Understanding why the first pieces fell in the Transatlantic transfers domino

By Gabriela Zanfir-Fortuna

The Austrian DPA and the EDPS decided EU websites placing US cookies breach international data transfer rules

Two decisions issued by Data Protection Authorities (DPAs) in Europe and published in the second week of January 2022 found that two websites, one run by a contractor of the European Parliament (EP), and the other one by an Austrian company, have unlawfully transferred personal data to the US merely by placing cookies (Google Analytics and Stripe) provided by two US-based companies on the devices of their visitors. Both decisions looked into the transfers safeguards put in place by the controllers (the legal entities responsible for the websites), and found them to be either insufficient – in the case against the EP, or ineffective – in the Austrian case.

Both decisions affirm that all transfers of personal data from the EU to the US need "supplemental measures" on top of their Article 46 GDPR safeguards, in the absence of an adequacy decision and under the current US legal framework for government access to personal data for national security purposes, as assessed by the Court of Justice of the EU in its 2020 *Schrems II* judgment. Moreover, the Austrian case indicates that in order to be effective, the supplemental measures adduced to safeguard transfers to the US must **"eliminate the possibility of surveillance and access [to the personal data] by US intelligence agencies"**, seemingly putting to rest the idea of the "risk based approach" in international data transfers post-*Schrems II*.

This piece analyzes the two cases comparatively, considering they have many similarities other than their timing: they both target widely used cookies (Google Analytics, in addition to Stripe in the EP case), they both stem from complaints where individuals are represented by the Austrian NGO *noyb*, and it is possiblethat they will be followed by similar decisions from the other DPAs that received a batch of 101 complaintsin August 2020 from the same NGO, relying on identical legal arguments and very similar facts. This piece analyzes the most important findings made by the two regulators, showing how their analyses were in sync and how these analyses likely preface similar decisions for the rest of the complaints.

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

In the first decision, the European Data Protection Supervisor (EDPS) investigated a complaint made by several Members of the European Parliament against a website made available by the EP to its Members and staff in the context of managing COVID-19 testing. The complainants raised concerns with regard to transfers of their personal data to the US through cookies provided by US based companies (Google and Stripe) and placed on their devices when accessing the COVID-19 testing website. The case was brought under the Data Protection Regulation for EU Institutions (EUDPR), which has identical definitions and overwhelmingly similar rules to the GDPR.

One of the key issues that was analyzed in order for the case to be considered falling under the scope of the EUDPR was whether **personal data** was being **processed** through the website by merely placing cookies on the devices of those who accessed it. Relying on its 2016 Guidelines on the protection of personal data processed through Web Services, the EDPS noted in the decision that "**tracking cookies**, such as the Stripe and Google Analytics cookies, are considered personal data, **even if the traditional identity parameters of the tracked users are unknown or have been deleted by the tracker after collection**". It also noted that "all records containing identifiers that can be used to single out users, are considered as personal data under the Regulation and must be treated and protected as such".

The EP argued in one of its submissions to the regulator that the Stripe cookie "had never been active, since registration for testing for EU Staff and Members did not require any form of payment". However, the EP also confirmed that the dedicated COVID-19 testing website, which was built by its contractor, copied code from another website run by the same contractor, and "the parts copied included the code for a cookie from Stripe that was used for online payment for users" of the other website. In its decision, the EDPS highlighted that "upon installation on the device, a cookie cannot be considered 'inactive'. Every time a user visited [the website], personal data was transferred to Stripe through the Stripe cookie, which contained an identifier. (…) **Whether Stripe further processed the data transferred through the cookie is not relevant**".

With regard to the Google Analytics cookies, the EDPS only notes that the EP (as controller) acknowledged that the cookies "are designed to process 'online identifiers, including cookie identifiers, internet protocol addresses and device identifiers' as well as 'client identifiers'". The regulator concluded that personal data were therefore transferred "through the above-mentioned trackers".

In the second decision, which concerned the use of Google Analytics by a website owned by an Austrian company and targeting Austrian users, the DPA argued in more detail what led it to find that personal data was being processed by the website through Google Analytics cookies, under the GDPR.

1.1 Cookie identification numbers, by themselves, are personal data

The DPA found that the cookies contained identification numbers, including a UNIX timestamp at the end, which shows when a cookie was set. It also noted that the cookies were placed either on the device or the browser of the complainant. The DPA affirmed that relying on these identification numbers makes it possible for both the website and Google Analytics "**to distinguish website visitors … and also to obtain information as to whether the visitor is new or returning**".

In its legal analysis, the DPA noted that "an interference with the fundamental right to data protection … already exists if certain entities take measures – in this case, the assignment of such identification numbers – to individualize website visitors". Analyzing the "identifiability" component of the definition of "personal data" in the GDPR, and relying on its Recital 26, as well as on Article 29 Working Party Opinion 4/2007 on the concept of "personal data", the DPA clarified that "a standard of identifiability to the effect that it must also be immediately possible

to associate such identification numbers with a specific natural person – in particular with the name of the complainant – **is not required**" for data thus processed to be considered "personal data".

The DPA also recalled that "**a digital footprint**, which allows devices and subsequently the specific user to be clearly individualized, constitutes personal data". The DPA concluded that **the identification numbers contained in the cookies placed on the complainant's device or browser are personal data**, highlighting their "uniqueness", their ability to single out specific individuals and rebutting specifically the argument the respondents made that no means are in fact used to link these numbers to the identity of the complainant.

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

However, the DPA did not stop here and continued at length in the following sections of the decision to underline why placing the cookies at issue when accessing the website constitutes processing of personal data. It noted that the classification as personal data "becomes even more apparent if one takes into account that the identification numbers can be combined with other elements", like the address and HTML title of the website and the subpages visited by the complainant; information about the browser, operating system, screen resolution, language selection and the date and time of the website visit; the IP address of the device used by the complainant. The DPA considers that "**the complainant's digital footprint is made even more unique following such a combination [of data points]**".

The "anonymization function of the IP address" – which is a function that Google Analytics provides to users if they wish to activate it – was expressly set aside by the DPA, considering that during fact finding it was shown the function was not correctly implemented by the website at the time of the complaint. However, later in the decision, with regard to the same function and the fact that it was not implemented by the website, the regulator noted that **"the IP address is in any case only one of many pieces of the puzzle of the complainant's digital footprint"**, hinting therefore that even if the function would have been correctly implemented, it wouldn't have necessarily led to the conclusion that the data being processed was not personal.

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

Drilling down even more on the notion of "identifiability" in a dedicated section of the decision, the DPA highlights that in order for the data processed through the cookies at issue to be personal, "it is not necessary that the respondents can establish a personal reference on their own, i.e. that all information required for identification is with them. […] Rather, **it is sufficient that anyone, with lawful means and justifiable effort, can establish this personal reference**". Therefore, the DPA took the position that "**not only the means of the controller [the website in this case] are to be taken into account in the question of identifiability, but also those of 'another person'**".

After recalling that the CJEU repeatedly found that "the scope of application of the GDPR is to be understood very broadly" (e.g. C-439/19 *B*, C-434/16 *Nowak*, C-553/07 *Rijkeboer*), the DPA

nonetheless stated that in its opinion, the term "anyone" it referred to above, and thus the scope of the definition of personal data, "should not be interpreted so broadly that any unknown actor could theoretically have special knowledge to establish a reference; this would lead to almost any information falling within the scope of application of the GDPR and a demarcation from non-personal data would become difficult or even impossible".

This being said, the DPA considers that the "decisive factor is whether identifiability can be established with a justifiable and reasonable effort". In the case at hand, the DPA considers that there are "**certain actors who possess special knowledge that makes it possible to establish a reference to the complainant and identify him**". These actors are, from the DPA's point of view, certainly the provider of the Google Analytics service and, possibly the US authorities in the national security area. As for the provider of Google Analytics, the DPA highlights that, first of all, the complainant was logged in with his Google account at the time of visiting the website.

The DPA indicates this is a relevant fact only "if one takes the view that the online identifiers cited above must be assignable to a certain 'face'". The DPA finds that such an assignment to a specific individual is in any case possible in the case at hand. As such, the DPA states that: "[…] if the identifiability of a website visitor depends only on whether certain declarations of intent are made in the account (user's Google account – *our note*), then, from a technical point of view, all possibilities of identifiability are present", since, as noted by the DPA, otherwise Google "could not comply with a user's wishes expressed in the account settings for 'personalization' of the advertising information received". It is not immediately clear how the ad preferences expressed by a user in their personal account are linked to the processing of data for Google Analytics (and thus website traffic measurement) purposes, and it seems that this was used in the argumentation to substantiate the claim that the second respondent generally has additional knowledge across its various services that could lead to the identification or the singling out of the website visitor.

However, following the arguments of the DPA, on top of the autonomous finding that cookie identification numbers are personal data, it seems that even if the complainant wouldn't have been logged into his account, the data processed through the Google Analytics cookies would have still been considered personal. In this context, the DPA "expressly" notes that "the wording of Article 4(1) of the GDPR is unambiguous and is linked **to the ability to identify and not to whether identification is ultimately carried out"**.

Moreover, **"irrespective of the second respondent"** – so even if Google admittedly did not have any possibility or ability to render the complainant identifiable or to single him out, other third parties in this case were considered to have the potential ability to identify the complainant: US authorities.

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

Lastly, according to the decision, the US authorities in the national security area "must be taken into account" when assessing the potential of identifiability of the data processed through cookies in this case. The DPA considers that "intelligence services in the US take certain online identifiers, such as the IP address or unique identification numbers, as a starting point for

monitoring individuals. In particular, it cannot be ruled out that intelligence services have already collected information with the help of which the data transmitted here can be traced back to the person of the complainant."

To show that this is not merely a "theoretical danger", the DPA relies on the findings of the CJEU in Schrems II with regard to the US legal framework and the "access possibilities" it offers to authorities, and on Google's Transparency Report, "which proves that data requests are made to [it] by US authorities." The regulator further decided that even if it is admittedly not possible for the website to check whether such access requests are made in individual cases and with regard to the visitors of the website, "this circumstance cannot be held against affected persons, such as the complainant. Thus, it was ultimately the first respondent as the website operator who, despite publication of the Schrems II judgment, continued to use the Google Analytics tool".

Therefore, based on the findings of the Austrian DPA in this case, at least two of the "any persons" mentioned in Recital 26 GDPR that will be considered when deciding who can have lawful means to identify data so that the data is deemed personal are the processor of a specific processing operation, as well as the national security authorities that may have access to that data, at least in cases where this access is relevant (like in international data transfers). This latter finding of the DPA raises questions whether national security agencies in general in a specific jurisdiction may be considered by DPAs as an actor who has "lawful means" and additional knowledge when deciding if a data set links to an "identifiable" person, also in cases where international data transfers are not at issue.

The DPA concluded that the data processed by the Google Analytics cookies is personal data and falls under the scope of the GDPR. Importantly, the cookie identification numbers were found to be personal data by themselves. Additionally, the other data elements potentially collected through cookies together with the identification numbers are also personal data.

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

Once the supervisory authorities established that the data processed through Google Analytics and, respectively, Stripe cookies, were personal data and were covered by the GDPR or EUDPR respectively, they had to ascertain whether an international transfer of personal data from the EU to the US was taking place in order to see whether the provisions relevant to international data transfers were applicable.

The EDPS was again concise. It stated that because the personal data were processed by two entities located in the US (Stripe and Google LLC) on the EP website, "personal data processed through them were transferred to the US". The regulator strengthened its finding by stating that this conclusion "is reinforced by the circumstances highlighted by the complainants, according to which all data collected through Google Analytics is hosted (i.e. stored and further processed) in the US". For this particular finding, the EDPS referred, under footnote 27 of the decision, to the proceedings in Austria "regarding the use of Google Analytics in the context of the 101 complaints filed by noyb on the transfer of data to the US when using Google Analytics", in an evident indication that the supervisory authorities are coordinating their actions.

In turn, the Austrian DPA applied the criteria laid out by the EDPB in its draft Guidelines 5/2021 on the relationship between the scope of Article 3 and Chapter V GDPR, and found that all the conditions are met. The administrator of the website is the controller and it is based in Austria, and, as data exporter, it "disclosed personal data of the complainant by proactively implementing the Google Analytics tool on its website and as a direct result of this implementation, among other things, a data transfer to the second respondent to the US took place". The DPA also noted that the second respondent, in its capacity as processor and data importer, is located in the US. Hence, Chapter V of the GDPR and its rules for international data transfers are applicable in this case.

However, it should also be highlighted that, as part of fact finding in this case, the Austrian DPA noted that the version of Google Analytics subject to this case was provided by Google LLC (based in the US) until the end of April 2021. Therefore, for the facts of the case which occurred in August 2020, the relevant processor and eventual data importer was Google LLC. But the DPA also noted that since the end of April 2021, Google Analytics has been provided by Google Ireland Limited (based in Ireland).

One important question that remains for future cases is whether, under these circumstances, the DPA would find that an international data transfer occurred, considering the criteria laid out in the draft EDPB Guidelines 5/2021, which specifically require (at least in the draft version, currently subject to public consultation) that "the data importer is located in a third country", without any further specifications related to corporate structures or location of the means of processing.

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

After establishing that international data transfers occurred from the EU to the US in the cases at hand, the DPAs assessed the lawful ground for transfers used.

The EDPS noted that EU institutions and bodies "must remain in control and take informed decisions when selecting processors and allowing transfers of personal data outside the EEA". It followed that, absent an adequacy decision, they "may transfer personal data to a third country only if appropriate safeguards are provided, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available". Noting that the use of Standard Contractual Clauses (SCCs) or another transfer tool do not substitute individual case-by-case assessments that must be carried out in accordance with the Schrems II judgment, the EDPS stated that EU institutions and bodies must carry out such assessments "before any transfer is made", and, where necessary, they must implement supplemental measures in addition to the transfer tool.

The EDPS recalled some of the key findings of the CJEU in Schrems II, in particular the fact that "the level of protection of personal data in the US was problematic in view of the lack of proportionality caused by mass surveillance programs based on Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order (EO) 12333 read in conjunction with Presidential Policy Directive (PPD) 28 and the lack of effective remedies in the US essentially equivalent to those required by Article 47 of the Charter".

Significantly, the supervisory authority then affirmed that "**transfers of personal data to the US can only take place if they are framed by effective supplementary measures in order to ensure an essentially equivalent level of protection for the personal data transferred**". Since the EP did not provide any evidence or documentation about supplementary measures being used on top of the SCCs it referred to in the privacy notice on the website, **the EDPS found the transfers to the US to be unlawful.**

Similarly, the Austrian DPA in its decision recalled that the CJEU "already dealt" with the legal framework in the US in its Schrems II judgment, as based on the same three legal acts (Section 702 FISA, EO 12333, PPD 28). The DPA merely noted that "it is evident that the second respondent (Google LLC – *our note*) qualifies as a provider of electronic communications services" within the meaning of FISA Section 702. Therefore, it has "an obligation to provide personally identifiable information to US authorities pursuant to 50 US Code §1881a". Again, the DPA relied on Google's Transparency Report to show that "such requests are also regularly made to it by US authorities".

Considering the legal framework in the US as assessed by the CJEU, just like the EDPS did, the Austrian DPA also concluded that the mere entering into SCCs with a data importer in the US cannot be assumed to ensure an adequate level of protection. Therefore, **"the data transfer at issue cannot be based solely on the standard data protection clauses concluded between the respondents"**. Hence, supplementary measures must be adduced on top of the SCCs. The Austrian DPA relied significantly on the EDPB Recommendation 1/2020 on measures that supplement transfer tools when analyzing the available supplementary measures put in place by the respondents.

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

When analyzing the various measures put in place to safeguard the personal data being transferred, the DPA wanted to ascertain "whether the additional measures taken by the second respondent close the legal protection gaps identified in the CJEU [Schrems II] ruling – i.e. the access and monitoring possibilities of US intelligence services". Setting this as a target, it went on to analyze the individual measures proposed.

The **contractual and organizational supplementary measures** considered in the case:

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

The DPA considered that "it is not discernable" to what extent these measures are effective to close the protection gap, taking into account that the CJEU found in the Schrems II judgment that even "**permissible (i.e. legal under US law) requests from US intelligence agencies are not compatible with the fundamental right to data protection under Article 8 of the EU Charter of Fundamental Rights**".

The **technical supplementary measures** considered were:

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

With regard to encryption as one of the supplementary measures being used, the DPA took into account that a data importer covered by Section 702 FISA, as is the case in the current decision, "has a direct obligation to provide access to or surrender such data". The DPA considered that "this obligation may expressly extend to the cryptographic keys without which the data cannot be read". Therefore, it seems that as long as the keys are kept by the data importer and the importer is subject to the US law assessed by the CJEU in Schrems II (FISA Section 702, EO 12333, PPD 28), encryption will not be considered sufficient.

As for the argument that the personal data being processed through Google Analytics is "pseudonymous" data, the DPA rejected it relying on findings made by the Conference of German DPAs that the use of cookie IDs, advertising IDs, and unique user IDs does not constitute pseudonymization under the GDPR, since these identifiers "are used to make the individuals distinguishable and addressable", and not to "disguise or delete the identifying data so that data subjects can no longer be addressed" – which the Conference considers to be one of the purposes of pseudonymization.

Overall, the DPA found that the technical measures proposed were not enough because the respondents did not comprehensively explain (therefore, the respondents had the burden of proof) to what extent these measures "**actually prevent or restrict the access possibilities of US intelligence services on the basis of US law**".

With this finding, highlighted also in the operative part of the decision, the DPA seems to *de facto* reject the "risk based approach" to international data transfers, which has been specifically invoked during the proceedings. This is a theory according to which, for a transfer to be lawful in the absence of an adequacy decision, it is sufficient to prove the likelihood of the government accessing personal data transferred on the basis of additional safeguards is minimal or reduced in practice for a specific transfer, regardless of the broad authority that the government has under the relevant legal framework to access that data and regardless of the lack of effective redress.

The Austrian DPA is technically taking the view that it is not sufficient to reduce the risk of access to data in practice, as long as the possibility to access personal data on the basis of US law is actually not prevented, or in other words, not eliminated. This conclusion is apparent also from the language used in the operative part of the decision, where the DPA summarizes its findings as such: "**the measures taken in addition to the SCCs … are not effective because they do not eliminate the possibility of surveillance and access by US intelligence agencies**".

If other DPAs confirm this approach for transfers from the EU to the US in their decisions, the list of potentially effective supplemental measures for transfers of personal data to the US will remain minimal – *prima facie,* it seems that nothing short of anonymization (per the GDPR

standard) or any other technical measure that will effectively and physically eliminate the possibility of accessing personal data by US national security authorities will suffice under this approach.

A key reminder here is that the list of supplementary measures detailed in the EDPB Recommendationconcerns all international data transfers based on additional safeguards, to all third countries in general, in the absence of an adequacy decision. In the decision summarized here, the supplementary measures found to be ineffective concern their ability to cover "gaps" in the level of data protection of the US legal framework, as resulting from findings of the CJEU with regard to three specific legal acts (FISA Section 702, EO 12333 and PPD 28). Therefore, the supplementary measures discussed and their assessment may be different for transfers to another jurisdiction.

2.3 Are data importers liable for the lawfulness of the data transfer?

One of the most consequential findings of the Austrian DPA that may have an impact on international data transfers cases moving forward is that "the requirements of Chapter V of the GDPR must be complied with by the data exporter, but not by the data importer" – therefore, under this interpretation, the organizations that are on the receiving end of a data transfer, at least when they are a processor for the data exporter like in the present case, cannot be found in breach of the international data transfers obligations under the GDPR. The main argument used was that "the second respondent (as data importer) does not disclose the personal data of the complainant, but (only) receives them". As a result, **Google was found not to breach Article 44 GDPR in this case**.

However, the DPA did consider that it is necessary to look further, and as part of separate proceedings, into how the second respondent complied with its obligations as a data processor, and in particular the obligation to process personal data on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, as detailed in Article 28(3)(a) and Article 29 GDPR.

3. Sanctions and consequences: Between preemptive deletion of cookies, reprimands and blocking transfers

Another commonality of the two decisions summarized is that neither of them resulted in a fine. The EDPS issued a reprimand against the European Parliament for several breaches of the EUDPR, including those related to international data transfers "due to its reliance on the Standard Contractual Clauses in the absence of a demonstration that data subjects' personal data transferred to the US were provided an essential equivalent level of protection". It is significant to mention that the EP asked the website service provider to disable both Google Analytics and Stripe cookies in a matter of days after being contacted by the complainants on October 27, 2020. The cookies at issue were active between September 30, when the website became available, and November 4, 2020.

In turn, the Austrian DPA found that "the Google Analytics tool (at least in the version of August 14, 2020) can thus not be used in compliance with the requirements of Chapter V GDPR".

However, as discussed above, the DPA found that only the website operator – as the data exporter – was in breach of Article 44 GDPR. The DPA decided not to issue a fine in this case.

However, the DPA pursues to impose a ban on the data transfers or a similar order against the website, with some procedural complications. In the middle of the proceedings, the Austrian company that was in charge of managing the website transferred the responsibility of operating it to a company based in Germany, therefore the website is not under its control any longer. But since the DPA noted that Google Analytics continued to be implemented on the website at the time of the decision, it resolved to refer the case to the competent German supervisory authority with regard to the possible use of remedial powers against the new operator.

Therefore, it seems that stopping the transfer of personal data to the US without appropriate safeguards seems to be the focus in these cases, rather than sanctioning the data exporters. The parties have the possibility to challenge both decisions before their respective competent Court and require a judicial review within a limited period of time, but there are no indications yet whether this will happen.

4. The big picture: 101 complaints and collaboration among DPAs

The decision published by the Austrian DPA is the first one in the 101 complaints that noyb submitted directly to 14 DPAs across Europe (EU and the European Economic Area) at the same time in August 2020, from Malta, to Poland, to Lichtenstein, with identical legal arguments centered on international data transfers to the US through the use of Google Analytics or Facebook Connect, and all against websites of local or national relevance – so most likely these complaints will be considered outside the One-Stop-Shop mechanism.

The bulk of the 101 complaints were submitted to the Austrian DPA (about 50), either immediately under its competence, as in the analyzed case, or as part of the One-Stop-Shop mechanism where the Austrian DPA acts as the concerned DPA from the jurisdiction where the complainant resides, which likely needed to forward the cases to the many lead DPAs in the jurisdictions were the targeted websites have their establishment. This way, even more DPAs will have to make a decision in these cases – from Cyprus, to Greece, to Sweden, Romania and many more. About a month after the identical 101 complaints were submitted, the EDPB decided to create a taskforce to "**analyse the matter and ensure a close cooperation among the members of the Board**".

In contrast, the complaint against the European Parliament was not part of this set, it was submitted separately at a later date to the EDPS, but relying on similar arguments on the issue of international data transfers to the US through Google Analytics and Stripe cookies. Even if it was not part of the 101 complaints, it is clear that the authorities indeed cooperated or communicated, with the EDPS making a direct reference to the Austrian proceedings, as shown above.

In other signs of cooperation, both the Dutch DPA and the Danish DPA have published notices immediately after the publication of the Austrian decision to alert organizations that they may soon issue new guidance in relation to the use of Google Analytics, specifically referring to the Austrian case. Of note, the Danish DPA highlighted that "as a result of the decision of the Austrian DPA" it is now "in doubt whether – and how – such tools can be used in accordance

with data protection law, including the rules on transfers of personal data to third countries". It also called for a common approach of DPAs on this issue: "it is essential that European regulators have a common interpretation of the rules", since data protection law "intends to promote the internal market".

In the end, the DPAs are applying findings from a judgment made by the CJEU, which has ultimate authorityin the interpretation of EU law that must be applied across all EU Member States. All this indicates that it is likely a series of similar decisions will be successively published in the short to medium future, with small chances of seeing significant variations. This is why these two cases summarized here can be seen as the first two pieces that fell in a domino.

This domino, though, will not only be about the 101 cases and the specific cookies they target – it eventually concerns all US based service providers and businesses that receive personal data from the EU potentially covered by the broad reach of FISA Section 702 and EO 12333; all EU based organizations, from website operators, to businesses, schools, and public agencies, that use the services provided by the former or engage them as business partners, and disclose personal data to them; and it might as well affect all EU based businesses that have offices and subsidiaries in the US and that make personal data available to these entities.

This article was published on January 27, 2022, and is available online at https://fpf.org/blog/understanding-why-the-first-pieces-fell-in-the-transatlantic-transfers-domino/