA has not issued a selector referring to the identifiers used by the US company, which would be prohibited because the NSA may not intentionally target a US person). Hence, any downstream acquisition is out of scope. However, the ECSP involved in the transmission of the message over the Internet may have to collect and produce it (in the form they collect it, which may be encrypted or unencrypted) if the selectors included

---

72 With limited exceptions for those considered to be an agent or employee of a foreign power (59 U.S.C. §1881b, §1881c).

73 See FISC November 2020 Opinion, p. 8, with further references (https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_FISC%20Cert%20Opinion_10.19.2020.pdf, archived at https://perma.cc/EW5J-MFBS).

the address used by the sender. If the sender and recipient used strong encryption (as is standard with today's mail servers in the US and (western) Europe, their message would not be accessible in plain text.

- **Use Case 2:** If a US company onward transfers the content of the Internet transmission (that includes a communication from a sender being a target, with such sender not being a participant of their communications) to another recipient in the US, then such transfer would again not be subject to Section 702. The sender and the recipient of the onward transfer would be located in the US and most likely both would be US persons. The transfer as such could, therefore, not be targeted, meaning that – if the NSA has worked properly – there should be no selectors that search for accounts or communications of the sender and recipient at issue; whether they communicate about a target is not relevant for the reasons explained above. Under the targeting procedures discussed above, the NSA would not be permitted to have their Internet transmissions collected based on communications contained *therein*, as this would form part of an "Internet transaction … not to or from a person targeted", which may not be acquired. Moreover, the NSA is not permitted to gather purely domestic traffic.
- **Use Case 3:** If an ECSP in the US receives an Internet transmission from a company in Europe that itself is not a target, but processes communication of a target, then such transmission would, again, not be subject to Section 702. Under the targeting procedures discussed above, the transmission received from the company in Europe would have to be considered an "Internet transaction … not to or from a person targeted", which may not be collected according to the above rules; consequently, any communications contained therein will not be collected, either (it would also be considered "abouts" communication by two non-targets, which are the ECSP and the company in Europe). Moreover, the ECSP in the US would not have to produce the transmission as part of any downstream (i.e. data at-rest) acquisition. If the ECSP were providing a communication service to the company in Europe (which is not a target), the selectors would not apply (assuming the NSA defined them appropriately). If the ECSP were not providing a communication service to the company in Europe but processing the transmission for its own purposes, then Section 702 would not apply with regard to producing the contents of its own account because this would entail targeting a US person.

Alan Charles Raul, partner at Sidley Austin, Former Vice Chairman of the Privacy and Civil Liberties Oversight Board (a group that monitors the US government's compliance including with Section 702) and Former Associate Counsel to the President, goes even a step further and

argues that typically all transfers under the EU SCC from Europe to a company in the US are "quintessentially U.S. person to U.S. person communications involving one person that is necessarily located in the U.S." and are, thus, excluded from acquisitions under Section 702.[74] He even recommends informing the US intelligence authorities of this circumstance to make it impossible for them to overlook this during their due diligence procedures required for determining targets.[75] It seems, though, that his conclusion is based on the assumption that the exporter is also considered a US person, which may be true only in certain cases, for example in the case of European subsidiaries controlled by US corporations.[76] As opposed to the definition of "US person" in other laws and regulations (e.g., the RICO Act, 15 CFR § 760.1), the definition of US person in FISA does not include such foreign subsidiaries. Yet, as the aforementioned Use Cases show, the targeting restrictions already exempt a significant portion of the cases from Section 702 acquisitions even where an ECSP in the US is involved on the part of the importer.

Raul also points to another important aspect concerning cloud providers. They are typically considered "Remote Computing Services" (RCS) under the Stored Communications Act and are therefore also ECSP under FISA. Whereas Stephen I. Vladeck, an expert mandated by German data protection authorities to produce an opinion on US lawful access laws, based on the wording of Section 702 believes that it is "not mattering" to which extent an ECSP is actually acting in its capacity as an ECSP to become subject to Section 702 production requests,[77] Raul takes a more differentiating view. He notes that where RCS are providing "processing" services in addition to cloud storage (which is most often the case), it is possible that they are considered the intended recipient of the communications and not merely a communication or storage conduit.[78] If they are the intended recipient of the communications, one may argue that these communications are again out of scope, because they would be considered the ECSP's *own* communications (and not third-party communications enabled by the provider, which is what Section 702 is all about).[79] A US-based ECSP's own communications would rather be subject to other forms of lawful ac-

---

74 Raul (footnote 40), p. 10 et seq.

75 See his blog post under https://www.sidley.com/-/media/publications/raul-law360transferring-eu-data-to-us-after-new-contractual-safeguards.pdf?la=en, archived at https://perma.cc/RB6R-VVUB; see also Raul (footnote 40), p. 12 et seqq.

76 Raul (footnote 40), p. 11, referring also to the FISA definition which also covers unincorporated associations of which a substantial number of members are citizens of the United States or aliens lawfully admitted for permanent residence, which he believes may also apply to foreign affiliates of US corporations because the NSA applies it also to US branches of non-US corporations.

77 Vladeck (footnote 39), p. 5.

78 Raul (footnote 40), p. 7, footnote 18.

79 Raul (footnote 40), p. 7 et seqq., with further references, arguing that Section 702 only apply in practice insofar a company that qualifies as a ECSP is "in the business of providing communication services (rather than essentially just using communication services)".

cess not relevant here. Moreover, requiring a US person to produce its *own* communications *under Section 702* may also be considered a violation of the Fourth Amendment (protection from unreasonable searches and seizures by the government), to which the Section 702 limitations expressly refer to; the Fourth Amendment also protects US businesses, not only individuals.[80] To this end, one may note that according to Vladeck, European subsidiaries are considered to be part of their US-based ECSP for the purposes of Section 702,[81] which – if true[82] – would mean that the communications between a US-based ECSP and its European subsidiary should be considered *own* communications of a US person and, thus, be exempted from collection under Section 702 pursuant to the foregoing principles. To that end, see Q32 whether Section 702 can be enforced against European subsidiaries of a US-based ECSP, and whether they are indeed considered "agents" of their US parents.

Last but not least, it could be viewed as a circumvention of the prohibition to target a US person if one were to require the US recipient of a communications to produce such communications it has received not as a mere conduit (= forwarding or storing communications) but further processing it (e.g., as part of a CRM, HR or ERP solution). This would have the same effect as directly targeting the US recipient by using the US-recipient's cloud service provider (i.e. another ECSP), which would not be permitted for downstream collections (see Use Case 1).

While these considerations have not all been tested in court, they arguably provide a basis for challenging Section 702 requests, which an ECSP is entitled (and under the EU SCC required) to do. It will in any event decrease the probability of such data being subject to foreign lawful access.

This results in additional use cases:

- **Use Case 4:** In its first case concerning "Google Analytics", the Austrian data protection authority contended that Google was technically able to link the pseudonymous IDs provided by the publisher of a website with a Google user account if the user was logged in at the same time.[83] This was factually not correct because "Signals" was turned off,[84] but even if (i) it were correct (i.e. Google could somehow link the account to the ID), (ii) Google had received a request under Section 702 (which it never

---

80 Brandon L. Garrett, The Constitutional Standing of Corporations, University of Pennsylvania Law Review, Vol. 163:95, p. 122 et seqq.

81 Vladeck (footnote 39), p. 9.

82 I believe this will often not be the case for the reasons discussed in Q32.

83 See https://www.vischer.com/en/knowledge/blog/how-to-legally-use-google-analytics-in-europe-39512/ (archived at https://perma.cc/7JJS-BHXQ) with further references.

84 Ibid.

did for Google Analytics according to Google[85]), (iii) the user had been a target, and (iv) its Google user account had been a selector provided by the NSA or FBI, Google would still not have been required under Section 702 to produce the website usage data it received under Google Analytics using the ID: *First*, because Google did not link the Google account with the ID (even though it could have done so under the above [wrong] assumption (i)), the account accessed by way of the selectors (i.e. the user's account) would not have contained the website usage data. Google would only have had to produce the account data that matches the selectors, but it is not required under Section 702 to investigate for other data that could be related to the same user. *Second*, if the publisher is not a target and Google is not a target (which we can assume), the Internet transmissions between them cannot be collected pursuant to the targeting procedures cited above, even if they happen to contain information about the target. The same applies if the ID were first transferred from the publisher to Google Ireland and only then onward transferred to Google in the US; if Google Ireland were qualified as a US person or considered to be part of Google in the US, it is even more clear that the transmission between them cannot be targeted. *Third*, if the publisher is not a target, then the contents of its Google Analytics account with Google would not be collected because there would be no selector that applies. *Fourth*, website usage data as such is not data that the NSA collects under Section 702, because it has no sender, no recipient and no content of communications (instead, it would collect the actual website usage traffic, for instance under EO 12333, see below). *Fifth*, Google US is neither transmitting nor storing communications, but is itself the intended recipient of a communications, which is the website usage data it shall use to create reports. Producing such data would mean that Google as an ECSP would have to target itself, which is out-of-scope of Section 702. Hence, even if Google were qualified as an ECSP, it would not be required under Section 702 to produce the website usage data it receives from Europe, even if the users of its customers were targets. Accordingly, the Austrian data protection authority was wrong in assuming that Section 702 would apply and could result in an acquisition of personal data.

- **Use Case 5:** The European subsidiary of a US-based cloud service provider requests its US parent to provide certain support in providing cloud services (e.g., an email server, shared drives, a CRM solution, an ERP system) to its European customers. For doing so, it provides the US-based parent constant access to its data centers located in Europe, including to customer data. The Eu-

85 https://blog.google/around-the-globe/google-europe/its-time-for-a-new-eu-us-data-transfer-framework/, archived at https://perma.cc/V8QA-79AT.

ropean customers are not targets, but they may have communications with targets (e.g., partners, suppliers, third parties). Under these circumstances, Section 702 would not result in a collection of data of such European customers:

- *First*, the US parent company, even if generally deemed an ECSP, is not acting as an ECSP, because it itself is the intended recipient of the communications, which is a request for help from its European subsidiary. It is the European subsidiary that provides a communications or communications storage service to a third party, not its parent. As discussed above, Section 702 is not used to compel companies (let alone US persons) to produce their own communications;
- *Second*, if the US parent is no target (because it is a US person) and neither is its subsidiary,[86] then the Internet transmissions between them cannot be collected pursuant to the targeting procedures cited above, even if they happen to contain information about the target ("abouts" communications);
- *Third*, the US parent is only required to search the accounts and traffic of its own users, not those of third parties (here: of its subsidiary) to which it may have access for other purposes (than providing the services of an ECSP to them);
- *Fourth*, even if the US parent were able to search the customer accounts of its European subsidiary (given that it has technical access to it), the search would not be successful, because the European customers of its subsidiary are not targets and, thus, the selectors would not create any hits. If there are no hits, there is no downstream collection of data. There is also no room for any upstream collection because the US parent is not involved in transmitting third party communications. It is merely on the receiving end of the support requests from its subsidiary;
- *Fifth*, Section 702 would also not require the US parent to collect and produce to the NSA all data to which it has access at its subsidiary's systems because the transfers of data from its European subsidiary to the US if one follows the legal theory that this would be considered a communication to a US person. According to such theory, if such data were collected in its entirety, this would effectively result in the targeting of a US person, which is prohibited under Section 702;

---

86 Which may or may not be itself be a US person, see above.

- *Sixth*, in view of the foregoing, the yield of any search would be negligible with corporate customers, even if it were possible in some rare instances. It is, therefore, highly unlikely that the US parent would receive a request from the NSA tasking it to search and collect information with regard to the customers of its European subsidiary in the first place. Based on what has become known over time, the NSA rather focusses on operators of public communications platforms that are used also from abroad (such as social media), hubs and exchanges of international telecommunications traffic and phone companies;
- Note that the above points do not yet address the territorial restrictions of Section 702 FISA that exist according to experts (see below).

- **Use Case 6:** If one applies the facts of Use Case 5 but assumes that one or several employees of a customer of the European subsidiary were a target, then the same applies as laid out for Use Case 5, except for the fourth reason. Instead, the following applies: Even if the US parent company were technically able to apply the selectors to the accounts maintained by the European for the employees of its own customers, the US parent would not act in its capacity as an ECSP and would, therefore, not be required and allowed to do so.[87] There is also no room for any upstream collection because the US parent is not involved in transmitting third party communications. It is merely on the receiving end of the support requests.
- **Use Case 7:** If one of the European customers were a target, again the same as in Use Case 6 applies.
- **Use Case 8:** A European company is a direct customer of a US provider that operates a CRM system for the company. Because it does so as a Software-as-a-Service and stores the CRM data on its systems, it would likely be considered an ECSP. However, since its customer base is highly unlikely to be targets pursuant to Section 702 (it has corporate customers who use the service to process marketing and sales information and send commercial communications) and the contents processed by it is highly unlikely to contain foreign intelligence information pursuant to Section 702 (information relevant for marketing, sales interactions and commercial communications), it is even less likely that the provider will be requested by the NSA to search its customer database for selectors. Even if one of those customers had, in its database, information about a target, such information could not

[87] This would also apply if the US parent had to treat the sub-accounts associated to the employees as accounts of their own and search *them* for selectors (in addition to the company-account itself and as such).

be collected because such collection would target a non-target and not be permitted according to the foregoing rules.

- **Use Case 9:** A European company outsources the processing of HR data to its parent company in the US. All HR data is transferred to the US using a computer system operated by the parent company for and on behalf all affiliates of the group. The US parent technically uses a US-based cloud service provider to run the computer systems used for storing and managing the HR data. The US-based cloud service provider would not be entitled to search the European HR data received in the US for the reasons explained in Use Case 1. The US headquarter itself could theoretically be considered an ECSP, because it is providing outsourcing services to its affiliates, but this kind of intra-group services are not what Section 702 is used for in practice because they do not involve international communications of third parties (see above). Moreover, HR data as such is neither communications nor likely to contain foreign intelligence information and, therefore, not in scope of Section 702. The only communications that occurs in the present context is the transfer of such data from the European company to the US parent. Even if the parent were considered an ECSP, it would not merely be serving as a conduit for communications but rather be the intended recipient of it. If the NSA attempted to collect such communications from the parent (given that its ECSP is not permitted to produce it), it would likely be considered targeting de-facto a US person (i.e. the parent) as it would require it to produce its own communications.
- **Use Case 10:** A US provider provides free email services to customers anywhere in the world. A freelance journalist in Europe uses the US-based email service for running his private email account. From time to time, the freelancer is hired by various companies for drafting press releases. Even if the journalist is not a target, it will nevertheless have to expect that the US provider has received a request from the NSA to have its user database searched for a set of selectors that concern its free email service and to turn over the contents and non-contents (i.e. metadata) of any account that results in a hit. Hence, if the freelancer is a target, its mailbox will end up with the NSA and may be queried by the NSA, the CIA, the NCTC and the FBI. If the freelancer is not a target, then his mailbox will not. If the freelancer is a US person, he will not become a target.

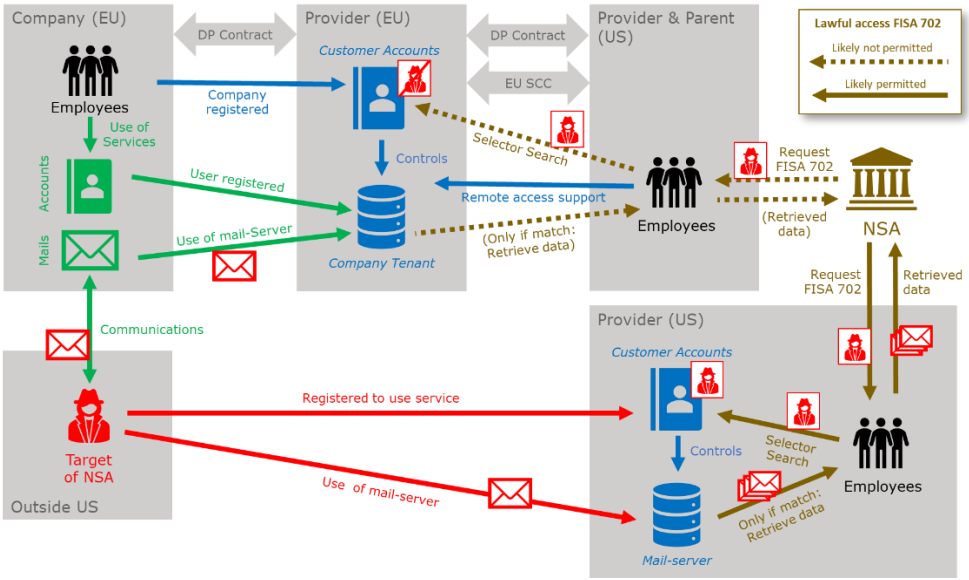
All of these use cases assume that the ECSP has "possession, custody or control" over the data at issue or the data at issue in plain text (Q35). If this is not the case (as a result of precautions frequently taken by customers or the provider itself) then this would be a further ar-

gument why a search, collection and production could not take place with regard to such data under Section 702.[88] If a customer were a target, but the provider has possession, custody or control of its data only in encrypted form, then the ECSP would only be required to produce it in encrypted form. It would not be required to produce the decryption key.

In the Use Cases 5, 6 and 7 one would also have to consider whether the applicability Section 702 actually extends to the gathering of data on data centers located *outside the US*. It by no means clear whether that is the case. Vladeck holds that it is not and, thus, only EO 12333 applies, which works differently (see below).[89]

Use Case 5 is apparently similar to the case that the Danish data protection authority decided upon in July 2022 (Case 2020-431-0061). The case involved Danish schools using the services of Google, which are typically offered through Google Ireland, but also involve Google in the US. The authority argued that the US person targeting restriction of Section 702 only applies if the access request has the purpose of obtaining information *about* a US person but not *from* a US person. In my view, it missed the point in several ways.[90] In addition to the reasons listed in Use Case 5, it in my view in this particular case can be reasonably assumed that neither the Danish schools nor their pupils are targets under Section 702, which is why their accounts will be safe even if none of them is a US person.

Here is a chart that illustrates the above Use Case 10 (in comparison with some elements of Use Case 5):




88 Vladeck (footnote 39), p. 9.

89 Vladeck (footnote 39), p. 9.

90 Although it may not be entirely relevant, the communications between Google Ireland and Google US for supporting Danish schools *is* communications "about" (i.e. of) a US person (here: Google US).

As one can see from the above Use Cases and procedures, and contrary to what EU data protection authorities tend to argue, it *is* of relevance for at least the "risk-based approach" how probable a particular European company or organization is a target under Section 702, which will only be the case if it is "expected to possess, receive, and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory authorized for targeting". Only if a company or organization has become a target, its contents and non-contents of its account can be collected and produced to the NSA under a Section 702 downstream request. Of course, it easily possible that communications of a company, its employees or customers is collected by the NSA in connection with accounts of *other* targets. This gathering of information, however, would happen by way of accounts or transmission that are beyond the company's control and do not have to be covered in a foreign lawful access analysis for data protection and professional secrecy purposes.

The Use Cases further show that European customers can get substantial additional protection against Section 702 collections by contracting with the European subsidiary of the US-based provider instead of entering into a direct contract with the US parent. Conversely, it does not provide any additional legal protection under Section 702, if a European customer uses a data center in Europe but still directly obtains the service from a US-based provider (i.e. becomes the US-based provider's direct customer). This is a common misunderstanding. See also Q32 on that point.

The same is true under the GDPR: If a European company contracts with a US-based provider (instead of its EEA entity) any transfer of data will be considered to fall under Chapter V of the GDPR even if the data center operated by the provider is located in the country of the European company. The reason is that even though the data center is located in the EEA, it remains the US-based provider who is in charge to process the data for its customer and, therefore, needs to be (contractually) required to comply with data protection law.

**Executive Order 12333**

The other US law that the CJEU criticized in the "Schrems II" discussion is the Executive Order (EO) 12333 of December 4, 1981.[91] It applies to collections of data performed by the NSA *entirely outside* the US (as opposed to Section 702 that governs collections *within* the US), for instance by tapping into telecommunications network connections from "communications systems around the world".[92]

---

91 https://www.archives.gov/federal-register/codification/executive-order/12333.html, archived at https://perma.cc/Q3ZE-XM3M.

92 https://irp.fas.org/nsa/nsa-story.pdf, archived at https://perma.cc/J7AN-5DTW.

In connection with cloud projects and other transfers out of Europe, EO 12333 usually plays no relevant role because (i) it focusses on collection data in-transit and (ii) such data is usually heavily encrypted when originating from Europe (this may not be the case for communications from other regions in the world where encryption is restricted or prohibited, thus permitting the foreign intelligence community to more easily eavesdrop on such communications).

Hence, if an exporter from Europe and importer in the US (or any other exporter and importer) undertake that their data transfers are encrypted using state-of-the-art methods (and with the key not available to the telecommunications companies, so that they themselves cannot decrypt the traffic), then EO 12333 usually represents no issue.

Furthermore, the same or at least similar limitations on targeting US persons as under Section 702 seem to apply also in the case of EO 12333.[93] That said, unlike under Section 702, it is not clear whether the selectors in all cases would be applied by the telecommunications providers (meaning that only hits are passed along to the NSA) or whether the NSA collects all traffic of a particular route in bulk (and itself searches it for selector hits). The distinction is of relevance from a data protection point of view as in the former case one could argue that no collection takes place if the sender and recipient of a transmission is no target.

For a discussion of the latest Executive Order 14086 see Q29a below.

**Applying the above using my method**

My method leaves it to each user to themselves freely determine which of the legal and other arguments cited above will be successful and convincing and to which degree. Each user is free to give them a 0 percent, a 100 percent or any other chance it deems reasonable under the circumstances.

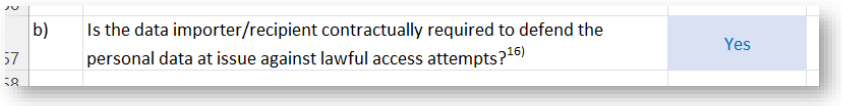
Both version of the method for US transfers cover mass surveillance under Section 702 FISA and EO 12333:

- **Upstream Surveillance:** The "EU SCC Transfer Impact Assessment (TIA)" for US law covers EO 12333 only in a very limited manner by asking whether any transmissions over public networks are encrypted in-transit. If not, the transfer is not considered permitted under the GDPR, Swiss DPA or EU SCC because it may become subject to NSA (or other foreign intelligence) collection activity somewhere in the world. In these cases, it would still be possible to argue that the exporter has no reason to believe that such collection will take place on the grounds that the sender and recipient is no target, but the argument does in my view not

93 Raul (footnote 40), p. 12 (including in particular footnote 29), with further references, arguing that the same US person limitations under Section 702 apply by way of presidential order.

apply in those cases where the NSA itself undertakes to search the transmission for selectors and, therefore, collects all traffic in bulk. In the other version of my form, "upstream" surveillance (under both Section 702 and EO 12333) can be assessed in more detail, namely whether the relevant data can be reviewed in-transit (which usually can be prevented by encryption, resulting in a 0% probability) and whether selectors are expected to create hits (i.e. whether it would contain traffic of targets) or are otherwise in-scope of upstream surveillance.

- **Downstream Surveillance:** Here, the "EU SCC Transfer Impact Assessment (TIA)" for US law is more detailed, but the other version of the method is compatible with it (see the corresponding references in the TIA Excel). "EU SCC Transfer Impact Assessment (TIA)" for US law first permits the user to assess the probability that the importer is *not required* under US law to permit a downstream data collection under Section 702. Of course, the has the possibility to take into account how likely the US intelligence authorities will comply with the legal prerequisites, particularly given the lack of judicial control. If the user concludes that there can be no effective judicial control and that even a "defend-your-data" clause is ineffective, it can change this value to "No":




If it is "No", the formula will take into account the probability that the authorities will comply with the rules (which is stated in Step 2 f)[94]).

If the probability of the *legal arguments* preventing a problematic lawful access is sufficiently low, the exporter and importer can argue that even under the "rights-based" approach, there is no reason to believe that Section 702 will be applied. Of course, there may be people who argue that given the lack of judicial control with regard to Section 702 there can never be reason to believe that the US authorities will comply with their rules. Each assessor will have to decide this on their own.

The legal arguments provided for are (i) whether the importer is an ECSP (and also acts as an ECSP with regard to the data transferred, i.e. is not required to produce own communications, such as in Use Case 5), (ii) whether the importer has possession, custody or control with regard to the data transferred (Q35), (iii) whether the targeting procedures (see above) may prevent a collection, (iv) whether the principle of international comity may

94 Example: If set to 50 percent, the probability calculated based on the legal arguments will be multiplied with 200 percent.

prevent the application of Section 702 (see Q29), and (v) whether there are other legal arguments that may play a role (e.g., the Fourth Amendment).

The two further assessments relate to (a) the way how Section 702 is applied in practice and would be applied in the specific case (e.g., whether the content at issue is of the type which the NSA requires to be collected or how likely the ECSP will receive a collection request under Section 702) and (b) the technical ability of the importer to search and find the selectors used by the NSA and produce the resulting data (which may be limited, for example, if the importer has only remote access). The overall probability of these further assessments together with the legal arguments can be used for the "risk-based" approach. In the other version of my method, the legal arguments are combined in one assessment.

29a. **What has the Executive Order 14086 and subsequent Adequacy Decision changed?**

On October 7, 2022, the US President (Biden) signed an Executive Order (**EO**) designed to resolve the current "Schrems II" data protection issues when having personal data transferred from Europe to the US.

In principle, the EO clarified and expanded the protections that are already provided for under the existing EO 12333 and PPD-28 (Q29 at the end), which govern "signals intelligence". It is not clear whether it will also apply to downstream collections under Section 702 FISA, but it may be the case. In essence, the EO provides that lawful access in the context of signals intelligence shall only occur "proportionate" and where "necessary" (as opposed to "as tailored as feasible") and provides for a redress mechanism by an independent body (which did not exist so far). The EO does not mention any country in particular. The redress mechanism is open only to individuals in "qualifying states", or – to be precise – to individuals who are permitted to submit such complaints through a qualifying state. It is the US Attorney General who ultimately designates a country (or group of countries, such as the EU) to be a qualifying state. As per the EO they may only do so under certain conditions, including (i) the existence of mutual protections for US persons with regard to signals intelligence in the qualifying state and (ii) where the qualifying state permits or is anticipated to permit commercial transfers of personal data to the US.

In the meantime, the US government has implemented the EO 14086, it has recognized the EEA, United Kingdom and Switzerland have been designated qualifying states, and it has agreed with the EEA, United Kingdom and Switzerland on the "Data Privacy Framework" (**DPF**), further development of the "Privacy Shield" program that permits certain US companies to self-certify that they will comply with basic principles that mirror European data protection ground rules. The European

Commission assessed the DPF and implementation of the EO 14086 and on July 10, 2023, issued an adequacy decision pursuant to Art. 45 GDPR for transfers to US companies that are self-certified under the DPF.[95] The United Kingdom and Switzerland followed.[96] While there are some that challenge the validity of these adequacy decisions, in particular in the EU (in fact, there may in the coming years be a "Schrems III" decision that may turn upside down the entire situation), they for the time being govern many transfers of personal data to the US, at least with regard to the use of a number of US-based online providers. For instance, the three hyperscalers Microsoft, AWS and Google are self-certified under the DPF, which means that personal data transfers from Europe to their US entities do not require any additional measures as per Chapter 5 of the GDPR or Art. 16 of the Swiss DPA.

Even where the recipient of personal data in the US is not self-certified under the DPF, transfers de-facto have become a non-issue to the US: While technically, every exporter under the requirements set forth by the "Schrems II" decision and Clause 14 of the EU SCC still needs to perform a Transfer Impact Assessment (**TIA**), this is today a pro-forma exercise in view of the fact that the European Commission and others have found US lawful access laws given the implementation of EO 14086 to be compatible with European data protection standards. We offer a pro-forma TIA template for the US, which can be downloaded here (EEA version) and here (Switzerland version) and that refers to these decisions.

Even the EU data protection authorities, who in the post-Schrems II years lost much credibility by strongly and unreasonably opposing any data transfers to the US (and later on tried to blame the CJEU for this), have suddenly fallen silent on the topic. Also, resistance against using cloud providers located in the US, at least from a data protection point of view, has diminished to a great extent on their part. Other privacy aspects of cloud computing have become more important.

This only somewhat changed in early 2025 when there were reports that the "Privacy and Civil Liberties Oversight Board" (PCLOB) may have become difunctional due to activities of the Trump administration, which could endanger DPF and ultimately the adequacy decision for the US.[97]

---

95 See https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.

96 For Switzerland, see https://www.vischer.com/en/knowledge/blog/swiss-us-dpf-how-to-transfer-data-to-the-us-with-and-without-it/.

97 See https://iapp.org/news/a/how-could-trump-administration-actions-affect-the-eu-u-s-data-privacy-framework-.

### 30. What about the US PATRIOT Act?

The US PATRIOT Act[98] was passed on October 26, 2001 as a direct reaction to the September 11 attacks and provided US authorities *inter alia* with broad surveillance powers, in particular in connection with what became known as Section 215. Section 215 permitted the FBI to access a broad range of information under the FISA and was used for conducting mass surveillance *within* the US.

While the PATRIOT Act was extended several times, US parliament failed to agree on an extension in 2020, which is why Section 215 and two other provisions have expired.[99] Meanwhile, in 2015 the US FREEDOM Act[100] came into force, which essentially replaced the PATRIOT Act, but limited the government's authority to collect data. To nevertheless permit the NSA's ongoing collection of international email and phone communications without court order and allow the FBI to access information under certain conditions, Congress included the program in the form of Section 702 FISA (Q29).[101]

### 31. What is the US CLOUD Act? Does it violate Swiss law?

The US CLOUD Act[102] was enacted in March 2018 and has two distinct parts that have to be distinguished, but are sometimes mixed up:

- **Part 1:** The first part of the US CLOUD Act amended the Stored Communications Act (**SCA**) following a court case involving Microsoft, where the company refused to turn over customer data requested by the US authorities by arguing that the data was not located in the US and that the SCA had no extraterritorial effect. Microsoft lost in the first instance, but contrary to all precedents, the appeals court sided with Microsoft. Before the US Supreme Court could decide the case, Congress passed the US CLOUD Act that clarified that US electronic communication service providers or remote computing service (which includes cloud providers) are required to produce customer data requested by US authorities in connection with the prosecution of a "serious crime" regardless whether the data is hosted on servers within or outside the US.

---

98 The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, see https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1281 (archived at https://perma.cc/65ZE-XPGU), with further references.

99 Vladeck (footnote 39), p. 10; https://www.eff.org/deeplinks/2020/12/section-215-expired-year-review-2020, archived at https://perma.cc/85Y3-2URY.

100 The Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring of 2015 (https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf, archived at https://perma.cc/C9JF-5958).

101 https://www.justsecurity.org/78753/rethinking-surveillance-on-the-20th-anniversary-of-the-patriot-act/, archived at https://perma.cc/RV5W-LZ84.

102 Clarifying Lawful Overseas Use of Data Act (https://www.justice.gov/dag/page/file/1152896/download, archived at https://perma.cc/U7PH-TGMF).

- **Part 2:** The second part of the US CLOUD Act permits the US government to, under certain conditions, enter into a so-called *Executive Agreement* with another country, permitting the law enforcement authorities of both countries to directly approach providers in the other country, subject to certain limitations (such as the protection of the citizens of such country). The providers could directly respond to such "international" production orders. The idea is to facilitate cross-border lawful access of data electronically stored by foreign providers without going through traditional judicial assistance. The UK and Australia have entered into such Executive Agreements with the US, the EU would like to have one, too. The Swiss Federal Office of Justice analyzed the possibility of Switzerland entering into an Executive Agreement and concluded that it would, in many respects, not be compatible with Swiss data protection law and the principles of judicial assistance.[103] While there initially was some lobbying on the part of Swiss-based service providers for an Executive Agreement, the prevailing opinion is that it would be a very bad idea for Switzerland to have one, as it would make it much more difficult than today to prevent lawful access by US authorities.

*Hogan Lovells* has published a very good brochure on "Demystifying" the US CLOUD Act, with many references to US case law.[104]

In connection with cloud projects and transfers to the US from Switzerland, only Part 1 of the US CLOUD Act is of relevance. Two scenarios have to be distinguished:

- **Professional and official secrecy:** If an organization needs to maintain professional or official secrecy, it usually (and absent any valid waivers) has to make sure that no lawful access from outside of Switzerland *at all* occurs. A lawful access pursuant to the US CLOUD Act or SCA would usually be considered a breach of professional or official secrecy. This is why these organizations (e.g., banks) need to make a foreign lawful access assessment that covers the US CLOUD Act or SCA and not only Section 702 FISA (Q12).
- **EEA and Swiss Data protection law:** If an organization transfers personal data to a country without an adequate level of statutory data protection but with the EU SCC in place, not all forms of foreign lawful access are problematic.

---

103 Gutachten des Bundesamts für Justiz vom 17. September 2021 (only in German and French) (https://www.bj.admin.ch/bj/de/home/publiservice/publikationen/berichte-gutachten/2021-09-17.html, archived at https://perma.cc/7S7Y-N9DA).

104 For a broad overview, see, for example, https://www.hoganlovells.com/en/publications/demystifying-the-us-cloud-act, archived at https://perma.cc/X4G4-8D5Y.

Data protection law permits foreign lawful access that respects certain essential procedural and other guarantees: (1) Access has to be subject to the principle of legality, i.e. of clear, precise and accessible rules, (2) it has to be subject to the principle of proportionality, (3) there have to be effective means of legal redress for the data subjects to pursue their rights in the target jurisdiction in connection with an access to their personal data, and (4) any access must be subject to legal recourse to an independent and impartial court (or other forms of independent recourse bodies). Last but not least, (5) foreign lawful access is only permitted for one of the purposes of Article 23(1) GDPR.[105]

Lawful access under the US CLOUD Act and SCA fulfill these requirements (see also below). This is why the form "EU SCC Transfer Impact Assessment (TIA)" cannot be used to validate the applicability of the US CLOUD Act, but only Section 702 FISA and EO 12333.

Data protection authorities in Switzerland have sometimes contended that lawful access under the US CLOUD Act is not compatible with Swiss procedures and data subject guarantees or is even contrary to Swiss public order. This is wrong. Some may have mixed up the US CLOUD Act with Section 702 FISA (Q29), some may have mixed up Part 1 and Part 2. They are apples and oranges:

---

[105] The legal basis is Art. 44 et seq. GDPR, Art. 6 Swiss Data Protection Act, Art. 16 et seq. revised Swiss Data Protection Act; the Recommendation 01/2020 of the European Data Protection Board (Version 2.0 of June 18, 2021); the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of the European Commission (C(2021) 3972 final of June 4, 2021); and the Guide for checking the admissibility of data transfers with reference to foreign countries (Art. 6 para. 2 letter a FADP) of the Swiss Federal Data Protection and Information Commissioner dated June 18, 2021 (as amended on June 22, 2021).

| | Stored Communications Act & US CLOUD Act (re territoriality) | Section 702 FISA (inside US) EO 12333 (outside US) |
|---|---|---|
| Purpose | Investigating "serious crimes" | Protecting national security, investigating crimes (FBI) |
| Type of lawful access | One-time targeted access to specific customer data held by a US provider | Continuous search of a US provider for communications of targets |
| Affected by lawful access | Suspect of a crime, individuals involved in such crime | Targets of US intelligence community (approx. 200k) + people communicating with them |
| Compatibility with European law | ✓ Art. 18(1) Cybercrime Convention | ✗ ECJ 16.7.2020 C-311/18 "Schrems II" ✓ With EO 14086 implemented |
| Comparable provisions under Swiss law | Art. 265 Swiss Criminal Procedure Law (territoriality: e.g., DFC 143 IV 270) | Art. 39 et seqq. Swiss Intelligence Service Act ("signals intelligence") |
| To be assessed for transfers of personal data (Art. 16 Swiss DPA) | No | Yes (only pro-forma, for EU SCC transfers) No (for transfers under the EU-US/CH-US DPF) |
| To be assessed for transfers under professional or official secrecy | Yes | Yes |
| Which assessment form to use (if pro-forma is not sufficient)? | "Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities" | "EU SCC Transfer Impact Assessment (TIA)" (included also in the left form) |

The right of law enforcement authorities to request a provider in their jurisdiction to turn over customer data under its possession, custody or control is not unusual. It is found in Article 18(1) of the Cybercrime Convention of the Council of Europe. The explanatory report explains that "control" may also means access "by means of a remote online storage service":[106]

> 173. Under paragraph 1(a), a Party shall ensure that its competent law enforcement authorities have the power to order a person in its territory to submit specified computer data stored in a computer system, or data storage medium that is in that person's possession or control. The term "possession or control" refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory (for example, subject to applicable privileges, a person who is served with a production order for information stored in his or her account by means of a remote online storage service, must produce such information). At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement.

In fact, under Swiss law, law enforcement authorities have at least the same rights as under Part 1 of the US CLOUD Act and they interpret and apply them accordingly. If a Swiss prosecutor asks a Swiss-based cloud service provider to turn over certain customer records, the provider will have to do so regardless of whether it is using a data center in Switzerland, Germany or Ireland to store such data.[107] What is rele-

---

106 https://rm.coe.int/16800cce5b, archived at https://perma.cc/C3TG-XWSP.

107 What Swiss law enforcement is *not* allowed to do (but neither are US law enforcement authorities) is to serve a production order to a foreign provider (see DFC 141 IV 108); for serving a foreign provider, judicial assistance is required; this is, in fact, what an Executive Agreement as discussed in Part 2 of the US CLOUD Act would change, but Switzerland has no such Executive Agreement.

vant is that such data is under the *possession or control* of the Swiss-based cloud provider.[108] Use of the Internet to access an account on a computer abroad is not considered a violation of the principle of territoriality under Swiss law, as recently confirmed by the Swiss Federal Tribunal[109] – which is exactly what the US CLOUD Act provides for.

Many other European countries have similar provisions in their law, because they are considered compatible with EU and Swiss data protection law. This is why Switzerland – despite provisions comparable to the US CLOUD Act – is nevertheless considered by the EU as a country with an adequate level of data protection, and vice versa.

This was ultimately confirmed by the adequacy decisions by the European Commission and for Switzerland by the Federal Council and the legal opinion of the Federal Office of Justice relied upon for the decision.[110] Had the US CLOUD Act not been considered compatible with European data protection law, an adequacy decision would not have been possible.

### 32. Will the US CLOUD Act or Section 702 FISA force European subsidiaries of US providers to produce data of European customers?

In many cases not – contrary to widespread belief.

A subpoena (or warrant) may only be directed to a provider if that entity is subject to personal jurisdiction in the US, which – in turn – requires such entity to have "minimum contacts" with the US, meaning that the entity "could reasonably expect to be haled into court"[111] in a particular US state.[112] Furthermore, minimum contacts can be of systematic and continuous nature (resulting in "general jurisdiction") or isolated or occasionally with regard to specific issues (resulting in "specific jurisdiction" only, which is limited in scope).

Whether personal jurisdiction applicable to US government production requests exist in the case for a subsidiary of a US provider is a question that needs to be decided on the circumstances of the case, and it is often not an easy decision. It is also important to understand that

---

108 Which was confirmed in DFC 143 IV 21, where Facebook Switzerland was served in Switzerland with a production order but successfully argued that it had no possession or control over the data sought; the data was controlled by Facebook Ireland.

109 DFC 143 IV 270; a Swiss prosecutor used account credentials of a suspect to log into a Facebook account and obtain data stored on servers in the US and Ireland. In another case, the Federal Tribunal did not find it acceptable to obtain data from a suspect by a tracking and recording device after the suspect had taken such device outside Switzerland (DFC 146 IV 36).

110 See https://www.vischer.com/en/knowledge/blog/swiss-us-dpf-how-to-transfer-data-to-the-us-with-and-without-it/.

111 World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286 (1980) (https://supreme.justia.com/cases/federal/us/444/286/, archived at https://perma.cc/6GZ4-ZRUT).

112 For example, as required under the "Due Process Clause" of the Fourteenth Amendment of the US Constitution.

this question has nothing to do with the extraterritorial effect provided for by the US CLOUD Act. If a company outside the US has no minimum contacts to the US, the US CLOUD Act simply does not apply to it, regardless of its extraterritorial effect and who owns the company.

If a US government body wishes to issue a production request (e.g., a subpoena) to a foreign subsidiary of a US provider and if it has jurisdiction over such subsidiary and all other conditions are fulfilled, too, it may indeed eventually issue such request to the foreign subsidiary. That does not mean that such request is practically enforceable. If such request conflicts with the local law applicable to the subsidiary (e.g., data protection law [as will usually be the case in Europe] or a blocking statute such as Art. 271 SPC [as in Switzerland, see Q37]), it will most likely be and have to be ignored by the subsidiary and, thus, be ineffective.

Furthermore, there may be more jurisdictional issues to be resolved. As opposed to the US CLOUD Act, Section 702 FISA is understood to cover collections of data only on US territory,[113] which condition would not be fulfilled in the case of a European subsidiary, unless the subsidiary were to use a data center in the US, which is unlikely to be the case. The US government would have to rely on judicial or administrative assistance to enforce it, if and to the extent available in the subsidiary's jurisdiction. Hence, in practice, US authorities will usually not directly issue such requests against foreign providers already due to the lack of enforceability (which would entail the risk of the provider informing its customer despite a prohibition to do so).

The foregoing has led to a discussion whether Section 702 FISA (or the Stored Communications Act and US CLOUD Act) could nevertheless apply to a foreign subsidiary of a US provider because such subsidiary could be viewed as the US parent's "agent".[114] While this is theoretically possible, the bottom-line would not be different. *First*, in the cases that are of interest here, it is unclear whether there is any agent involved in the first place. But even if there were an agent, the European subsidiary would rather be the principal of its US parent, with the latter being the agent. This is because most US providers with European subsidiaries will use the *European* entity to contract with their European clients and not the US entity. Hence, the European subsidiaries are in charge of providing the cloud or other online services to their European customers, with the US parents only supporting them (but not representing them vis-à-vis the customer). In the case of Section 702 FISA, the principal of a US-based Electronic Communication Service Provider (**ECSP**) would not qualify as "an officer, employee, or agent of

---

113 Vladeck (footnote 39), p. 9, stating that "where data of non-U.S. persons is held by non-U.S. companies outside the territorial United States, section 702 does not apply at all".

114 Vladeck (footnote 39), p. 9.

an entity"[115] of an ECSP and, therefore, not be covered by Section 702. *Second*, even if the European subsidiary were considered an agent of the US parent, the problem of enforcing a request against the subsidiary referred to above still applies.

This means that even if one were to consider the European subsidiaries as ECSP with personal jurisdiction, the only way how to enforce Section 702 against them would be vis-à-vis *their* officers, employees or agents located in the US and only with regard to data located on US territory. Even if their US parent were considered to be their agent, which may or may not be the case, they under Section 702 FISA could only be forced to produce the data on US territory, which may be nothing.

This seems to be confirmed by Stephen I. Vladeck, the expert mandated by the German data protection authorities to opine on Section 702 FISA, in November 2021 concluded: *"I have a hard time conceiving of a fact pattern in which the U.S. government could be attempting to acquire data under section 702 from an electronic communication service provider that has no footprint in the United States."*[116] According to him, the US government would have to proceed against the *"entity that has a U.S. presence in order to compel compliance with a directive issued under section 702"*.[117]

Hence, instead of directing production requests to foreign subsidiaries of US-based providers, a US authority will primarily approach the US parent in its capacity as an ECSP. Instead of relying on arguments that its European subsidiaries are its "agents" or the US parent being their agent, the US authority will rather assess the level of "control" that the US parent has over the data processed by its subsidiary in Europe.

In practice, this is the only realistic path for US authorities to gain access to data processed by the European subsidiaries of a US-based provider: The European subsidiary grants its parent either *legal control* (which will usually not be the case, in particular not where the US-parent is solely a sub-processor) or *day-to-day control* with regard to the customer data it is processing (which can well happen depending on how it makes such data available to its US parent). I refer to the discussion of "possession, custody or control" under Q35.

The foregoing considerations show how important it is for customers in Europe to contract with the European subsidiary of a US-based provider and not with the parent company and make sure that the US parent has no day-to-day or legal control over the data at issue.

---

115 Definition as per 50 U.S.C. § 1881(b)(4)(E) (https://www.law.cornell.edu/uscode/text/50/1881).

116 Vladeck (footnote 39), p. 10.

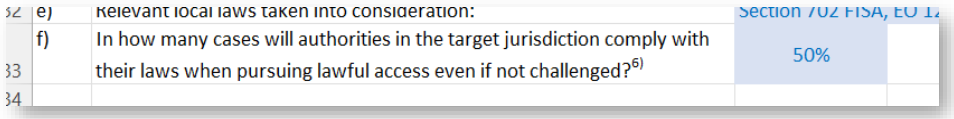
117 Ibid.

### 33. Can we rely on foreign authorities complying with their laws and what does that mean for your method?

This will very much depend on the country at issue. We will have to distinguish between those countries where laws are generally obeyed with and where appropriate judicial control exists to ensure so and those countries where this is not the case.

In fact, even in Switzerland or any country of the EEA, law enforcement, intelligence authorities and other public bodies will not always comply with the law. As such, this does not prevent us from disclosing data into such countries. What is relevant from a legal perspective is whether the laws in such countries are, in principle, acceptable and whether there are means to verify and enforce compliance with them.

My method takes this into account as well. It considers whether the recipient of data (i.e. the provider or other form of "importer") is required to challenge any production request. A contractual obligation of the recipient to challenge each and every request from a government body (a so-called "defend your data" clause) is, therefore, essential. If there is no such obligation, then the reliability of the local authorities has to be assessed, as well:



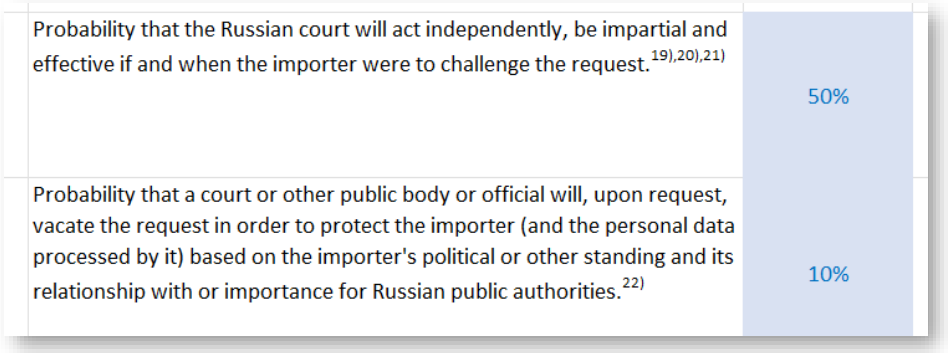

With regard to the US, every assessor will have to form its own opinion about whether and to which extent the US government can be expected to comply with its own rules, and how much they threaten the rights of a data subject. They will have to consider that one of the main shortcomings of Section 702 FISA (and EO 12333) is the lack of judicial control, which is usually considered necessary to ensure compliance with law. That said, there is – even from within the US – considerable pressure on the US intelligence community and the US Congress to limit Section 702 FISA; in the case of the limitations concerning "abouts" communications (see Q29) that were introduced in the last years, such pressure was apparently at least partially successful.[118] Whether that will continue to be the case under the Trump administration remains to be seen. With the multi-scenario worksheets, it is possible to take a differentiating view on this aspect and consider also a scenario in which US authorities will no longer feel bound by the rule of law and separation of power as has been the case in the past.

---

[118] See, for example, the https://www.aclu.org/letter/coalition-letter-urging-reforms-section-702-fisa (archived at https://perma.cc/X9PW-MA3K), requesting the prohibition of collection of "abouts" communication.

The tools I offer are agnostic to that end with regard to the US. They permit every assessor to itself conclude their level of confidence that a particular legal argument will prevail in preventing lawful access.

In some countries, though, it is clear that there is no reliance on the judicial system, even where it is formally in place. This is why versions of my "Transfer Impact Assessment" for other countries focus on this aspect specifically. For example, the Russian version of the Transfer Impact Assessment expressly considers this aspect (leaving up to the assessor to fill in an appropriate value):



| | |
|---|---|
| Probability that the Russian court will act independently, be impartial and effective if and when the importer were to challenge the request.[19),20),21)] | 50% |
| Probability that a court or other public body or official will, upon request, vacate the request in order to protect the importer (and the personal data processed by it) based on the importer's political or other standing and its relationship with or importance for Russian public authorities.[22)] | 10% |

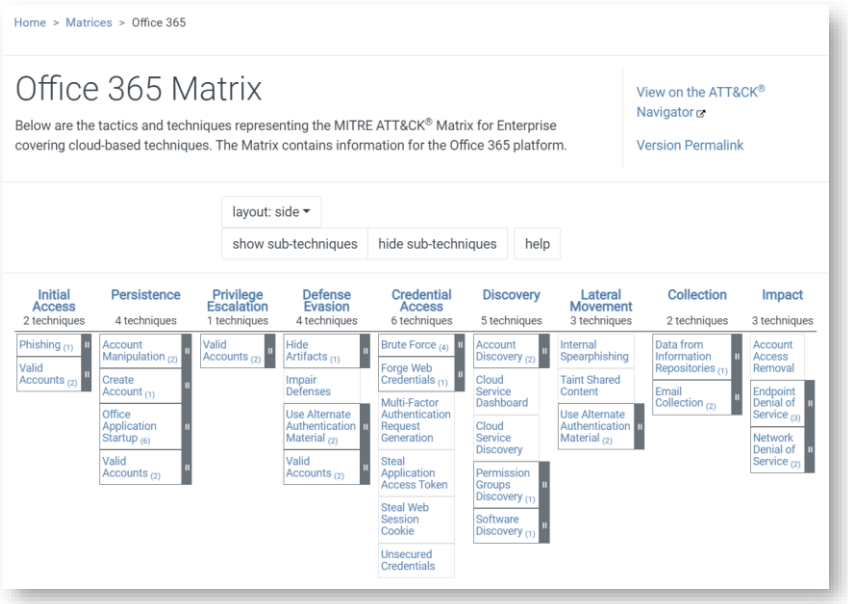
34. **Forget about lawful access – the US intelligence authorities will break into our computers and networks and steal our data!**

This may certainly be true in certain cases, and EO 12333 (Q29) actually permits them to do in certain cases. However, this kind of intelligence activity is out of scope of my method because such forms of lawful access does not rely on a rule of law to gain access (i.e. compelling a provider to produce customer data), but by circumventing the data security (i.e. "hacking" the provider).

These scenarios have to be considered as well in every project, but it is a different type of risk assessment. It is the same kind of risk assessment that also has to be done in view of attacks of cybercriminals. It consists of analyzing the potential vulnerabilities of a particular system and organization and assessing how probably they can be misused.

For example, if an organization uses Office 365 (or M365), there are a number of well-known ways to attack the system. This is an overview of such methods provided by MITRE ATT&CK:[119]

[119] https://attack.mitre.org/matrices/enterprise/cloud/office365/.




In each M365 project, these attack paths (and other aspects of data security) have to be analyzed. Then, the organization has to implement appropriate technical and organizational measures to make it difficult for both cybercriminals and foreign governments to undertake such attacks. At the end, a risk assessment has to be made to determine the residual risks of data security (see also Q23 on how such assessments are done)

In view of the foregoing, some data security experts tell me that they believe that it is more likely that cybercriminals and foreign governments will access "their" data by way of hacking into their systems than by proper and official foreign lawful access. This is one reason why they are eager to move to the cloud, even if the provider is US-based. They believe that these cloud offerings provide them a better level of security than they could achieve with their on-premise systems.

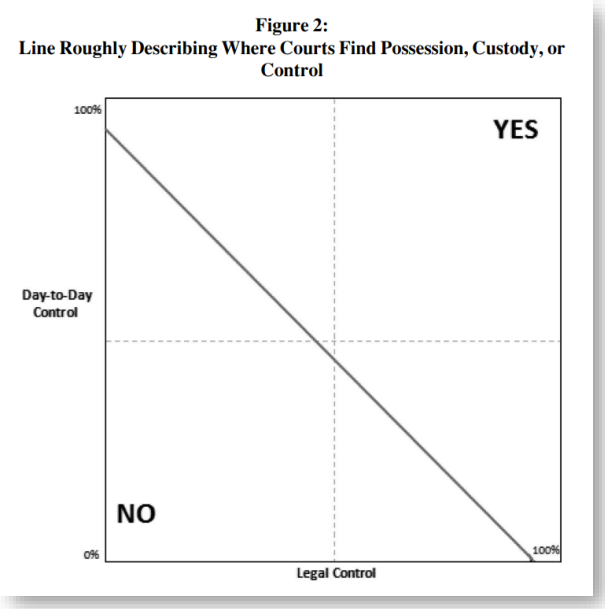
Last but not least, some US lawyers contend that using the services of a US-based provider may, in certain setups, actually even provide *better protection* against access by US intelligence authorities than relying on a non-US-based provider because US intelligence authorities are *not* permitted targeting US persons or communications among US persons or occurring within the US (but have much more leeway in acting against non-US-persons), which I find is quite an interesting argument (see Q29 for details).

## E. HOW TO CONSIDER US LAW IN THE ASSESSMENT

### 35. Does it make a difference whether a US provider only has remote access in certain specific cases?

Yes, this can make a big difference. This is one of the mostly overlooked factors to prevent foreign lawful access in the US (another one is discussed in Q37). Under US law, a provider will only have to give authorities access to customer data in plain text if such data is under its "possession, custody or control".[120]

At this point, it is important to understand that the term "control" has a different meaning under the GDPR and US law. Rather, the standard "possession, custody or control" is a rule that has been established in US law already for many years, including in civil and criminal procedure law. Under US law, even a processor (in terms of the GDPR) can be found to have "control" over data and, subsequently, be required to produce it to the authorities. Under the GDPR, "control" refers to controlling how data is processed, whereas under US law, "control" refers to the right to obtain the data as such ("legal" control) or actual access in the ordinary course of business even if there is no legal ownership or control ("day-to-day" control). See Hogan Lovells "Demystifying the U.S. CLOUD Act" and the work of Hemmings, Srinivasan and Swire to better understand the concept. I found the following chart of the latter source to be very illustrative for the present purposes – if you manage to end up in the lower left part, you are "safe":




120 18 U.S. Code § 2713 (https://www.law.cornell.edu/uscode/text/18/2713), which ist the provision that was added to the Stored Communications Act by the US CLOUD Act (https://www.justice.gov/dag/page/file/1152896/download, archived at https://perma.cc/W4KE-TPQY).

A European exporter can usually avoid "legal" control on the part of the importer by having the right contractual clauses in place, for instance by way of a data processing agreement that permits the provider to process the personal data only as per the documented instructions of the customer (where such instructions do not include any use of the personal data for the provider's own purposes).[121] Courts have defined "legal" control as "the legal right to obtain documents requested upon demand."[122]

Avoiding "day-to-day" control is more difficult but will often be possible to a certain degree even without full encryption. Day-to-day control has been defined as "a company's ability to demand and have access to documents in the normal course of business gives rise to the presumption that such documents are in the litigating corporation's control."[123] All circumstances can be considered.

In the case of a cloud computing setup, the mere technical ability of a US provider to technically gain access to the data at issue is not sufficient to assume "day-to-day" control. When being served with a government production order, a provider is not required to circumvent technical controls that prevent its own employees to access customer data; a provider also does not have to "hack" into its own systems in order to fulfill the request or implement "back doors". Given how US courts handle the "day-to-day" control criteria, mere organizational measures that ensure that a provider's employees in the US do not have access to plain text customer data in the ordinary course of business will already result in a good chance of success according to US counsel. An example of such a measure is Microsoft's "Customer Lockbox" service. Other providers have different ways for achieving similar results.

The counterexample to avoid would be a European subsidiary that contracts with European customers but has its cloud data centers operated by its US parent. The actual location of the data center would be irrelevant. What counts is whether the US parent has control over the data stored therein in plain text, even if only for providing the services to its European subsidiary. The US authorities could argue that the US parent has "possession, custody or control" of the data at issue.

The "possession, custody or control" requirement also determines whether a US provider can be required to produce documents that are

---

121 Whether a "processor-to-sub-processor" DPA would result in legal control to the processor due to the right of the processor to provide instructions to the sub-processor is unclear. Since the processor is, itself, only complying with instructions, this level of control would probably not result in "legal" control, because it can only be exercised for making data available to the customer (i.e. the controller) and not the processor.

122 United States v. Int'l Union of Petroleum & Indus. Workers, AFL-CIO, 870 F.2d 1450, 1452 (9th Cir. 1989).

123 Jonathan D. Jordan, Out of "Control" Federal Subpoenas: When Does a Nonparty Subsidiary Have Control of Documents Possessed by a Foreign Parent?, 68 Baylor L. Rev. 189, 200-01 (2016).

held by its foreign subsidiary (see Q32 on this question). It is a myth that the US CLOUD Act requires any subsidiary of a US provider to produce documents requested just because it has a parent is in the US. Ironically, US courts most often have to decide the opposite setup, i.e. whether a US subsidiary had control over documents stored by its foreign parent.

My method does not require you to be sure about the "possession, custody or control" argument; you can say that Microsoft will have only an 80 percent chance of winning on this legal argument when challenging a production request in court (which Microsoft's contracts require it to do).

Normally, the biggest issue in practice is to *find out* about these measures. Many providers are still unwilling to be transparent and refuse to answer corresponding questions or only come up with "hot air" (you can use my questionnaire to provide you the relevant responses). They have not yet understood that it would be in their own best interest to set up their operations in a manner that better protect themselves from lawful access requests out of the US. This is particularly true where providers offer their services out of Europe, but still require their US parent company to have access to customer data in extraordinary situations (e.g., support cases, emergency situations). It would often not be a problem to set up the necessary organizational controls that will allow them to argue that US staff has no "day-to-day" control of personal data of European customers.

### 36. How do we assess whether a US-based cloud provider has "possession, custody or control" of our data?

Possession (and custody) means physical possession, which condition is usually not fulfilled, because most (customer-facing) providers do not own the data centers and servers they are using for providing the services and hosting customer data (rather, their parents, affiliates or third-party providers do). Therefore, in practice, the term "control" is much more relevant.

See Q35 for more about this, how to avoid "possession, custody or control" and how to evaluate whether a provider has "control".

See also Q32 on the question whether the US CLOUD Act or Section 702 FISA also applies to European subsidiaries of US providers, which is related to "possession, custody or control".

### 37. Your method relies on whether a foreign lawful access in the US violates Swiss or other local law – why? What is Art. 271 SPC?

Contrary to common belief, foreign law does not always prevail over local law – even when applied abroad.

According to the legal doctrine of "international comity", a foreign court or authority may decide that foreign instead of national law shall apply out of respect for foreign sovereigns. It also refers to the practice of countries to mutually recognize judicial, legal and executive acts. Some laws even prohibit their own authorities to perform official acts on foreign countries that have not been pre-approved by the government of the foreign country.

In the case of governments or public-sector organizations moving into the cloud, this doctrine will help to protect their data from being accessed by a foreign government, because such access would be considered a violation of sovereignty – which many western countries will shy away from doing, at least for traditional law enforcement purposes; they will rather rely on judicial assistance, at least where such treaties are in place (which is the case between Switzerland and the US). I do not share the optimism of two other legal authors who wrote an opinion for the City of Zurich[124] claiming that in the case of the US the Foreign Sovereign Immunities Act (**FSIA**) will simply prohibit US law enforcement access to cloud data of foreign governments. The FSIA has been created to govern *civil* claims against foreign governments, and there are many that dispute its applicability in the criminal context, let alone in a national security context (as it would effectively prevent gathering foreign intelligence).[125] Yet, we seem to agree that the principle of international comity requires the US authorities and courts to carefully consider whether a particular cause merits violating Swiss sovereignty in the case of cloud data of a Swiss public sector client and that the bar will be high.

The doctrine of international comity will also protect the private sector in the cloud, though.

For example, German law has strictly limited the right of German authorities to conduct cross-border investigations by way of remotely accessing servers located in Switzerland. I have been involved in obtaining government authorizations for such setups.

As another example, US law supports the doctrine of international comity by requiring authorities and courts to apply certain standards and rules in resolving conflicts between US and foreign laws.[126] This can be decisive in a case of foreign lawful access: If a US court or au-

---

124 Christian Laux, Alexander Hoffmann, Rechtmässigkeit von Public Cloud Services, September 16, 2021, paras. 184, 199 (https://www.lauxlawyers.ch/wp-content/uploads/2022/07/Cloud-Gutachten-fuer-OIZ-Stadt-Zuerich.pdf, archived at https://perma.cc/ND3R-HLA8).

125 See, for example, https://www.jtl.columbia.edu/volume-60/the-scope-of-sovereign-criminal-immunity-instrumentalities-under-the-foreign-sovereign-immunities-act, archived at https://perma.cc/HW69-WTU3, and https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1989&context=ncilj, archived at https://perma.cc/P2XL-YGQP.

126 See, for example, William S. Dodge, International Comity in American Law, in: Columbia Law Review, Vol. 115, No. 8, December 2015 (https://columbialawreview.org/wp-content/uploads/2016/03/Dodge-William-S..pdf, archived at https://perma.cc/A4WL-B8HU).

thority orders a company to produce certain evidence located on Swiss territory under the threat of criminal or quasi-criminal sanctions, the company has a good chance to get the order lifted if it can show that compliance with it likely results in the company's officials committing a crime under Swiss law (and that the corresponding provision of Swiss law is not "dead letter").

Demonstrating this will usually not be difficult because Swiss law protects data stored on Swiss territory pretty well: Article 271 Swiss Criminal Code (**SCC**) provides for jail sentences and fines for those who carry out official activities on Swiss territory without the permission of the Swiss government or for those who help them.[127]

I had to refer to this provision many times in my career in connection with foreign lawful access, and in all cases, US courts and authorities (e.g., US DOJ, FTC, SEC) accepted that they could not force the production of Swiss data under these circumstances.

Thus, it is quite clear that if Microsoft, Google, AWS or any other hyperscaler were ever compelled by US authorities to produce customer data *out of Switzerland*, they would challenge such request on the basis of Article 271 SCC to prevent the production of customer data and protect their own staff and officials in Switzerland *and* abroad (under Swiss law, people can be prosecuted under Article 271 SCC *wherever* they are located[128]).

These restrictions can be used to protect data against foreign lawful access even in cases where there is no measure in place that would technically prevent a foreign authority to access the data. This is one of the reasons why it is important for most Swiss banks and Swiss authorities to keep their data at-rest *only* in Switzerland even though they cannot exclude that their provider could remotely access such data from outside Switzerland. To be clear: Storing data at-rest in Switzerland is *not* required under Swiss data protection or professional or official secrecy law, but it is a relevant lawful access risk factor and, thus, a relevant measure. This is also a reason why we can take this into account as an effective "supplemental (organizational) measure" and in assessments using my method.

## F. RECEPTION OF THE METHOD AND OFFICIAL SUPPORT

### 38. Who uses and supports your method?

The feedback I received from peers and the market has been very encouraging. The support is broad, and it appears that my method is today used widely for assessing foreign lawful access risks in Switzer-

---

127 See, for instance, see, for example, the decision of the Federal Tribunal of November 1, 2021, 6B_216/2020, involving the (voluntary!) production of own documents to US authorities.

128 Art. 4 para. 1 SCC.

land. In March 2022, the Canton of Zürich (Switzerland's most populous canton) has actually declared it to be the official standard for all its government cloud projects.[129] The Canton's risk assessment for M365 was made by a group of experts from the IT department, the public prosecutor's office, the tax authority, the state chancellery and the police using the techniques and considerations described in this FAQ, and more. It has meanwhile been published.[130]

Over the last years, my team and I have used the method in many cloud projects involving dozens of financial institutions (banks, insurance companies), public sector clients (hospitals, governments, compensation funds) and other organizations that are subject to professional or official secrecy. Similarly, we used the "Schrems II" version of the method for cross-border data transfers of various multinational companies.

We also hear from various other law firms and consultants in Switzerland and abroad (including the "Big Four") that they do the same and recommend my method to their clients for sensitive international data transfers and cloud projects. Since nobody needs to report to me for using my method, I have no statistics. I also do not track downloads.

On September 1, 2021, the International Association of Privacy Professionals (IAPP) has published two implementations of my method under its own brand.[131,132] Various authors have picked up on the method, for example Nina Diercks and Heiko Markus Roth,[133] Nicolas Kötter[134] and Daniel Hürlimann and Martin Steiger.[135] Switzerland's most popular privacy blog datenrecht.ch reported about it several times, for example following the Zurich decision.[136]

The Dutch government has made it public that it relies on it (in a modified form) for its own cloud assessments.[137] In Denmark, the data pro-

---

129 https://www.zh.ch/bin/zhweb/publish/regierungsratsbeschluss-unterlagen./2022/542/RRB-2022-0542.pdf, archived at https://perma.cc/Y4K8-ZCDN.

130 https://steigerlegal.ch/wp-content/uploads/2022/08/20220324_zh_risikobeurteilung-microsoft-365.pdf, archived at https://perma.cc/W3VH-4NQS.

131 https://iapp.org/resources/article/transfer-impact-assessment-templates/, archived at https://perma.cc/PHQ7-6TV7.

132 I was no member of the IAPP and did not approach them.

133 https://www.wolterskluwer.com/en/expert-insights/data-transfer-to-unsafe-third-countries, archived at https://perma.cc/MGB3-BZGY.

134 https://www.dr-datenschutz.de/drittlanduebermittlung-leitfaden-zu-transfer-impact-assessments/, archived at https://perma.cc/3E65-4JAQ.

135 https://steigerlegal.ch/wp-content/uploads/2021/05/anwaltsrevue_2021-05_huerlimann-steiger_digitale-anwaltskanzlei.pdf, archived at https://perma.cc/J7YP-6UAJ.

136 https://datenrecht.ch/regierungsrat-zuerich-gruenes-licht-fuer-m365-risikobeurteilungsmodell-rosenthal-kanonisiert-risikogrenze-bei-10-ueber-5-jahre/, archived at https://perma.cc/L9AN-TDJR.

137 https://slmmicrosoftrijk.nl/wp-content/uploads/2022/02/Explanation-DTIA-on-MS-Teams-SharePoint-and-OneDrive.pdf, archived at https://perma.cc/6ZLN-NMEQ.

tection authority considered it in a specific case[138] (but rejected the assessment on grounds I believe are wrong, see Q26, Q29, Q39 and Q42).

I received also requests to approve the translation of the "Schrems II" version of my method into other languages, namely French, German and Swedish (no approval is necessary: Q45).

The Zurich High Court's Supervisory Commission on the Zurich Bar (Switzerland) *inter alia* refers to my publication of the method when asked by attorneys whether they can move to the cloud in view of their professional secrecy obligations.

The Public Prosecutor's Office of the Canton of Basel-Stadt, following a request of the Cantonal data protection authority in a pilot project involving two public hospitals in Basel, Switzerland, the review of the project documentation and a workshop to understand the method, on April 19, 2022, confirmed to me in writing that it considers the method suitable for determining whether an organization bound by Swiss professional and official secrecy can move to the cloud:

**Einschätzung mit Blick auf die Frage, ob mit der Inanspruchnahme von Cloud-Diensten eine Offenbarung eines gesetzlichen Geheimnisses (hier: des ärztlichen Berufsgeheimnisses) stattfindet**

Nach der Durchführung des Workshops und der Durchsicht der Dokumentation können aus Sicht der Staatsanwaltschaft die folgenden Punkte festgehalten werden:

- Ob die Auslagerung geheimnisgeschützter Daten in eine Cloud strafrechtlich als Verletzung des Berufs- oder Amtsgeheimnisses gewertet werden könnte ist davon abhängig, ob die für die Wahrung des Geheimnisses verantwortlichen Personen unberechtigten Dritten Zugriff auf die geheimnisgeschützten Daten gewähren oder zumindest billigend in Kauf nehmen, dass unberechtigte Dritte auf diese Daten zugreifen.

- Die Bedenken bezüglich einer strafrechtlichen Verantwortlichkeit beschränkt sich mit Blick auf das geplante Outsourcing in die Microsoft Cloud, gemäss Ihren Angaben, auf die Frage des "Lawful Access" ausländischer Behörden auf die geheimnisgeschützten Daten. Im Vordergrund steht dabei die Gefahr eines Zugriffs US-amerikanischer Behörden auf Grundlage des US Cloud Acts. Dieser Einschätzung kann aus Sicht der Staatsanwaltschaft zugestimmt werden.

- Die Berechnung des Risikos eines ausländischen "Lawful Access" erscheint nach Ansicht der Staatsanwaltschaft grundsätzlich ein geeignetes Kriterium, um die Vertretbarkeit der Auslagerung auch vor einem strafrechtlichen Hintergrund zu beurteilen. Eine Überprüfung des Ergebnisses im konkreten Fall ist der Staatsanwaltschaft indes nicht möglich, da dieses letztlich von den Einschätzungen der einzelnen Berechnungsfaktoren abhängt. Diese können von aussen nicht überprüft werden.

- Ob ein Provider im Ausland allenfalls gezwungen werden könnte, Daten in der Schweiz an ausländische Behörden herauszugeben, ist nach Auffassung der Staatsanwaltschaft letztlich primär eine datenschutzrechtliche und keine strafrechtliche Problematik. Hinzu kommt, dass die konkrete Ausgestaltung eines ausländischen Zugriffs sowie die Möglichkeiten sich dagegen juristisch zur Wehr zu setzten, primär nach ausländischem Recht zu beurteilen sein dürfte.

The third bullet contains the key statement and reads: "In the opinion of the public prosecutor's office, the calculation of the risk of foreign

[138] See the Datatilsynet decision of July 14, 2022 re Helsingør Kommune (Case 2020-431-0061) (https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jul/datatilsynet-nedlaegger-behandlingsforbud-i-chromebook-sag-, archived at https://perma.cc/3Q4N-V8CD).

lawful access appears to be a suitable criterion for assessing the justifiability of outsourcing against a criminal law background. However, it is not possible for the Public Prosecutor's Office to review the result in the specific case, as this ultimately depends on the assessments of the individual calculation factors. These cannot be verified from the outside."

The Federal Chancellery referred to my method as "good practice" in its report on the use of cloud services in the Federal Government.[139] The report, which analysis the legal preconditions for Federal government bodies moving into the cloud, also comes to the conclusion that, as opposed to the statements made by some data protection authorities, a risk-based approach applies. The report also in several areas cites this FAQ.

The Swiss online magazine Republik.ch published a detailed report on the Swiss Federal Government using cloud-based services. It also discusses my method and the controversy surrounding the risk-based approach in Switzerland.[140]

In July 2023, two experts of the University of Basel Law School rendered an expert opinion on the constitutionally compliant use of M365 by municipalities in the Canton of Zurich.[141] The opinion concludes that my method can indeed fulfill its purpose from a fundamental rights perspective. To determine the probability of a possible violation, according to the report, risk analysis methods must necessarily be used, i.e., recourse must be made to elements of risk management, which is what my method does. The report states that so far *"no alternative method has been developed that allows for a comparably structured argumentation regarding the risk of lawful access under the CLOUD Act/SCA."* It further states that the guidelines and fact sheets of the data protection authorities do not really say what exactly needs to be done to assess the risks. The opinion raises in essence three reservations with regard to my method or its use in specific cases:

- Depending on how the Excel is filled out, it will not always be clear how the value of the assessment follows the stated reason for it. This is generally true. Attention should be paid to this when using the Excel.

---

139 Bundeskanzlei, Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung, Bericht in Umsetzung vom Meilenstein 5 der Cloud-Strategie des Bundesrates, 31. August 2022 (https://bit.ly/3gvwdAe referring to www.bk.admin.ch, archived at https://perma.cc/SP2Q-KVMB).

140 https://www.republik.ch/2022/09/02/zunehmend-bewoelkt, archived at https://perma.cc/9JUF-CKD2

141 The original expert opinion is available at https://www.rosenthal.ch/downloads/Gutachten-Schefer-Glass-M365.pdf; a version, together with an addendum, was published on Dezember 20, 2023, in Jusletter IT; since the expert opinion contains various false and misleading statements about US law, I published a public response to it on February 15, 2024 also in Jusletter IT, available at https://www.rosenthal.ch/downloads/Rosenthal_Cloud-Gutachten-Replik.pdf (all in German).

- The quality of the result depends on the quality of the experience data, and this can change. This is also true in principle. After all, the values used regularly include surcharges based on experience, as a precaution. The values are in turn based on empirical values that reflect the interest of US authorities in data from a canton. However, contrary to statements to that effect in the report, a causal link between the storage of data in the cloud and the interest of US authorities has not been demonstrated, because the interest is not based on where an authority has stored the data and the US authorities generally obtain this data more easily, successfully and quickly via legal assistance in the cases relevant to the CLOUD Act/SCA.
- There is a lack of binding criteria for carrying out a reassessment, as the assumptions made can change. This criticism was true with regard to the specific use of the method the authors had in mind, but has nothing to do with the method; it is a matter for the user. The method itself is carried out for a defined period of time; at the latest after this, the assessment must be repeated if the circumstances do not change beforehand.

See also Q47 on how the method developed over time.

### 39. What do data protection authorities think about the method?

You should ask them. They have largely been silent in public. What I can say is that my method is today widely used in Switzerland and abroad, and that there is in essence no real alternative. Also, there have been various projects where data protection and other authorities have ultimately accepted the method as part of the risk assessments undertaken (see also Q38).

I have the impression that some European data protection authorities are suspicious; it appears that they cannot believe that it is possible to "calculate" a foreign lawful access risk or to describe it in the form of a number. This seems to include the Swiss Federal Data Protection and Information Commissioner (see Q41). The Danish data protection authority apparently opposed the use of the method because it believes the risk of foreign lawful access must be zero (which I believe is wrong: Q42). I also have the impression that it misunderstood the meaning of the probability (see Q26 for more details).

The Data Protection Commissioner of the Canton of Zurich has also openly criticized my method and the risk-based approach altogether; given that for sensitive data, she believes no risk is acceptable ("not even if the probability of access is 0.0001 percent"), she concluded

that there is also no point in undertaking a risk assessment using my method.[142]

I offered each of the few data protection authorities that criticized the method or refused to accept to get an introduction in how it really works, because based on my experience they usually neither know about the method nor the underlying legal concepts. Unfortunately, none of these offers were accepted.

40. **Have there been any court decisions concerning your method?**

No, I am not aware of any. See also Q38 and Q39.

41. **The Swiss data protection authority criticized the use of your method in one particular case – can you comment?**

The Federal Data Protection and Information Commissioner (**FDPIC**) did not assess my method. In an opinion dated May 13, 2022, he critically comments on how Suva (the state-owned Swiss accident insurance company) applied it to their M365 project and raised doubts about whether the so-called "risk-based approach" (Q42) is available for international transfers under Swiss law.[143]

Many privacy professionals in Switzerland reacted with confusion and incomprehension to the FDPIC's statements which they considered misguided or outright wrong. To that end, the FDPIC published the response of Suva of June 9, 2022 alongside his own opinion. Suva explains why it believes the FDPIC is wrong[144] (note that Suva also involved me in their case[145]). The FDPIC did not take any regulatory action. He rather considers his statement to be a contribution to a public discussion not yet decided by the courts.[146] He later on followed-up in an interview, re-iterating his position.[147]

The FDPIC's move is not unusual. In my opinion, his comments were not intended for Suva, but rather as a message to the European Commission, which is currently considering the renewal of Switzerland's adequacy decision (and to other Federal bodies currently evaluating M365). He on various occasions made it clear that he does not want to

---

142 https://www.inside-it.ch/zuercher-datenschuetzerin-zum-cloudeinsatz-der-regierungsratsbeschluss-aendert-gar-nichts-20220930, archived at https://perma.cc/NTQ9-5EBM.

143 https://bit.ly/3VRW3hX referring to www.edoeb.admin.ch, archived at https://perma.cc/2PZ9-9PYT.

144 https://bit.ly/3D2vspZ referring to www.edoeb.admin.ch, archived at https://perma.cc/HR69-8DJD.

145 I making this statement for reasons of transparency; I am not disclosing any insights here.

146 https://www.edoeb.admin.ch/edoeb/en/home/latest-news/aktuell_news.html#1498496300, archived at https://perma.cc/NC9F-S7AG.

147 https://www.inside-it.ch/edoeb-vertrauen-behoerden-nur-auf-private-gutachten%2C-koennen-sie-sich-eine-blutige-nase-holen-20220928, archived at https://perma.cc/GYY9-9WVN.

create the impression that Switzerland is not in line with EU data protection law. This explains why he refers to the same (unconvincing) argument against the risk-based approach that is currently relied upon by EU data protection authorities (Q42). At the same time, the FDPIC is known for trying to keep all options open, which is why he did not rule out the risk-based approach, but simply raised doubts about it. A year ago, when the majority of the EU data protection authorities were in support of the risk-based approach, he also supported it. He did not initiate any proceeding against Suva, as this would have forced him to go into a legal dispute.[148] As opposed to some of his EU colleagues, the FDPIC is not acting for ideological, but rather opportunistic reasons on this point, which is why his position can change at any time.

Also, the FDPIC's Suva statement is not authoritative or otherwise legally binding. It does, of course, create "FUD" ("fear, uncertainty and doubt"). Yet, I am not aware of any cloud project in Switzerland that has been suspended, changed or stopped due to the FDPIC's statements. As far as I know, none my peer at other law firms are advising clients to change their approach. Regulatory action is not expected.

The FDPIC:

- considers it "doubtful" whether the "risk-based approach" is available under Swiss law for transfers to third countries without an adequate level of data protection; he does so by arguing that the corresponding provision of the Swiss DPA does not expressly mention to the risk-based approach (para. 26, 27);
- considers the probability of foreign lawful access determined by Suva (2.52 percent) to be too low, given that he believes that intelligence and national security authorities in the US have the ability to force US-based parent companies to search any and all customer data managed by its foreign affiliates and it is to be assumed that this is happening regardless of whether or not there is specific interest in Suva (para. 31-33);
- considers it questionable that Suva has determined the probability of foreign lawful access so precisely and has used figures that extrapolate it over several hundred years (para. 37).

With regard to the first point, the general opinion in Switzerland is that the risk-based approach is valid under Swiss law, has always been so and continues to be (see also Q42). The arguments cited by the FDPIC are generally considered far-fetched and wrong. If they were true, most transfers to the US and many other countries would become illegal. In the past, nobody ever claimed this to be the interpretation of the current Swiss DPA and it is clear that Swiss parliament did not

[148] It is, in fact, doubtful whether the FDPIC was even entitled to make such comments. He relied on Art. 31(1)(b) Swiss DPA, which allows him to comment on proposed laws and measures of the Federal government that are relevant for data protection.

want to change this with the revised Swiss DPA (to become law in September 2023). The risk-based approach is one of the fundamental principles of Swiss data protection law, and it continues to be so.

With regard to how to properly perform foreign lawful access risks, the FDPIC commented on Suva's use of my method. In my view, he was wrong on his key points:

- His criticism of Suva assessing the US CLOUD Act risk (para. 23) using Suva-specific criteria (para. 29 et seqq.) misses the point. He mixes up targeted lawful access and mass-surveillance and is apparently not taking into account several essential elements with regard to Section 702 FISA. Suva was correct in applying Suva-specific criteria (see Q28 and Q29).
- He mixes up Section 702 FISA and the US CLOUD Act. The two laws follow different procedures, have different guarantees and serve different purposes (see Q29 and Q31). Lawful access under the CLOUD Act is based on Art. 18(1) of the Cybercrime Convention of the Council of Europe and is – contrary to the FDPIC's statements (para. 18) – compatible with European procedures and guarantees (see Q31).
- The FDPIC believes the US CLOUD Act applies to companies in Switzerland if and because they are owned by a US company (para. 18). This is wrong. What counts is whether the US company has "control" of the data at issue, which often is not the case (see Q35 and Q32).
- The FDPIC apparently got confused about the meaning and the apparent precision of the percentage numbers and years that resulted from Suva's assessment (para. 37). The assessment period is five years only. The 903 years means that the statistical probability of a foreign lawful access occurring in the five year period is much smaller than the Suva building being destroyed by an earthquake. See also Q10, Q22 and Q23.

In a blog post on the FDPIC's statement, my peer David Vasella at WalderWyss commented as follows on this last point: *"David Rosenthal's form uses probability values not because there is a demand for accuracy, but for self-reflection in an otherwise emotional risk assessment (this is shown by the statement of the FDPIC) and as an instrument of risk communication. Of course, 'garbage in, garbage out' applies, but for which assessment does this not apply?"*[149]

Vasella further noted that the key question in the Suva case was, in fact, not dealt with by the FDPIC: *"It is true that certain basic principles of US law are deficient from a Swiss perspective. As long as they*

[149] https://www.edoeb.admin.ch/edoeb/en/home/latest-news/aktuell_news.html#1498496300, archived at https://perma.cc/NC9F-S7AG.

*are not applied in a specific case, however, these principles have no concrete significance and cannot lead to a violation of privacy, certainly not a serious one. The FDPIC has omitted examining this aspect – whether the deficient U.S. law applies – by arguing that there is no risk-based approach. This mixes up two questions: under what conditions are these laws applicable and what is their scope of applicability, and – if they are applicable – with what probability does an authority make use of them. Only the second question deserves the name 'risk-based approach.' The first question, however, should not be ignored."*

My method takes care of both questions (Q3).

I note that Suva continued using the cloud irrespective of the FDPIC's reaction, and in the last years, the FDPIC refrained from further comments as above.

## G. THE VALIDITY OF THE RISK-BASED APPROACH

### 42. Is the "risk-based" approach still valid for international transfers?

Since the European Commission's adequacy decision for the US, this topic is no longer discussed; the risk-based approach appears to be the accepted standard also for international transfers.

That was not always the case. This is what I wrote in 2022:

Yes, and most of my colleagues seem to agree. However, EU data protection authorities are currently trying to establish an interpretation of the GDPR where this is no longer the case.

The agenda is to (admittedly) force "big-tech" companies such as Google or Microsoft to offer their services entirely out of Europe and keep European data in Europe to the extent possible until the US has changed its mass-surveillance laws. This resulted in a number of decisions against their offerings (e.g., Google Analytics, Google Fonts, Google Chromebooks).

Although several of these decisions have been met with broad criticism and incomprehension because the offerings do not involve any relevant risk of problematic foreign lawful access, it is generally expected that various authorities will continue trying to push the GDPR beyond its limits until courts intervene (see Q44 on this point).

Notably, as one of my colleagues noted, a problem with this approach is that it can be considered a breach of the fundamental democratic principle of the *separation of powers*[150] – it is not up to the supervisory

[150] David Vasella, Dänemark: Verbot der Verwendung von Chromebooks und Google Workspace durch Gemeinden, in: datenrecht.ch, July 15, 2022 (in German, https://datenrecht.ch/daenemark-verbot-der-verwendung-von-chromebooks-und-google-

authorities to change the law because they believe they know it better – this is the task of parliament.

See Q44 for why I do not believe that the promised "Trans-Atlantic Data Privacy Framework" (aka "Privacy Shield 2.0") will change much.

I have not yet seen any convincing explanation why the risk-based approach should not apply also under Chapter V (or the Swiss DPA). The argument that the risk-based approach does not apply to international transfers because it is not expressly *mentioned* in Chapter V is not convincing, given that the entire GDPR is following the risk-based approach. There was never a need to mention it in each and any provision. In fact, even the definition of "personal data" provides for a risk-based approach without expressly stating so.[151] Because Chapter V relies on it, Chapter V must be risk-based, too.[152]

Calling for "zero-risk" interpretation is also inconsistent with other authority recommendations. As shown above (Q3), the EDPB recommendation on supplementary measures clearly provides for the risk-based approach and so does Clause 14 of the EU SCC.

The "Schrems II" decision does also not say otherwise. The CJEU only holds that Section 702 FISA and EO 12333 are not compatible with EU law *if and when they are applied* but the court. It is for the exporter to assess whether this will be the happen in a particular case. Notably, the "Schrems II" decision does not limit the circumstances that the exporter may be taken into consideration, and the CJEU does not say which level of confidence the exporter must achieve. Only if the result of this assessment is *not* satisfactory then supplementary measures are necessary on top of the EU SCC to achieve an adequate level of protection.

The risk-based approach is also valid when dealing with professional and official secrecy obligations under Swiss law (see the confirmation of the Basel-Stadt public prosecutor in Q38 and my scientific paper on this topic[153]). The level of protection of Swiss professional or official secrecy is usually considered stricter than the protection provided for by

---

workspace-durch-gemeinden/, archived at https://perma.cc/XVT3-W4TL, machine translation in English is available).

151 See Recital 26 of the GDPR referring to "means reasonably likely" to be used to identify a data subject.

152 If there are "no means reasonably likely to be used" by foreign authorities to identify the data subjects of a transfer because the probability of a lawful access is minimal, how can there be personal data? If there is no personal data, how can Art. 46 GDPR be violated? Apparently, the EU data protection authorities have seen this argument coming, which is why they started to change the definition of "personal data" by arguing that it is sufficient if *anybody* can identify the data subject ("absolute" approach), not only those who get access to the data ("relative" approach). However, the European Court of Justice has said in "Breyer" (C-582/14) and, most recently, in "OLAF" (T-384/20) that the relative, not the absolute approach applies.

153 David Rosenthal, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter 10. August 2020 (only available in German) (https://www.rosenthal.ch/downloads/Rosenthal-CloudLawfulAccess.pdf, https://www.rosenthal.ch/downloads/Rosenthal-CloudLawfulAccess-Anhang.pdf, archived at https://perma.cc/HF65-X8UY and https://perma.cc/J35T-QSWT).

the Swiss DPA. Hence, if the risk-based method is fine from a professional or official secrecy point of view, it must suffice also for data protection purposes. I have a few times heard the argument that official secrecy also requires a zero-risk approach based on the argument that the government (as opposed to a private company) cannot "accept" a risk to the detriment of its subjects of law. I do not believe this is correct.

I found it helpful to take the view of the data subject: For data subjects, a foreign lawful access to their personal data is nothing else than a breach of data security. Data security is about ensuring the confidentiality, integrity and availability of personal data. A lawful access is a breach of *confidentiality*. It is comparable to an *un*lawful access. Both events are to be avoided by the controller, with the main difference being that in a foreign *lawful* access, the data subject's personal data ends up in the hands of a foreign government. In the case of an *unlawful* access, the data may be with a cybercriminal. Even the "zero-risk" proponents believe that the GDPR does *not* require data security to be perfect; they accept the "risk-based" approach when it comes to data security (Article 32 GDPR). Yet, they have never been able to explain why for the very same problem, Chapter V allegedly provides for an entirely different approach, i.e. why transfers need to provide *perfect* data security when it comes to foreign lawful access. For the same reasons, I also do not see why the official secrecy obligations of public bodies require a zero-risk approach.[154]

The inconsistencies in their logic do not end there. The proponents of the "zero-risk" approach seem to overlook that international "transfers" are not only possible under Chapter V, but also under Article 32 GDPR, where the risk-based approach undisputedly applies. Article 32 GDPR and not Chapter V seems to apply whenever data is transferred by a company in the EEA to a *branch* in the US.[155] Does this mean that in those cases of "transfers" the risk-based approach can be used, but not so in cases of transfers under Chapter V, even though in both cases the data ends up in the US?

This could lead to the following practical solution: All European exporters set up branches in the US for transferring their data across the ocean to the US (which is not subject to Chapter V but only Art. 32 GDPR), and then have their branches in the US onward forward the da-

---

154 It is accepted that a government does not have to undertake unreasonable measures simply to reduce the risk of a breach of data security to zero. It is accepted that that it suffices if the government acts diligently in protecting its data, it being understood that this will never result in 100 percent protection. This is true with cybersecurity as well as with physical security (doors, windows of buildings). I do not see why different standards should apply when it comes to protecting against foreign lawful access than when securing against unlawful access.

155 European Data Protection Board, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, adopted on November 18, 2021, para. 15 et seq. (https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en, archived at https://perma.cc/DQ3E-PUR8).

ta to its final destination. While this onward transfer is subject to Chapter V, it can be easily shown that such onward transfers within the US are not subject to Section 702 (Q29). All problems would be solved …

Not quite! A very clever colleague of mine argued that in the above example one could consider an EEA company with a branch in the US to be located (also) in the US, which means that every transfer to such EEA company would already be subject to Chapter V – even if occurring entirely within the EEA. His point is valid. It, however, makes the situation even worse, because a large number of EEA companies have branches in third countries (including the US) or have employees (or other persons pursuant to Article 29 GDPR) working from home offices and other locations in such countries. The logic would apply to all of them. This means that the next time you make available personal data under the GDPR to a controller or processor within the EEA, you first have to make sure that this recipient does not have any such foreign branch or foreign workers. Otherwise, you are in deep trouble, because you would – strictly speaking – have to put in place contractual safeguards and perform a transfer impact assessment, which you will find difficult to do accomplish. I am sure that if I were to ask the EU data protection authorities about how to deal with this situation, they would probably recommend me taking a risk-based approach.

In my view, this shows how absurd the discussion initiated by the EU data protection authorities currently is. Apart from that, if they were right, many applications in real life would simply no longer be possible. This could explain why they are currently enforcing more or less only against the "big tech" applications, but not against intra-group data transfers of other companies, scientists or other widespread applications.

But maybe, after all, the "zero-risk" approach of EU data protection authorities is simply the result of a misunderstanding (see Q43 on that).

What can companies do in this awkward situation when they realize that it is not reasonably possible to comply with the international data transfer rules advocated by the EU data protection authorities? When asked this question in a public discussion, the head of the Liechtenstein data protection authority, Marie Louise Gächter, gave the advice to take a risk-based approach in complying with Chapter V of the GDPR.[156] Hence, the risk-based approach exists, in one way or another, and most seem to do exactly as recommended. And Stefan Brink, head of the German data protection authority in Baden-Württemberg, recently summarized the manner in which the GDPR is currently being applied: "This is not how the GDPR was intended".[157]

---

156 6. Datenschutzrechtstagung, Das Risiko im Datenschutz, Schweizer Forum für Kommunikationsrecht, May 25, 2022, Zurich, Switzerland.

157 Stefan Brink, Jan Oetjen, Rolf Schwartmann, Axel Voss, So war die DSGVO nicht gemeint, Frankfurter allgemeine Zeitung, July 18, 2022

See also Q44 on possible outcomes.

43. **Is the debate about the "zero-risk" approach the result of a misunderstanding?**

Again, this discussion is more or less over following the adequacy decision for the US Data Privacy Framework by the European Commission in 2023.

My response from 2022:

This may be the case. I believe there is a misunderstanding as to what "risks" we are talking about.

When reading decisions of some EU data protection authorities, they state that the "risk-based" approach is not valid, but they do not explain what exactly they mean when referring to it.

Let's start looking at what they believe is happening whether personal data is transferred to the US. At least some of them believe that whenever personal data gets into the hands of a US cloud or Internet provider, the US government *is* entitled to access any data they have. Some even go as far in believing that Section 702 FISA (or the US CLOUD Act) also entitles the US government to access any data held by their European subsidiaries. The latest decision of a German procurement authority is evidence of such belief[158] and so are the statements of the Swiss data protection authority (Q41).

While this is all not true (see Q29 and Q32), I can understand why an authority with the aforementioned belief comes to the conclusion that transferring data to such US providers is prohibited under "Schrems II". Hence, if an exporter tells such an authority that even though a US-based provider is involved, the exporter still has no reason to believe that the US government can access the data, the authority will of course disagree. Instead, it will believe that the exporter has come to this conclusion only on the basis that the US government is *not interested* in the particular exporter at issue.

I suspect that *this* what some data protection authorities consider being the "risk-based" approach. From discussions I had with data protection authorities (e.g., the BayLDA), they argue that in the case of mass-surveillance it is irrelevant whether the US government is interested in a particular exporter. On this basis they reject any transfer impact assessment that involves a US provider because they cannot

---

(https://www.faz.net/aktuell/wirtschaft/digitec/so-war-die-dsgvo-nicht-gemeint-was-bei-ihrer-anwendung-schieflaeuft-18179521.html#void, archived at https://perma.cc/ZD6S-CJKU).

158 See Vergabekammer Baden-Württemberg, Decision of July 13, 2022 (1 VK 23/22) (the decision is no longer available; more on the decision is here https://steigerlegal.ch/2022/07/26/daten-export-usa-europa/, archived at https://perma.cc/PG87-C2RR).

imagine how personal data accessible to such US provider cannot be subject to a Section 702 FISA request.

In my view, these authorities are legally wrong on this point, too, because they seem to misunderstand how US lawful access laws work. But let's rather focus on another point, which is whether it is correct to qualify this way of thinking of such data protection authorities as a "zero-risk" approach.

I believe it is not correct. These authorities themselves do not refer to it as a "zero-risk" approach. They know exactly that there is no such thing as "zero-risk" in life. They rather refer to their view as the "rights-based" approach, which is a more suitable term in my view. They are asking: Can Section 702 FISA apply to a particular set of personal data transferred to the US?

In their view, this question has to be answered by an analysis of US law. In *theory*, this is a simple task. If the answer of the analysis is no, then the transfer is permitted. The key *practical* question is, however, how *confident* must the person answering the question be? Does the person have to be 100 percent sure with not even the slightest chance that a court or authority will come to a different conclusion?

I assume that everybody will agree that such absolute certainty will never exist in a legal assessment and, thus, never be required. Hence, if an assessor concludes that Section 702 FISA is not applicable to a particular use case and is, say, 90 percent convinced to be right, then I assume that everybody will agree that this is a result that is as reliable as it can get. There is still a 10 percent residual risk that a court may come to a different conclusion, but in my understanding this kind of residual risk in legal assessments is *not* what the EU data protection authorities are concerned about. They are part of the normal life of every lawyer.

This resolves the *first key misunderstanding* between the proponents of the rights-based approach and those of the risk-based approach: Even when applying the rights-based approach, a residual risk is acceptable. It is the residual risk that the analysis of US law (as to whether Section 702 FISA can apply in a particular case) has been wrong. I note that my method covers this aspect and helps calculating the level of confidence in the legal analysis (see Q10, Q20).

Now, what is the "risk-based" approach really about? The "risk-based" approach goes a step further than what the data protection authorities refer to as the "rights-based" approach. It does not ask whether Section 702 FISA *can* apply to a particular set of personal data transferred to the US. It asks whether it *will* be applied. This is also what Clause 14 of the EU SCC requires the parties to assess.

When answering to this question, more factors can be taken into consideration than in a purely legal analysis. Here, factors such as the interest of the US government in certain types of communications or the

lack thereof can be considered. Also, past experience can be taken into account. It can also be considered whether the parties involved are or can be targets of the US government, because if they cannot, this has an impact on whether Section 702 FISA will be applied in a manner that will result in the acquisition of personal data by the US government.

This is the *second key misunderstanding*. The risk-based approach is not tolerating personal data to become acquired by the US government, but it rather takes into account factors other than only legal factors. My method supports this type of assessment, as well. I believe, for reasons detailed in Q42, why I believe this risk-based approach is valid. I also do not see any statement in the "Schrems II" decision of the CJEU that prohibits considering any circumstances that will help answering the question; in fact, I believe it is precisely what the CJEU had in mind.

What is important, though, is that the assessor documents why a particular conclusion has been reached. I see many cases where this is unfortunately not done, with exports complaining about data protection authorities rejecting their assessments. To me, this appears to be one of the fundamental problems in the current discussion – the lack of understanding of what we are talking about, and what we are doing in assessing the risks.

While all of the foregoing will not make any difference and likely be ignored by those EU data protection authorities that pursue an ideological "agenda" in terms of international transfers (Q42), I do hope that at least some of the others will be ready to bring the discussion to a new level in order to find workable solutions and common grounds.

### 44. Is Privacy Shield 2.0 the solution? What other developments do you see coming?

Here, for the record, my response from 2022:

The easiest solution would be the European Court of Justice (**CJEU**) ruling on a case that will put to an end the current hysteria about international transfers. This appears to be still some years away, though, and since the CJEU's decisions are often political, as well, it is not entirely clear how it would resolve the situation without letting US providers "off-the-hook". I do hope, though, that the CJEU will stop the EU data protection authorities in their current attempt to broaden the definition of personal data, as this attempt violates existing CJEU case law.[159]

I originally had doubts that the new EO 14086 (see Q29a) will change much, given that it raises a number questions (such as being only a

[159] See footnote 152.

presidential directive, only covering "signals intelligence" and not being specific as to how the US authorities will interpret the term "proportionate"). It is also likely that Maximilian Schrems and his NGO NOYB.eu will challenge the new efforts, which they referred to as a "pig with a lipstick".[160] I meanwhile believe that the pressure to resolve the situation the data protection authorities created in the wake of the "Schrems II" decision is so big that they and in any event the European Commission may see the EO 14086 as a face-saving opportunity to get out of their corner. See Q29a on how this could work out.

Of course, the EU data protection authorities could also get reasonable again, start studying US lawful access laws, my and other method for transfer impact assessments and listen to experts on why the risk-based approach is valid under the GDPR and Swiss DPA. And they could start thinking about the fact that their zero-risk approach is a dead end. As David Vasella rightfully commented on his blog, *"a consistent zero-risk approach would lead to the collapse of the Swiss economy. Not only would there be no more Teams calls - there would also be no global corporations and no international cancer research. There is no realistic alternative for international data transfers. A zero-risk approach takes the entire economy hostage to political wrangling, arguing that the US under certain conditions – which are not examined![161] – can access certain categories of data too extensively."* [162]

This, however, seems for political and other reasons not very likely. The following developments are in my view more likely to solve the problem – in addition to the new EO 14086:

- US-based providers will increasingly provide their services exclusively out of Europe. Cloud services will lead the effort with other services following. The big three hyperscalers Microsoft, Google and AWS have already begun doing so. Note, however, that they may eventually stop short of promising in their contracts that no access to customer data will be possible or happen from outside the EEA, UK or Switzerland. For example, Microsoft's "EU Data Boundary" will apparently not really mean that there is no transfer of personal data to the US or other regions of the world. It only means that non-EU-access will only happen via remote access (and not by "physically" transferring data outside Europe):[163]

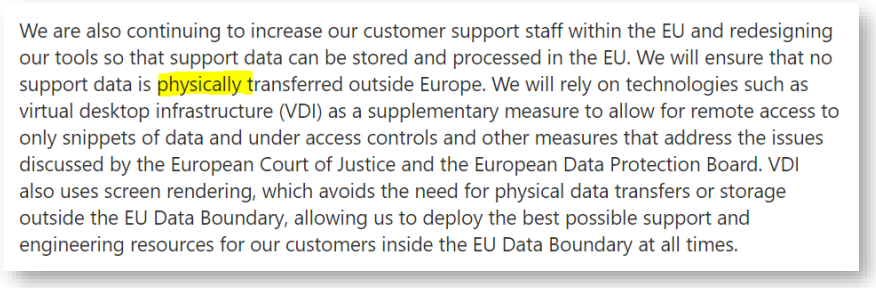
---

160 See https://noyb.eu/en/open-letter-future-eu-us-data-transfers (archived at https://perma.cc/YHG5-9SQ9) and https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems (archived at https://perma.cc/F3T3-FWZ5).

161 Referring to the Swiss data protection authority FDPIC, which in a particular case itself criticized the involvement of a US provider even though it did itself not examine whether any lawful access could actually occur (Q41).

162 David Vasella, EDÖB: Zweifel am risikobasierten Ansatz, in: datenrecht.ch, June 13, 2022 (in German, https://datenrecht.ch/edoeb-zweifel-am-risikobasierten-ansatz/, machine translation in English is available, archived at https://perma.cc/B3Z5-X7D8).

163 https://blogs.microsoft.com/eupolicy/2021/12/16/eu-data-boundary-for-the-microsoft-cloud-a-progress-report/, archived at https://perma.cc/6MX3-ELUJ.


We are also continuing to increase our customer support staff within the EU and redesigning our tools so that support data can be stored and processed in the EU. We will ensure that no support data is physically transferred outside Europe. We will rely on technologies such as virtual desktop infrastructure (VDI) as a supplementary measure to allow for remote access to only snippets of data and under access controls and other measures that address the issues discussed by the European Court of Justice and the European Data Protection Board. VDI also uses screen rendering, which avoids the need for physical data transfers or storage outside the EU Data Boundary, allowing us to deploy the best possible support and engineering resources for our customers inside the EU Data Boundary at all times.

While the "zero-risk" approach also clearly prohibits such "remote access only" setups, I would not be surprised if the EU data protection authorities were to seize the opportunity to give up their radical approach and at least pretend that offerings such as the "EU Data Boundary" are sufficient, which they usually are under a risk-based approach.

- Another development that I am already seeing in specific cloud projects is that the data protection authorities formally oppose the "risk-based" approach and my method, but de facto accept it under a different label. This is done in two steps:
  - First, they redefine the "risk-based" approach to be an approach where one exclusively relies on the practical past lawful access experience of a provider. This is what many providers do, but it is *not* my method. They refer to this as an "exclusively" or "absolute" risk-based approach.
  - Second, they propose a "compromise" approach that in addition also takes into account the law in the country of the importer to decide whether there is reason to believe that a problematic lawful access can happen. This is *precisely* what my method does. See also Q43 on this.
- Most companies and public institutions will simply proceed on the basis of the "risk-based" approach and the supervisory authorities will not intervene, at least in the case of private sector organizations where there is no complaint. Everybody will get used to it and the problem will silently go away over the next few years.
- Most companies and public institutions will no longer directly contract with US-based providers but rather with their European subsidiaries, meaning that these subsidiaries take over the primary responsibility for complying with Chapter V of the GDPR. This will mean that regulatory intervention will primarily have to focus at these providers and not their customers. These providers will take decisions to court, where the issue will hopefully be resolved in a few years from now. Yet, I do see signs of some authorities undermining this approach by claiming that contracting

with the European subsidiary of a US-based provider can already be considered a violation of Chapter V of the GDPR.[164]

## H. VARIOUS QUESTIONS

### 45. Can I create my own version of the form?

Yes. While I reserve all rights in the spreadsheets I have created and in the method, I have made them available under the free Creative Commons "Attribution-ShareAlike 4.0 International" license. This means you are not only allowed to copy and redistribute the material in any medium or format, you are also allowed to remix, transform, and build upon the material for any purpose, even commercially. This is under the following two terms:

- **Attribution:** You must give appropriate credit to me and the "home" of the method,[165] provide a link to the license (which is included in the spreadsheet), and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests that I endorse you or your use.
- **ShareAlike:** If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

Note that the "blue" input fields (i.e. those with the blue background) and sample text in the spreadsheets are not subject to the license and may be changed and shared without applying the same license. This means that if you complete the form for your transfer or project, you can ensure its confidentiality even if you share it.

With the license, you are free to create translations of the spreadsheets, improve them or make changes to better suit your needs. Of course, I would appreciate if you let me know about the changes or translations you may have done, but technically you are not required to inform me.

If you need a different license, contact me at david@rosenthal.ch.

### 46. Do you offer professional advice in using the form?

Yes, of course, but so do a number of my colleagues in other law firms in Switzerland and abroad. While at my firm, VISCHER, my team and I do advise on GDPR matters, we will not advise on local law. All information we provide concerning on foreign law is for informational pur-

---

164 See Vergabekammer Baden-Württemberg, Decision of July 13, 2022 (1 VK 23/22) (the decision is no longer available; more on the decision is here https://steigerlegal.ch/2022/07/26/daten-export-usa-europa/, archived at https://perma.cc/PG87-C2RR).

165 Attribution must also include reference to the link where the original and master version of this file can be obtained at www.rosenthal.ch.

poses only. We work with various fine law firms around the world for getting local law advice.

You will also find a lot of information in these FAQ and the detailed instructions and other explanations contained in the files that I have made available in connection with my method. If you take your time to study these materials (and maybe some of the other publications I have made available on my personal homepage), you will be able to use my method on your own.

For data protection authorities, I offer online workshops to present and discuss the method at no cost. Just send me an email.

47. **Why did you create this method? How did it develop over time?**

It all started in 2019. A large Swiss bank asked me to advise them on the technical and organizational measures needed for lawfully storing client data in the cloud.

At that time, nobody had a clear (and defensible) answer to the question. I found it difficult to provide an answer in a traditional legal opinion because the problem had too many "moving parts": There were technical factors to consider as well as legal aspects of both US and Swiss law. I had the idea of using a spreadsheet to connect all these risk factors. This would also allow me to try out how they would interact with each other in various configurations and combinations. I familiarized myself with probability calculations and found that they were the right way to combine all pieces of the puzzle and understand the big picture. This was the birth of my method.

The bank – and in particular its management – was pleased with the approach for two reasons: First, it produced a number, not some vague lawyer wording. Second, it allowed them to "play around" with the various measures and test their impact.

The bank decided to proceed with their cloud project and I started to test the method with other clients. I continuously expanded and improved it and added new features. One of my clients, a pan-European insurance group, arranged for their actuarian to help me convert the residual risk percentage in "years", which made it easier for some to get a "feeling" of risk assessment's result.

In July 2020, the European Court of Justice rendered the "Schrems II" decision and I included into my spreadsheet a section for assessing the risk of foreign mass-surveillance as discussed in the court's decision.

In August 2020, I published method together with a scientific paper on cloud projects from a professional secrecy point of view and under which conditions they are possible under Swiss law. The article also explained the method. The spreadsheet was made available under a free open-source license for everyone to use; I also did not include my firm logo. This would allow the method to be used by other law firms,

be peer-reviewed and improved. My idea was to provide the privacy community with a means to solve a problem that everybody was struggling with. For many years, I have been freely sharing my know-how with the community (see also https://www.rosenthal.ch/).

One of the frequently cited benefits of the method was that it allowed people to look at the risk of foreign lawful access more objectively and with fewer emotions (see, for example, an interview with Microsoft's National Technology Officer in October 2020).

An increasing number of companies, many of them Swiss banks, got interested in the method and started to use it – some on their own, some with my help. My team and I continued to use it in client projects, both in the financial industry and the public sector. So did other law firms and advisors in the Swiss market, including at the "Big Four". The method became more and more popular in Switzerland and others began citing it, for example Daniel Hürlimann and Martin Steiger in their report about cloud services for Swiss law firms. However, till then, the focus was always professional (and official) secrecy under Swiss law, not data protection.

This changed in Summer 2021 when I – during my usual weekend jogging run with my dog – had the idea to use my method for solving the problem created by the "Schrems II" decision. Across Europe there was the need for such a tool to perform a meaningful "Transfer Impact Assessment", i.e. analyzing whether a transfer of personal data to the US could trigger problematic foreign lawful access. By then, I felt that nobody in Europe had a reasonable and convincing solution for this problem – except for having foreign law firms writing expensive legal opinions in each single case. This was not feasible, in particularly not for small and medium enterprises.

On August 1, 2021 I released a draft for public comment of a Transfer Impact Assessment based on my method. It focused exclusively on the issues raised by the "Schrems II" decision. My new spreadsheet immediately received a lot of attention across Europe. The International Association of Privacy Professionals (IAPP), the worldwide largest privacy association, became aware of this and asked me for my permission to include my tool in their official online resources. They created IAPP-branded versions of both implementations and published them on September 1, 2022 (see report on this on datenrecht.ch). This further increased the popularity of my method outside Switzerland. I am regularly receiving feedback from users across Europe. The Dutch government published various risk assessments based on my method. Others asked me for permission to translate it into local languages.

Over time, I continuously expanded the offering. I added new country-specific versions of the Transfer Impact Assessment for India, China and Russia (with the help of local counsel and clients), I added addi-

tional tools and questionnaires and other law firms contributed materials to the open-source tool set, as well.

Another big step happened on March 30, 2022 when the Canton of Zürich officially declared my method standard for all cloud government projects in the canton, after itself having performed a foreign lawful access risk assessment using the method with various stakeholders. This recognition triggered other cantons to follow suit. In the following, there were various other recognitions of the method.

Yet, there also have been less supportive developments. A number of EU data protection authorities have been embarking on a mission to prevent data transfers to the US as much as possible and force "big tech" companies to offer their solutions entirely out of Europe (see my position in Q42); this made it pointless to undertake any risk assessment in the first place.

Another less supportive development was the publication of the Swiss Federal Data Protection and Information Commissioner (**FDPIC**) in the matter of Switzerland's state-owned accident insurance Suva. They used my method on their own for a cloud project, which he criticized. As one commentator noted, the FDPIC missed the point on several aspects. I was not surprised though (see Q41 why). Other authorities did take the time to scrutinize my approach carefully and came up with a different view. Most notable is the Public Prosecutor's Office of the Canton of Basel-Stadt (Switzerland), which in essence confirmed the suitability of my approach under Swiss law (see Q38).

Following the adequacy decisions for the US in 2023 and 2024, I had the impression that the need for the method diminished to a certain extent given that many organizations had successfully taken their decisions on how to use cloud offerings from US-based providers such as Microsoft, Google and AWS. However, there are three developments that are worth being mentioned:

- There has been an increased interest in undertaking foreign lawful access assessments for outsourcings within Europe (example: A Swiss bank outsources certain activities that are subject to banking secrecy to a provider based in Germany). As opposed to that, most initial assessments were focused entirely on the US.
- I have developed a "light" version of the method that can be completed within five minutes. It is based on asking eight questions to identify standard provider situations that permit standard assessments. This can help an organization to handle large amounts of use cases.
- Most recently, my team received various requests on how to deal with the uncertainties under the Trump administration since early 2025. This is why I have developed the latest multi-scenario version of the method.

48. **Why do you do all this work and provide your know-how for free?**

This is a question I ask myself from time to time (and my family, too).

Some of my work is paid by clients who are looking for a solution to their problems. I like in particular problems for which nobody else has found a good solution so far (and there are enough). Since most data protection authorities (and also some lawyers) only tell people what is *not* possible, people describe me as somebody who has an intrinsic motivation in *solving problems* rather than just pointing to them.

If you read my books, scientific papers and articles you know that I do not only raise questions, but usually offer answers, even if this means taking a controversial position and speak-up. See my blog post on Google Analytics as a recent example.

The clients usually agree to have the work published and made available for free because they themselves benefit from the effects of the publication. This way, the work gets scrutinized and can improve and if the community likes the solution that I proposed and adopts it, it becomes a standard, which helps everybody – including my clients. I am also making mistakes, and publishing my work helps me identify them.

I do commercially benefit from all the uncertainty and confusion created by the data protection authorities concerning international transfers. I even benefitted from the skeptical reaction of the Swiss data protection authority (Q41) because this caused several clients to ask (and pay) me for advice. Still, I believe the development is going into the wrong direction. I believe that in particular some "ideological" EU data protection authorities are causing considerable collateral damage. And I am not alone.[166] This is why I feel it is necessary to counteract.

I have been sharing my know-how extensively for over 20 years (see, e.g., https://www.rosenthal.ch and https://dsat.ch) and found it to work very well. While sharing know-how also has a positive marketing effect and contributes to my professional reputation, it first above all helps "fueling" the discussion and application of data law in Switzerland and abroad, which again helps me and my peers in our job in finding reasonable solutions to the problems of our clients. After all, we do not want to rely on guidance by the supervisory authorities only.

---

166 See, for example, Stefan Brink, Jan Oetjen, Rolf Schwartmann, Axel Voss, So war die DSGVO nicht gemeint, Frankfurter allgemeine Zeitung, July 18, 2022 (https://www.faz.net/aktuell/wirtschaft/digitec/so-war-die-dsgvo-nicht-gemeint-was-bei-ihrer-anwendung-schieflaeuft-18179521.html#void, archived at https://perma.cc/ZD6S-CJKU).