Hildén, Jockum

Article

Mitigating the risk of US surveillance for public sector services in the cloud

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Hildén, Jockum (2021) : Mitigating the risk of US surveillance for public sector services in the cloud, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 10, Iss. 3, pp. 1-24, https://doi.org/10.14763/2021.3.1578

This Version is available at:
https://hdl.handle.net/10419/245339

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 10 **Issue** 3

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Mitigating the risk of US surveillance for public sector services in the cloud

Jockum Hildén *University of Helsinki* hello@jockumhilden.com

DOI: https://doi.org/10.14763/2021.3.1578

Published: 30 September 2021
Received: 6 December 2020 **Accepted:** 21 January 2021

Funding: This research was funded by the Academy of Finland, decision no. 320895. The contribution was written during a visiting fellowship at the European University Institute.
Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Hildén, J. (2021). Mitigating the risk of US surveillance for public sector services in the cloud. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1578

Keywords: Cloud services, CLOUD act, Surveillance, GDPR, Digital public services

Abstract: Despite efforts to mitigate European concerns over US governmental access to European data, the US regulatory framework is still problematic from a fundamental rights perspective, as elevated by the Schrems II ruling. The issues associated with transnational transfers of data have been further complicated by the European Data Protection Board's recommendations that state that EU personal data cannot be processed in the clear in third countries where public authorities demand access to data. Based on empirical case studies from the Netherlands and Sweden, the present contribution outlines possible remedies that mitigate this problem, but the fundamental issue appears unsolvable. While the US has taken steps to grant foreign nationals more rights, significant challenges remain with the US approach to mass surveillance and EU citizens' lack of judicial redress.

This paper is part of **Governing "European values" inside data flows**, a special issue of *Internet Policy Review* guest-edited by Kristina Irion, Mira Burri, Ans Kolk, Stefania Milan.

1. Introduction

Never has it been so easy to share data. Decentralised operations can operate seamlessly thanks to cloud services, allowing for real-time updates of databases and other documentation. Digitising public services has been an integral part of the European Union's digital strategies for over a decade (EC, 2010). However, the US surveillance scandals and associated regulatory frameworks make the digitisation of public services in Europe difficult. The use of cloud services necessitates a lack of "data sovereignty", as control over data and infrastructures are relinquished to the service provider (Irion, 2012). In cases where transborder data flows are required, jurisdictional issues arise. Transborder flows of personal data often give rise to conflicts between fundamental rights and the competences of surveillance authorities in third countries such as India, China, or the US. As US companies provide the most popular cloud-based services, it is especially problematic to reconcile the requirements to secure data used for public services in the EU and the US regulatory framework. The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) grants law enforcement the power to compel US-based companies to disclose data on their servers if they obtain a warrant. [1] The proposed solution to this issue is a treaty between the EU and the US, according to which also law enforcement in the EU member states could get granted access to data held in the US (EC, 2019; Vasquez Maymir, 2020). While such an agreement enables reciprocity and might be seen as an adequate political solution, it only solves the formal conflict with article 48 of the GDPR, [2] but not necessarily the problems associated with a lack of respect for fundamental rights.

In Sweden, this has led to a deadlock, where public authorities cannot readily move their operations to the cloud and use the services of US companies because sensitive personal data of Swedish citizens could be transferred to US law enforcement without Swedish judicial review, which is illegal under Swedish law (eSam, 2019). Furthermore, foreign court orders outside the scope of mutual legal assistance treaties are not regarded as a legal basis for transfers under the GDPR (Euro-

1. 18 U. S. C. §2701 et seq.

2. Article 48 specifies that "Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement."

pean Data Protection Supervisor and the European Data Protection Board, 2019, p. 3). Similarly, a comprehensive impact assessment of Microsoft Office in the Netherlands revealed that the software's data collection and transfers of telemetry data posed significant risks when used by governmental organisations (Privacy Company, 2018). As a result, Microsoft provided some new settings and adjusted their contracts with the Dutch government—but even those solutions were not completely satisfactory (Privacy Company, 2020). The situation is further complicated by *Schrems II,* which invalidated the Privacy Shield agreement and stated that transfers to third countries need to be protected by additional safeguards, without specifying what those might be. [3] Even if Microsoft or other cloud service providers are able to accommodate the security needs of the public sector, it is questionable whether they can insulate themselves from the data to such a degree that absolutely no data is within their control.

The purpose of this contribution is to provide an overview of the legal challenges associated with the use of US cloud services in the public sector in the EU. It shows how both administrative law and the EU fundamental rights framework together raise questions on the legality of using such services. Nonetheless, based on the Dutch and Swedish cases, this contribution also highlights to what extent these challenges can be mitigated with technical, organisational, and contractual measures. These can be specified in public procurement provisions.

The present contribution proceeds as follows. Section two briefly outlines how US law enforcement and the intelligence community may (legally) access data held by US cloud service providers. Section three presents to what degree this legal framework is incompatible with European fundamental rights as argued by the Court of Justice of the European Union (CJEU) in *Schrems II*. This ruling is further analysed in light of the European Data Protection Board's (EDPB) (2020) recommendations on supplementary measures, the European Commission's (2020) draft standard contractual clauses (SCCs) and the European Data Protection Supervisor's (EDPS) and the EDPB's (2020) joint opinions on said SCCs. Section four discusses how this presents a challenge for public services wishing to use the services of US cloud providers. This is demonstrated through two case studies: the evaluation of the Dutch government's contract with Microsoft, and the debate surrounding the use of cloud services in the Swedish public sector. The contribution concludes with a discussion on what consequences this has for the future of the digitisation of the public sector in Europe.

3. Case C-311/18, Data Protection Commissioner vs Facebook Ireland Ltd, Maximillian Schrems, (*Schrems II*) ECLI identifier: ECLI:EU:C:2020:559.

2. US access to EU data

The Snowden revelations laid bare to what extent data on US services were subject to the intelligence gathering operations of the National Security Agency (NSA). What had been suspected by critics of the intelligence community was fundamentally confirmed by the leaked documents. The leaks would have a major impact on the diplomatic relations between the US and the EU member states, and importantly for the focus of this contribution, they put a dent in the trust of US tech companies (see Daskal, 2018, p. 236). The surveillance scandal has left a permanent stain on the US tech industry, which desperately tries to rid itself of the image that any data stored on their servers is automatically accessible by the NSA. Google's (2020) and Microsoft's (2020a) transparency reports with their adjoined Frequently Asked Questions are testimony to this. The existing data sharing frameworks on passenger name records and banking data between the US and the EU have also demonstrated that a global (or at least a transatlantic) framework agreement on the protection of personal data is needed (Vara 2014, p. 260; Mitsilegas, 2016). Especially the EU citizens' access to justice in the US has been questioned.

In the aftermath of the NSA revelations the US government engaged in diplomatic damage control. President Obama famously issued Presidential Policy Directive 28 (PPD-28), stating that "All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information" (The White House, 2014). The consequences of PPD-28 are hard to measure—while the intelligence community is bound by presidential directives, nothing stops the president from overturning the directive and not making the decision public (Dwyer, 2002). Fahey (2019) has demonstrated that the degree of transparency in transatlantic relations is highly dependent on the political landscape in the US, showing that the friendly relations under Obama were highly challenged under Trump. In this environment, guarantees based on presidential directives appear fraught. If, however, for the sake of argument, one takes the directive at face value, it establishes a principle that is not recognised by the US Supreme Court: that non-US persons have fundamental rights not just inside but also outside the US.

The crux of the matter is that the Fourth Amendment of the US Bill of Rights granting "The right of the people to be secure in their persons, houses, papers, and effects" does not apply to foreign nationals abroad (Veneziano, 2019; De Filippi, 2013). The constitutional limits on national surveillance do not apply to foreign intelligence gathering operations. Instead, intelligence activities are regulated by Executive Order (EO) 12,333, which was issued by President Reagan (The White

House, 1981). The relevant provisions can be found in section 2.3, which states (among other things) that the collection, retention and dissemination of foreign intelligence information, including information concerning corporations or other commercial organisations, is permissible.

EO 12,333 remains in force, but the surveillance capabilities of the intelligence community have been somewhat modified by section 702 of the Foreign Intelligence Surveillance Act (FISA). [4] Importantly, US tech companies are compelled to assist the government in the following manner:

> … the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to—
>
> (A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition. [5]

In other words, US tech companies are compelled to assist the US government and cannot inform their customers that they have been targeted. They can nevertheless publish statistics on governmental requests in their transparency reports. This obviously has profound consequences for US cloud service providers that wish to have the European public sector as their customers—there is no guarantee that the data the European public authorities upload to the cloud will be left alone.

On 13 January 2021, the NSA released a document on the guidelines that govern signals intelligence, the so-called SIGINT Annex. [6] While mostly focused on the protections awarded to US persons, it did include some protections for non-US persons abroad, the main restriction being that data collection should be restricted to foreign intelligence requirements, support to military operations or to protect the safety of a US person held captive (Kris, 2021, p. 25). There are also further requirements to filter non-pertinent information (Kris, 2021, p. 77). However, foreign intelligence is a very broad category, and such a limitation does not in itself pro-

4. 50 U.S.C. ch. 36 § 1801 et seq.

5. 50 U.S.C. ch. 36 § 1881(a)(i)(1)(A).

6. Procedures governing the conduct of DoD intelligence activities: Annex governing signals intelligence information and data collected pursuant to section 1.7(c) of E.O. 12333, https://assets.documentcloud.org/documents/20454757/redacted-annex-dodm-524001-a.pdf.

vide any safeguards for the fundamental rights of foreign nationals.

It is not only the intelligence community that wishes to gain access to data held by cloud service providers, but also law enforcement more broadly speaking. The CLOUD Act, which amended the Stored Communications Act, makes it possible for law enforcement to request access to records held by US companies abroad if they can obtain a warrant. The CLOUD Act differs from the surveillance capabilities regulated by EO 12,333 and FISA section 702 in two important ways—first, each request is subject to judicial review, and second, law enforcement will have to demonstrate probable cause to obtain a warrant. [7] According to Microsoft's (2019) transparency report its enterprise customers are hardly ever targeted by US law enforcement, but individual, regular user accounts across the world are regularly subject to law enforcement requests.

However, from the perspective of public authorities there appears to be fewer concrete concerns related to law enforcement access—but as will be demonstrated later in this contribution, the procedure as such might make the arrangement incompatible with the laws of EU member states. Woods (2018, p. 400) has argued that such conflict of laws should be taken into account by the court considering the warrant based on comity principles recognised in US law. In short, the principles maintain that courts should consider any conflicts of laws that might arise and refrain from issuing decisions that undermine the laws of another nation. However, whether courts would actually be prone to taking European data protection rights into account, for instance when considering whether law enforcement should be granted access to data held by a US company abroad, is uncertain at best. The European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) (2019, p. 2) have issued an impact assessment in which they cast doubt over whether companies subject to CLOUD Act warrants will challenge them with reference to common law comity.

To conclude, the US surveillance framework is wide-reaching and lacks safeguards for foreign citizens outside the territory of the US. While the public authorities' access to personal data on US soil may be further limited by law, the power to limit foreign surveillance rests with the president, which makes the US surveillance framework unpredictable and subject to sudden shifts.

7. 18 U.S. Code § 2703(c)

3. The question of additional safeguards

3.1 Inadequate decisions, says the CJEU

The US legal framework clearly enables governmental access to data held by US companies—to such a degree that the CJEU has invalidated not one but two Commission (2000; 2016) adequacy decisions based on the Safe Harbor agreement (*Schrems* I) [8] and the Privacy Shield arrangement (*Schrems II*). The agreements had enabled international data transfers from the US to the EU even though the former did not formally offer an adequate level of protection of EU data. [9] Without going into the details of either the Safe Harbor agreement or the Privacy Shield arrangement, it is necessary to point out the conflict of laws that gave rise to the Court's invalidation of the two decisions.

The central problem with the US surveillance regime outlined in the previous section is that it undermines the right to privacy, the right to data protection, and the right to an effective remedy and to a fair trial as stated by articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union. Essentially, both decisions were invalidated because the US surveillance framework did not recognise the fundamental rights of non-US persons. Whereas the Commission viewed PPD-28 as testimony to the privacy rights of Europeans, the court did not agree to this conclusion:

> It follows therefore that neither Section 702 of the FISA, nor E.O. 12333, read in conjunction with PPD-28, correlates to the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary.(*Schrems II*, p. 184).

The invalidation of the Privacy Shield decision did not come as a surprise to data protection lawyers (Krouse, 2018; Callahan-Slaughter, 2016). The surveillance conducted by the US governmental agencies was still neither proportionate nor necessary by European standards, it was not based on European Union or member state laws, and a newly instated Privacy Shield Ombudsperson for handling data was not seen as equivalent to the right to effective redress according to article 47

8. C-362/14, Maximillian Schrems v. Data Protection Commissioner 6 October 2015, (*Schrems I*) ECLI identifier: ECLI:EU:C:2015:650

9. Adequacy decisions were issued with reference to article 25 of the Data Protection Directive (95/46/EC) and are now issued with reference to article 45 of the General Data Protection Regulation (2016/679).

of the Charter. However, the court did not invalidate Standard Contractual Clauses (SCCs), a contractual arrangement for transferring data to so-called third countries that, for one reason or another, are not able to offer EU data adequate protection. However, given that contractual terms do not bind other than the parties, it is clear that the SCC will not put a stop to US governmental access to data. Instead, the court referred to recital 109 of the GDPR, which states that controllers can add "other clauses or additional safeguards", and added that "[the standard data protection clauses] may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection" (*Schrems II*, p. 133). Data protection lawyers have struggled with what, exactly, these supplementary measures might be.

In sum, the US approach that limits fundamental rights to its residents in combination with its propensity to use blanket surveillance measures pose a significant problem for the European fundamental rights regime. While the CJEU did leave the door open for some protective measures, exactly what would be considered a sufficient safeguard in light of the legal requirements to grant a third country access to personal data was not addressed by the court.

3.2 A tale of two interpretations

A few months after the *Schrems II* decision, the EDPB issued its own recommendations on the topic of supplementary measures. From the perspective of EU entities using US cloud services, the news was not good. In the recommendations, the Board stated that if the legal regime in a third country allows for public authorities' access to data in a manner which goes beyond what is necessary and proportionate in a democratic society, no effective safeguards can be found. Specifically,

> where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys. (EDPB 2020, p. 27)

Essentially, the conclusion was that no US Software-as-a-Service (SaaS) solutions would be able to fulfil the conditions of *Schrems II*. For a SaaS solution to be able to work, the service provider in question needs to have access to the cryptographic keys, at least momentarily. No contractual, organisational or technical measures

can currently remedy this problem. Importantly, the EDPB (2020, p. 14) clarified that an assessment should be based on "objective factors", that is, the legal framework or factual capabilities of public authorities in the third country in question, and not "subjective ones such as the likelihood of public authorities' access to your data in a manner not in line with EU standards."

The Commission would nevertheless not support this conclusion. In its draft SCCs, the Commission stated that when controllers or processors warrant that they have no reason to believe that personal data will be disclosed to public authorities, they should take due account of

> (i) the specific circumstances of the transfer, including the content and duration of the contract; the scale and regularity of transfers; the length of the processing chain, the number of actors involved and the transmission channels used; the type of recipient; the purpose of processing; the nature of the personal data transferred; any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred. (Commission 2020, clause 2)

The conclusion was the polar opposite of what the EDPB had recommended. Expectedly, the EDPB and the EDPS (2020) refuted the Commission's interpretation of *Schrems II*, and recommended that the Commission delete "the content and duration of the contract"; "the scale and regularity of transfers"; "the number of actors involved and the transmission channels used"; "any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer" from the clause. The Commission (2021) adopted the updated SCCs on June 4, but did not accept the EDPS suggestions, leaving the disputed quotes in recital 20.

In a direct response to the Schrems II ruling, the NSA (2020) published its internal targeting procedures. While most of it is concerned with demonstrating in what way US persons are not targeted, there are some parts which address how foreign intelligence is acquired:

> NSA must also reasonably assess, based on the totality of the circumstances, that the target is expected to possess, receive, and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory authorized for targeting under a certification or authorization executed by the

> Director of National Intelligence and the Attorney General in the manner prescribed by section 702 (NSA, 2020, p. 4)

If one follows the Commission's subjective assessments of unauthorised access, the risk analysis a public authority must make is whether, "based on the totality of the circumstances", the documents they upload to the cloud might be regarded as foreign intelligence from a US perspective. This obviously rules out defence departments, ministries, and possibly members of parliament, but what about the provision of welfare services? While the processed personal data may be highly sensitive for the person concerned, it is not likely that this type of information would be deemed "foreign intelligence", unless that someone would be a person of interest for other reasons.

Schrems II has led to some difficult discussions at the EU level, given that the EU institutions (EUIs) themselves use US cloud services. On 27 May 2021, the EDPS (2021) opened two investigations on the EUI's use of Amazon Web Services and Microsoft Office 365. Moreover, Max Schrems' organisation noyb (2020) filed a complaint with the EDPS against the European Parliament on behalf of six MEPs, claiming that the Parliament's EcoCare site illegally transferred personal data to the US through the installation of cookies.

While the EU institutions are attempting to find common ground relating to how Schrems II should be interpreted in practice, the use of US cloud services in the EU remains extensive in both the public and private sectors. In the following section, I will look at two concrete cases where data transfers to US cloud service providers have been put into question at the national level.

4. Moving the public sector to the cloud: some fundamental challenges

4.1 The case of Microsoft Office in the Netherlands

It is an established fact that the global cloud market is heavily dominated by US firms (Synergy Research Group, 2020). This is especially true of SaaS solutions. When it comes to all-encompassing productivity software used for editing documents, drafting presentations, and analysing spreadsheets, there are only two major players on the market: Google and Microsoft. While there is scant information on public sector SaaS adoption, SaaS revenues represent two thirds of total public cloud revenues on the EU market (DESI, 2020, p. 9). A Swedish study of cloud use

in the public sector revealed that 53 per cent of Swedish public authorities used SaaS (*Pensionsmyndigheten*, 2015, p. 60). Given that Microsoft does not even sell its Office software to enterprise customers as a stand-alone product, that percentage is likely to be much higher today.

Public contracts are regulated by national procurement legislation and EU directives if the tenders exceed certain monetary thresholds. In the public procurement procedure, a public authority specifies certain criteria that the tenderer should fulfil. Price, economic standing, and technical and professional ability are the most important criteria, but whether price is valued higher than quality depends on the contract in question. For SaaS, the quality assessment should not only include a review of the functionality of the software, but also its level of security and data processing practices.

It speaks volumes that the Dutch government has a dedicated team just for handling its Microsoft contracts, Strategic Vendor Management Microsoft (SLM Rijk). In 2018, SLM Rijk commissioned a data protection impact assessment of Office 365 from Privacy Company, a consultancy specialised in data protection. In their initial report, Privacy Company (2018, p. 107) concluded that "the processing of diagnostic data about the use of the mobile Office apps and the Controller Connected Experiences leads to five high data protection risks. Only Microsoft can effectively mitigate these risks. Government organisations are advised to create policies for their employees to not use Office Online and the mobile Office apps". One of the biggest problems was that Microsoft had retained controller status for the mobile and online apps, therefore effectively deciding how the data was being processed without the Dutch authorities having a say. [10]

Some of the high risks mentioned in the report related to the lack of transparency into what data gets transferred to Microsoft, no way to disable "connected experiences" [11] and employee access to mobile apps, unlawful collection of data through connected experiences, a lack of purpose limitation for the mobile apps and the connected experiences, and not enough control over sub-processors of data (Privacy Company, 2018, pp. 104-5).

The findings from the impact assessment prompted Microsoft to introduce new tools for transparency, limit the scope of data collection and use of sub-processors,

10. According to EU jurisprudence, a controller defines the nature and purpose of the processing, while the processor only processes the personal data on documented instructions, see article 28 of the GDPR.

11. Services include Smart Lookup, Office Store, and 3D Maps.

and new audit rights were granted to the Dutch government (Privacy Company, 2019). As a result, no high risks for using Office software remained according to Privacy Company, but the online and mobile apps were still problematic. A follow-up study in June 2020 concluded that while high risks related to the web and mobile apps remained, Microsoft had agreed to limit their data collection and, crucially, only act as a processor for the mobile and web apps (Privacy Company, 2020, pp. 134-136). These actions, in combination with measures taken at the governmental level, would mitigate the remaining data protection risks. The report recognises that the risk for unauthorised US governmental access remains but determines that the "likelihood … is remote", resulting in a low risk for data subjects (Privacy Company, 2020, p. 126).

As a result of the impact assessments and the negotiations with the Dutch government, Microsoft (2020b) updated its "Online Services Data Protection Addendum (DPA)" worldwide. In the addendum, Microsoft states that it is primarily regarded as a processor and not a controller for the main online services (Microsoft, 2020b, p. 8). It is worth highlighting that Microsoft used to be the controller for the web and mobile apps. This is a welcome development for European public authorities that wish to use Microsoft's services. Still, it is nevertheless necessary to limit data flows to Microsoft, which means that some IT expertise is still needed in-house. The primary lesson from SLM Rijk is that the complexity of SaaS solutions requires expert knowledge to properly assess whether or not the services offered are GDPR compliant. Furthermore, it is not enough to review the contracts, but data flows need to be examined as well. A combination of legal and technical expertise is necessary to ensure that what is stated on paper also holds true in bits.

Given the complexity of the matter it is doubtful whether smaller municipalities and other authorities are able to manage the negotiation of cloud contracts and limiting settings to the bare minimum in a way which enables GDPR compliance. Whereas a small administrative entity could, with relative ease, buy a few hundred copies of productivity software, cloud service contracts are no less complex if they concern a hundred users or a hundred thousand users. While the controllership and therefore responsibility for personal data must lie with a public authority, it is not realistic that each public authority negotiates their contracts separately—at least not on the level of data flows and retention policies.

It is also worth noting that insulating the service provider completely from the content is not possible with SaaS—something Microsoft (2020c) also admits. Since that requires that the customer controls the encryption key, web apps are not supported. Microsoft recommends that "Hold Your Own Key" is "typically suitable only

for a small number of documents". This leads to one major organisational challenge and one major legal challenge.

Microsoft's description of its Hold Your Own Key service hints at the organisational problem—that if the most secure measures are instated and functionality is worsened, this could mean significant pushback from employees. As the Clinton email scandal demonstrated, individuals might go against internal regulations and security policies if an external service is easier to use. While Hillary Clinton was the secretary of state, she had sent emails containing classified information from her private email server (Labott, 2015). Even though public sector employees may be instructed to not use the cloud features for certain documents, it is possible that less technically oriented employees fail to understand the difference between using Office software on the desktop and in the browser.

The legal challenge is that if Microsoft controls the encryption keys, Microsoft remains at least partly "in control" of customer data, thus being in a position where it can be forced to cooperate with either US law enforcement or the intelligence community, which would be contrary to the EDPB's recommendations. Whether this hypothetical possibility is a concrete risk for the fundamental rights of EU residents depends on the public authority in question.

4.2 Swedish administrative law and the CLOUD Act

Whereas the data protection impact assessment of Microsoft Office was mostly focused on the GDPR, in Sweden a debate has surfaced surrounding the use of cloud services with reference to the national law on secrecy and publicity. [12] The main point of concern in the Swedish context has not been the foreign intelligence gathering operations but the impact of the CLOUD Act. Different public authorities, cloud service providers and law firms have taken turns debating whether using an US cloud service constitutes an unlawful disclosure of classified information (see eSam, 2019; Frydlinger & Olstedt Carlström, 2020; Delphi, 2020; Westling Palm & Öberg, 2020). A city's use of Microsoft 365 was even reported to the parliamentary ombudsman (Dataskydd.net, 2020), although the ombudsman decided not to take up the case with reference to ongoing governmental investigations (Justitieombudsmannen, 2020).

According to the Swedish law of secrecy and publicity, certain types of information are regarded as classified, and in order for the information to be disclosed, the authority in control of the information must make an assessment of whether the dis-

12. Sw. *Offentlighets- och sekretesslag* (2009:400)(OSL).

closure could cause harm to either the Swedish public interest or an individual. The threshold for harm depends on the information and the context, and it applies to both personal data and non-personal data. The problem boils down to this: does uploading confidential information to a US cloud service provider's server *in itself* constitute an unlawful disclosure of confidential information based on the fact that US cloud service providers can be compelled to disclose information on their customers abroad? Some argue that the legal requirement introduced by the CLOUD Act means that any contract between a cloud service provider and a public authority specifying the secrecy of information will be rendered null and void (Westling Palm & Öberg, 2020). Others argue that the likelihood that US law enforcement would access documents in this way is so low that such an interpretation of the law is absurd (Frydlinger & Olstedt Carlström, 2020). In essence, the Swedish debate precluded the discussion on supplementary measures after *Schrems II*: should risk assessments be based on the legal framework, or the practical circumstances?

In a way, both sides are correct—given the billions of Microsoft customers across the world, it is not likely that US law enforcement would request access to documents held by a small Swedish municipality. On the other hand, if that situation were to occur, the Swedish municipality could not stop the cloud service provider from turning over the documents, which would be a breach of the law of secrecy and publicity. While there is no clear way out of this dilemma, some contractual measures could mitigate the concerns. As a first step, cloud service providers could be contractually obliged to redirect law enforcement agencies directly to the customers, as Microsoft (2020b, p. 7) promises to do in its data protection addendum. Daskal (2018, p. 235) highlights that corporations ultimately decide if they wish to challenge or comply with governmental access requests. It is therefore possible to make this a contractual obligation.

Furthermore, following Woods (2018), it is possible to challenge CLOUD Act warrants with reference to common law comity. The EDPS and the EDPB (2019) have doubts regarding whether companies would actually challenge warrants in this way, but they did not address the possibility of adding such a requirement to the cloud contract—when faced with a warrant regarding information held by a public authority, the cloud service provider should always challenge the request with reference to common law comity. Given the very low occurrence of extraterritorial requests to enterprise customer data (see Microsoft, 2019), such terms could provide a sufficient layer of contractual safeguards. While such terms are meaningless in the face of FISA requests that a) tend to be secret and b) do not require a warrant,

at least classified information that holds no foreign intelligence value could be better protected from unsanctioned governmental access.

Somewhat paradoxically, it appears that the most mundane—typing away on Google Docs or Microsoft Word in a browser—would be the most challenging feature to incorporate in a way which is consistent with European fundamental rights. Cloud service providers already offer data to be stored within Europe, and although that type of requirement is quite meaningless in the face of US governmental access to European data, the data is at least fairly secure from physical intrusion. The data can be further encrypted, and the keys held by the customers, which insulates the cloud service provider from the content. This isa lot less challenging than creating new SaaS solutions, given the enormous advantage especially Microsoft has in productivity software. In fact, a study commissioned by the Swedish Competition Authority indicated that many public authorities tend to specify in their policy documents and procurement procedures that they prefer the proprietary standards and products provided by US technology companies over open standards (Lundell, Gamalielsson, & Tengblad, 2016, pp. 100-105). Another study by the Swedish Legal, Financial and Administrative Services Agency (2019, p. 50) concluded that Google and Microsoft are the only providers of web-based productivity software that can provide the necessary functionality.

The Swedish debate surrounding the CLOUD Act shows that clearing the hurdles associated with GDPR compliance is often not enough—public authorities process personal data for a wide variety of reasons, and national regulatory frameworks may add further restrictions to how data can be processed. The Swedish law on secrecy and publicity was not drafted with cloud services in mind, but as a filter for the otherwise far-reaching transparency of public documents. The underlying idea behind the law is that the administrative entities that gather sensitive data should make risk assessments of whether specific information can be transferred to the public domain. It is ill-fitted for handling routine submissions of large quantities of documents to subcontractors that are only supposed to store the data. Rather, this type of risk analysis is more appropriate to be conducted in the course of a rigorous data protection impact assessment. Here, the question of scale and scope becomes imperative. When a journalist requests access to a file held by the child protective services, the person responsible for the file is the right individual to make the assessment—s/he will know what the concrete risks are for the people mentioned in the file. When the child protective services transfer their entire database to the cloud, they might not possess the necessary expertise to properly gauge the risks. While the nature of the data is important also in that case, the risk analysis

takes completely different variables into account. To put it bluntly, child protective services are not trained for making assessments of what constitutes foreign intelligence according to the US intelligence community.

4.3 Selective legal compliance

At the same time as the *Schrems II* ruling invalidated the Privacy Shield and introduced strict requirements for transferring data to third countries using SCCs, millions of European employees and students are still using productivity software that the US intelligence community could require access to as if nothing changed. To use Svantesson's (2017, p. 220) terminology, both European customers and US cloud service providers are engaging in "selective legal compliance". A few months after *Schrems II*, the EDPS (2020) issued a new strategy for how the EU institutions (EUIs) could comply with the ruling. In it, the EDPS (2020, p. 8) "strongly encourages EUIs to ensure that any new processing operations or new contracts with any service providers does not involve transfers of personal data to the United States". Given the way SaaS operate, ensuring that not a single transfer of personal data occurs is a daunting task. While data at rest can quite easily remain in Europe—the big technology companies all have data centres in Europe—it is significantly harder to stop all flows of telemetry data associated with the services (see also Christakis, 2020, pp. 69-70). While the Dutch example has shown that at least telemetry data may be limited at the organisational level, web-based and mobile applications need to transfer data to the US for functional purposes. Based on the experiences from the Dutch and Swedish cases, it is nevertheless possible to draw a few conclusions.

First, it is evident that cloud service contracts need to include provisions that force US service providers to challenge law enforcement requests. While there are no guarantees that such protests will be taken into account in US courts, it at least contractually hinders companies from cooperating voluntarily. Second, significant attention should be devoted to scrutinising who determines the means and purposes of the processing, so that public authorities remain controllers for all personal data. Third, to satisfy the EDPB's conditions, US service providers should be insulated from content and telemetry data to the furthest degree possible. In practice this means limiting the service provider's access to data, and not submitting encryption keys to the service provider. However, this means that SaaS will not work, which leads to a fourth point: if mobile and web app functionality is needed, it is essentially not possible to comply with *Schrems II* according to the EDPB's interpretation. However, the Commission's interpretation that a subjective assessment is compatible with *Schrems II* indicates that a detailed risk analysis that thor-

oughly analyses the nature of the processing and the personal data involved might be sufficient. Lastly, the Dutch case shows that it is necessary to periodically assess the data flows to make sure that no data leaks occur.

5. Towards a European cloud?

After the Snowden revelations a lot more attention has been devoted to analysing the US regulatory framework on governmental access to data. This is a welcome development, because this screening has also resulted in increased knowledge of how personal data is processed, used, and transferred. Nevertheless, it is worth asking whether there is a risk that too much attention is devoted to data transfers that, despite their impermissibility, are unlikely to cause real harm. Is the telemetry data of productivity software the right focus? As US commentators are often keen to point out, European intelligence agencies also engage in significant surveillance operations (Schwartz & Peifer, 2017), but these fall under the list of permissible exceptions in the GDPR and other laws. The latest EU e-evidence proposal is also testimony to European law enforcement agencies' ambition to access data across borders (Vazquez Maymir, 2020). A consequence might be that more attention is devoted to telemetry data transferred to the US than content data in the EU. Still, claims of hypocrisy fail to consider that at least in Europe, the subjects of surveillance have access to justice, which is not dependent on the nationality of the appellant (Vara, 2014, p. 260).

It is nonetheless clear that for some public authorities, using SaaS by US providers will never be an option due to the sensitivity of the data they process. But it is equally true that a lot of documents get processed that will *never* be of interest to the US intelligence community. The problem is that public authorities in Europe will not know if and when a person in their files will be a person of interest for the US intelligence community. Most public authorities are presently incapable of making this risk assessment themselves. In October 2020, the *Commission Nationale de l'Informatique et des Libertés* (CNIL - 2020) decided that the Health Data Hub needed to relocate its data following the Schrems II ruling. The purpose of the Health Data Hub is to centralise all health registries in France. The French government had negotiated a contract with Microsoft, which had ensured that the data was being stored on European soil. However, due to the same issues presented in this contribution, the CNIL did not see this as a sufficient safeguard. Microsoft controlled the encryption keys and could therefore potentially unlock the database, should the US intelligence community request so.

The CNIL has proposed that a potential solution would be to licence the Microsoft

product to a European company that does not have significant activity in the US and is therefore protected from FISA or EO 12,333 orders. This way European customers could benefit from the Microsoft product without risking data breaches. It is perfectly imaginable that cloud-based infrastructure or platforms could operate in this way, but it is less likely to work in a SaaS environment that requires constant updates to a range of products. Unfortunately, it appears as if this problem will not be solved until there is a global or transatlantic political solution (see Mitsilegas, 2016). While international frameworks for regulating mass surveillance have been presented, they are not likely to be successful (Gstrein, 2020). In a world of global interdependence (Farrell and Newman, 2019), it is problematic that the country which is home to the most widely used IT services does not recognise the fundamental rights of people of other nations.

6. Conclusion

This contribution has pointed out that public authorities are facing overwhelming legal challenges when they are using US cloud services that provide more functionality than simple data storage. The only way to guarantee compliance with EU data protection jurisprudence is to insulate the service provider completely from the data, which effectively strips the service of any added functionality and renders SaaS completely unusable. Fundamentally, the present dilemma can be summarised in five points:

1. The US Supreme Court has not, and will probably not, grant non-nationals outside its territory fundamental rights.
2. The US is unlikely to limit surveillance to what is necessary and proportionate by European standards.
3. The US is unlikely to grant non-US persons access to justice in a manner which fulfils the Charter's requirements.
4. Cloud services with other functionality than data storage require that the service provider has, at least momentarily, access to data in the clear.
5. EU data localisation has no effect, because US-based companies are subject to the demands of US public authorities.

Does this, or should this, mean that no US-based cloud services can be used? While the EDPB's answer appears to be yes, such a conclusion would lead to a situation where cloud-based software solutions that originate from third countries are unavailable for the public sector in the EU. This has ramifications also for the private sector, which would need to consider the risks in continuing with a practice that the European data protection authorities have, in essence, deemed incompatible with fundamental rights.

The Dutch and Swedish cases demonstrate that there are contractual, organisational, and technical steps available to minimise the risks involved in using US cloud services, but the requirement that no personal data whatsoever can be processed in the clear by an US company is virtually impossible to satisfy without breaking the services completely. Furthermore, the measures are complex, and smaller administrative units cannot perform these tasks alone. The Dutch example has shown that a centralised public procurement procedure is a better option. Large public contracts are far more attractive for cloud service providers, which puts public authorities in a better negotiating position. In the Dutch case the commissioned data protection impact assessments were used to renegotiate the service terms and contracts, effectively raising Microsoft's data protection standards in the process.

All this goes to show that a transatlantic solution is urgently needed—but for the reasons outlined above, a completely satisfactory one is unlikely. The global frameworks that have been proposed have failed to materialise, and while the US has taken steps to accommodate the needs of EU member states, significant issues remain with the US approach to mass surveillance and EU citizens' lack of judicial redress.

ACKNOWLEDGEMENTS

I would like to thank reviewers Marieke de Goede and Marijn Sax for their thoughtful comments and helpful suggestions, editors Ans Kolk and Kristina Irion for their guidance, Thorsten Wetzling for his recommendations, and managing editor Frédéric Dubois for his stylistic remarks. I also want to thank Matthew D. Green for helping me understand cryptography in the cloud.

References

C.-311/18 Data Protection Commissioner vs Facebook Ireland Ltd, Maximillian Schrems (Schrems II), ECLI:EU:C:2020:559 (Court of Justice of the European Union 20 July 2020). https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1

C-362/14, Maximillian Schrems vs Data Protection Commissioner (Schrems I), ECLI:EU:C:2015:650 (Court of Justice of the European Union 6 October 2015). https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1

Callahan-Slaughter, A. (2016). Lipstick on pig: The future of transnational data flow between the EU and the united states. *Tulane Journal of International and Comparative Law*, *25*(1), 239–258.

Christakis, T. (2020). *European Digital Sovereignty: Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy* [Study (Preprint)]. Multidisciplinary Institute on Artificial Intelligence; Grenoble Alpes Data Institute. https://doi.org/10.2139/ssrn.3748098

Clarifying Lawful Overseas Use of Data Act (CLOUD Act) of 2018. 18 U. S. C. §2701 et seq. (n.d.).

Commission Nationale de l'Informatique et des Libertés. (2020). *Conseil d'état. Section du contentieux. Refere l. 521-2 CJA. Memoire en observations*. https://cdn2.nextinpact.com/medias/observations-de-la-cnil-8-octobre-2020-1---1-.pdf

Daskal, J. (2018). Borders and Bits. *Vand. L. Rev*, *71*(1), 179–240. https://vanderbiltlawreview.org/lawreview/2018/01/borders-and-bits/

Dataskyddnet. (2020). *JO-anmälan av Göteborgs Stad*. https://dataskydd.net/files/JO-Anmalan_Goteborgs_stad_molntjanster.pdf

De Filippi, P. (2013). Foreign clouds in the European sky: How US laws affect the privacy of Europeans. *Internet Policy Review*, *2*(1). https://doi.org/10.14763/2013.1.113

Delphi. (2020, May 28). Replik på eSams uttalanden om "röjande-begreppet" enligt OSL [Blog post]. *Delphi Tech Blog*. https://www.delphi.se/sv/tech-blog/replik-pa-esams-uttalanden-om-rojande-begreppet-enligt-osl/.

Digital Economy Society Index 2020: Integration of digital technology. (2020). [Report]. European Commission. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=67076

Dwyer, C. M. (2002). The US Presidency and national security directives: An overview. *Journal of Government Information*, *29*(6), 410–419. https://doi.org/10.1016/j.jgi.2002.05.001

eSAM. (2019). *Kompletterande information om molntjänster*. https://www.esamverka.se/download/18.4c1250a116d1bb3a3f094fe1/1568977769756/Kompletterande%20information%20om%20molnfr%C3%A5gan%202019-09.pdf

Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.), Pub. L. No. 2000/520/EC:, OJ L 215 7 (2000). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000D0520.

European Commission. (2010). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe*. https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52010DC0245.

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance), OJ L 207/1 (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016D1250.

European Commission. (2019). *Security Union: Commission receives mandate to start negotiating international rules for obtaining electronic evidence*. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_19_2891/IP_19_2891_EN.pdf.

European Commission. (2020). *ANNEX to 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*. https://ec.europa.eu/info/law/better-regulation/h

ave-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.

Commission Implementing Decision (EU) 2021/914 of 4 June 2021 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 (Text with EEA relevance), Pub. L. No. C/2021/3972, OJ L 199, 31 (2021). http://data.europa.eu/eli/dec_impl/2021/914/oj.

European Data Protection Board. (2020). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

European Data Protection Supervisor. (2020). *Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling* [Strategy]. European Data Protection Supervisor. https://edps.europa.eu/sites/edp/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf

European Data Protection Supervisor. (2021). *The EDPS opens two investigations following the "Schrems II" Judgement* [Press Release]. Press & Publications. https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en

European Data Protection Supervisor & European Data Protection Board. (2019). *ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence*. European Data Protection Supervisor. https://edps.europa.eu/sites/edp/files/publication/19-07-10_edpb_edps_cloudact_annex_en.pdf

Fahey, E. (2019). Transparency in transatlantic trade and data law. In V. Abazi & G. Rosen (Eds.), *Foreign Policy Secrets in the Age of Transparency*. Oxford University Press.

Farrell, H., & Newman, A. L. (2019). *Of privacy and power: The transatlantic struggle over freedom and security*. Princeton University Press.

Frydlinger, D., & Olstedt Carlström, C. (2020). *Molntjänster, offentlighet och sekretess i offentlig sektor: Utredning om och förslag till lagstiftning rörande offentlig sektors möjligheter att använda publika molntjänster* [Study]. Cirio Advokatbyrå AB. https://cirio.se/assets/uploads/images/hero-images/Molntjanster-offentlighet-och-sekretess-i-offentlig-sektor-Cirio-12-maj-2020-002.pdf

Google. (2020). *Global requests for user information*. Google Transparency Report. https://transparencyreport.google.com/user-data/overview

Gstrein, O. (2020). Mapping power and jurisdiction on the internet through the lens of government-led surveillance. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1497

Executive Order 12,333, Pub. L. No. 46 FR 59941, 3 CFR, 1981 Comp. (1981).

Irion, K. (2012). Government Cloud Computing and National Data Sovereignty. *Policy & Internet*, *4*(3), 40–71. https://doi.org/10.1002/poi3.10

Justitieombudsmannen. (2020). *Dnr. 551-2020*.

Kris, D. S. (2021). The NSA's New SIGINT Annex. *Journal of National Security Law & Policy*. https://jnslp.com/2021/01/19/the-nsas-new-sigint-annex/

Krouse, W. (2018). The inevitable demise of privacy shield: How to prepare. *Computer and Internet Lawyer*, *35*(6), 19–22.

Labott, E. (2015, July 24). Official: Clinton emails included classified information. *CNN*. https://edition.cnn.com/2015/07/24/politics/hillary-clinton-email-justice-department.

Lundell, B., Gamalielsson, J., & Tengblad, S. (2016). *IT-standarder, inlåsning och konkurrens: En analys av policy och praktik inom svensk förvaltning* (Commissioned research report 2016:2). Konkurrensverket (Swedish Competition Authority). https://www.konkurrensverket.se/globalassets/publikationer/uppdragsforskning/forsk_rapport_2016-2.pdf

Microsoft. (2019). *Law Enforcement Requests Report. Requests received for all Microsoft Services from July to December 2019*. Microsoft. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4sg0d

Microsoft. (2020a). *Hold your own key (HYOK) details for Azure Information Protection*. Microsoft Docs. https://docs.microsoft.com/en-us/azure/information-protection/configure-adrms-restrictions

Microsoft. (2020b). *US National Security Orders Report* [Report]. Microsoft. https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report.

Microsoft. (2020c). *Microsoft Online Services Data Protection Addendum*. Microsoft; Internet Archive. https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=17880

Mitsilegas, V. (2016). Surveillance and digital privacy in the transatlantic war on terror: The case for a global privacy regime. *Columbia Human Rights Law Review*, *47*(3), 1–77.

noyb. (2020). *Complaint under article 63(1), 67 Regulation 2018/1725. Noyb Case-No: C-035*. noyb. https://noyb.eu/sites/default/files/2021-01/NOYB%20COMPLAINT%20C035_Redacted.pdf

NSA. (2020). *NSA's 2019 Section 702 Targeting Procedures, Sep. 17, 2019*. Office of the Director of National Intelligence (ODNI. https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_NSA_Targeting_17Sep19_OCR.pdf.

Palm, K. W., & Öberg, N. (2020, May 26). *Kommentar till kritisk rapport om molntjänster i offentlig sektor*. eSam. https://www.esamverka.se/aktuellt/nyheter/nyheter/2020-05-26-kommentar-till---kritisk-rapport-om-molntjanster-i-offentlig-sektor.html

Pensionsmyndigheten. (2015). *Molntjänster i staten. En ny generation av outsourcing* [Report]. Pensions Myndigheten. https://www.pensionsmyndigheten.se/content/dam/pensionsmyndigheten/blanketter---broschyrer---faktablad/publikationer/svar-p%C3%A5-regeringsuppdrag/2016/Uppdrag%20att%20analysera%20potentialen%20f%C3%B6r%20anv%C3%A4ndning%20av%20molntj%C3%A4nster%20i%20staten%20.pdf

Privacy Company. (2018). *DPIA diagnostic data in Microsoft Office Proplus* [DPIA report]. Ministry of Justice and Security. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjPm9DxwrLzAhUiRkEAHfr3A84QFnoECAIQAQ&url=https%3A%2F%2Fwww.rijksoverheid.nl%2Fbinaries%2Frijksoverheid%2Fdocumenten%2Frapporten%2F2018%2F11%2F07%2Fdata-protection-impact-assessment-op-microsoft-office%2FDPIA%2BMicrosoft%2BOffice%2B2016%2Band%2B365%2B-%2B20191105.pdf&usg=AOvVaw2739WkmYX_ksXqQ5Wj1njb

Privacy Company. (2019). *DPIA Office 365 ProPlus version (June 2019)* [DPIA Report]. Ministry of Justice and Security. https://www.government.nl/documents/publications/2019/07/22/dpia-office-365-proplus-version-1905

Privacy Company. (2020). *DPIA Office 365 for the Web and mobile Office apps. Data protection impact assessment on the processing of diagnostic data* [DPIA report]. Ministry of Justice and Security. https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2020/06/30/data-protection-impact-assessment-office-365-for-the-web-and-mobile-office-apps/DPIA+Office+for+the+Web+an

d+mobile+Office+apps+30+June+2020.pdf

Schwartz, P. M., & Peifer, K. (2017). Transatlantic data privacy law. *Georgetown Law Journal*, *106*(1), 115–180. https://www.law.georgetown.edu/georgetown-law-journal/in-print/volume-106/volume-106-issue-1-november-2017/transatlantic-data-privacy-law/

Svantesson, D. J. B. (2017). *Solving the internet jurisdiction puzzle*. Oxford University Press. https://doi.org/10.1093/oso/9780198795674.001.0001

Swedish Legal, Financial and Administrative Services Agency. (2019). *Webbaserat kontorsstöd*. (Pre-study report Dnr 23.2-6283-18.).

Synergy Research Group. (2020, May 7). *Amazon & Microsoft Lead the Cloud Market in all Major European Countries* [News release]. GlobeNewswire. https://www.globenewswire.com/news-release/2020/05/07/2029605/0/en/Amazon-Microsoft-Lead-the-Cloud-Market-in-all-Major-European-Countries.html

The White House. (2014, January 17). *Presidential Policy Directive 28: Signals Intelligence Activities* [Statement]. The White House Briefing Room. https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

Vara, J. (2014). Transatlantic counterterrorism cooperation agreements on the transfer of personal data: A test for democratic accountability in the EU. In E. Fahey & D. Curtin (Eds.), *A Transatlantic Community of Law: Legal Perspectives on the Relationship between the EU and US Legal Orders* (pp. 256–288). Cambridge University Press. https://doi.org/10.1017/CBO9781107447141.017

Vazquez Maymir, S. (2020). Anchoring the Need to Revise Cross-Border Access to E-Evidence. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1495

Veneziano, A. (2019). Applying the US Constitution Abroad, from the Era of the US Founding to the Modern Age. Fordham Urb. *Fordham Urban Law Journal*, *46*(3), 602–640. https://ir.lawnet.fordham.edu/ulj/vol46/iss3/4

Woods, A. K. (2018). Litigating Data Sovereignty. *Yale Law Journal*, *128*(2), 328-406 3 2 2 2 2 233 3 107 8-.

Funding

This research was funded by the Academy of Finland, decision no. 320895. The contribution was written during a visiting fellowship at the European University Institute.

Declaration of novelty and no competing interests

By submitting this manuscript I declare that this manuscript and its essential content has not been published elsewhere or that it is considered for publication in another outlet.

No competing interests exist that have influenced or can be perceived to have influenced the text.

Published by


in cooperation with