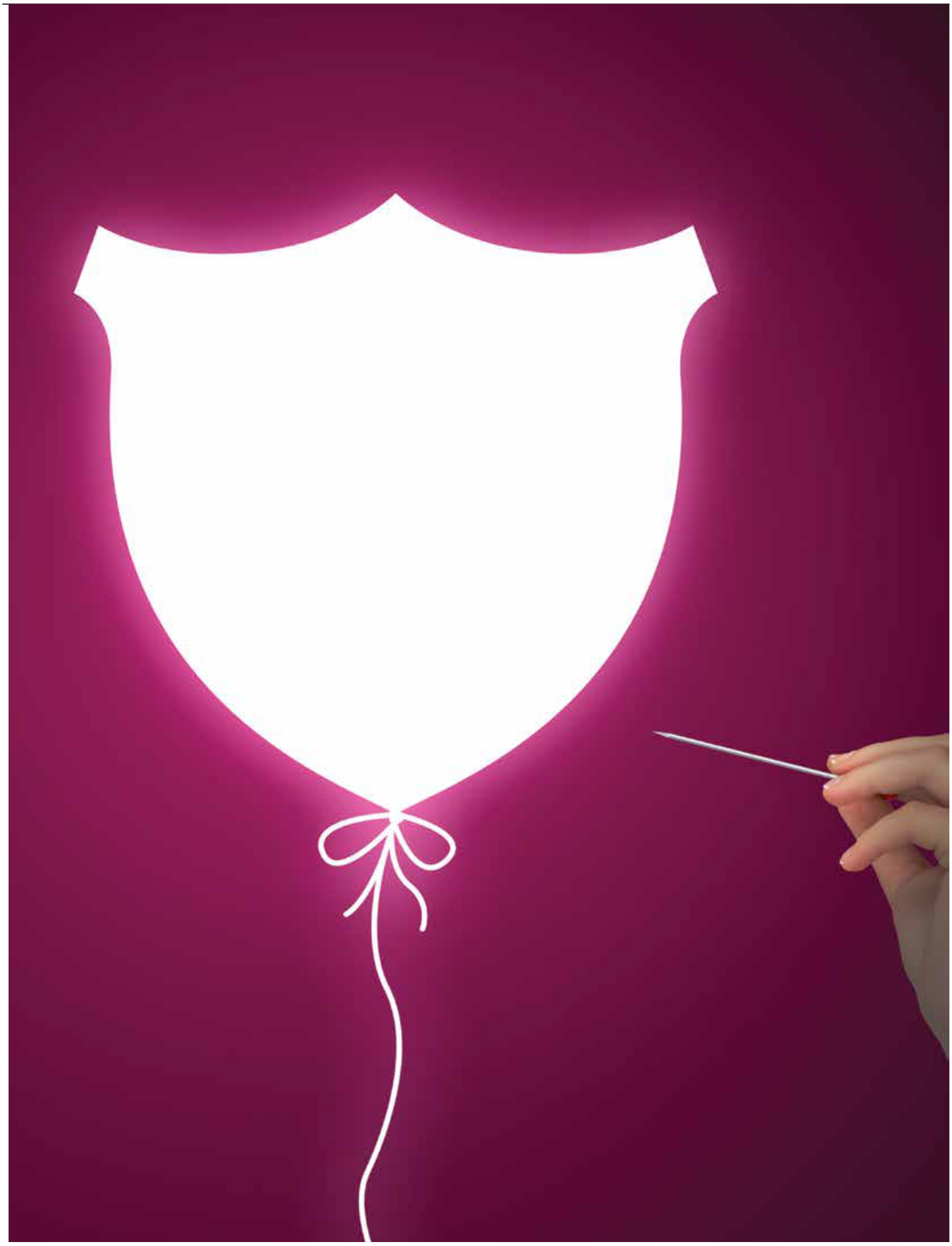
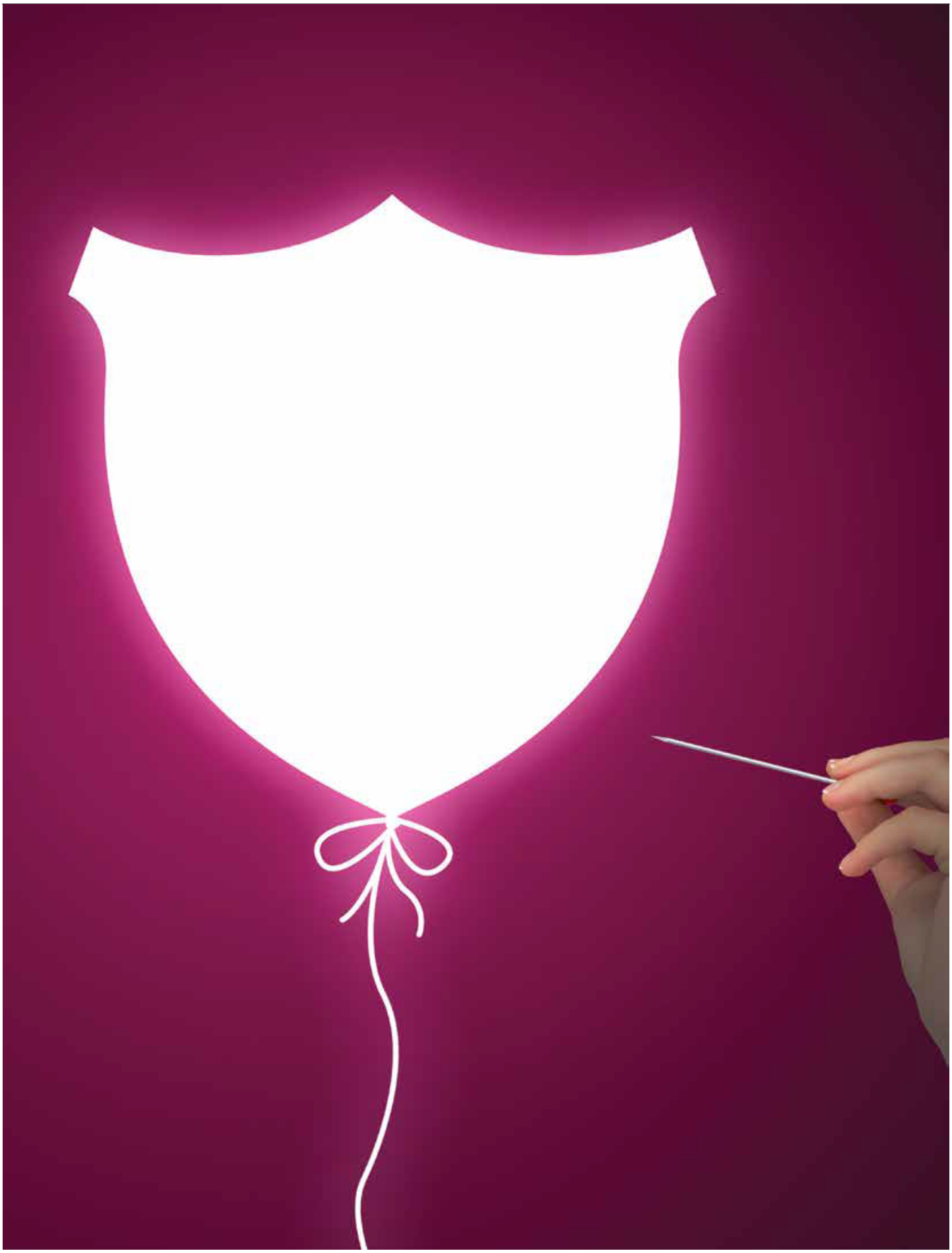
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Is the Privacy Shield Doomed to Fail? And How Your Company Can Protect Itself

Government

Technology, Privacy, and eCommerce





CHEAT SHEET

- ***Close the loophole.*** The first concern raised by the CJEU was that the Safe Harbor agreement allowed US intelligence agencies to access the personal data of EU citizens under the guise of national security.
- ***Fight fire with fire.*** Under the new framework, the Article 29 Working Party recommended that the new Privacy Shield framework allow EU citizens to bring claims for damages in the European Union through a competent EU national court. However, the drafters of the legislation did not include any provisions to this effect.
- ***Recommendation unanswered.*** In reviewing the Safe Harbor Agreement, the CJEU noted that the legislation hinders data protection authorities from performing their duties. This issue was not rectified in the new framework, and the Privacy Shield contains the same language as the invalidated Safe Harbor Agreement.
- ***Next steps.*** Although the new agreement has made great strides at compromise, the likelihood of any amendment to the newly enacted agreement in accordance with the concerns of the CJEU is doubtful. In-house counsel should prepare accordingly to ensure the legal flow of trans-Atlantic data.

On July 12, 2016, after two years of intense negotiations, the European Commission and the US Department of Commerce reached an agreement on a new framework to legally restore the trans-Atlantic data exchange. For in-house counsel, this new regulation potentially represents a major challenge. The proposed framework, called the EU-US Privacy Shield, will ensure key protections for European Union (EU) citizens when their personal data is transferred to the United States. The framework is designed to build trust in the global digital economy and will ultimately drive our digital future. Unfortunately, this new agreement is not likely to survive if challenged in the Court of Justice of the European Union (CJEU). Nonetheless, there is a practical solution for every organization relying on data exchange between the European Union and the United States.

In 2015, the original Safe Harbor framework — on which thousands of US companies relied — was invalidated in the Schrems case because the framework did not sufficiently protect EU citizens' personal data when transferred to the United States. Specifically, the CJEU found the Safe Harbor framework invalid for three reasons: (1) The framework allowed US intelligence agencies to interfere with EU citizens' privacy protections, (2) it did not provide adequate legal remedies to EU citizens whose privacy rights had been violated, and (3) it prevented EU Data Protection Authorities (DPAs) from executing their legal obligations.

In light of the CJEU's rationale, there are serious concerns that the Privacy Shield framework, as enacted, does not adequately address these issues. A number of experts and privacy advocates have denounced the agreement as inadequate. Max Schrems, the Austrian law student who brought the lawsuit that eventually invalidated the Safe Harbor agreement, has voiced criticism by stating that "if this case goes back to the [CJEU] — which it very likely will — then it will fail again." For the Privacy Shield to survive a legal challenge, it must provide an "essentially equivalent" level of protection for EU citizens when their personal data is transferred to the United States.

Before delving into an analysis of the Privacy Shield, it should be clear that every organization that

relies on the transfer of data between the European Union and the United States should strongly consider self-certifying for the Privacy Shield. Despite this, counselors should also consider implementing binding corporate rules (BCRs) or standard contract clauses. This “Privacy Shield + 1” approach is quickly becoming the best practice to ensure a continued flow of data if the Privacy Shield becomes invalidated through court decisions. Although this article will argue that the Privacy Shield framework will likely not survive a legal challenge, that does not mean it cannot be relied on until its demise. In fact, counselors should use the Privacy Shield because it is inexpensive and relatively easy to self-certify. However, counselors should also explore alternative methods while self-certifying — as the Privacy Shield will not survive indefinitely.

This article examines the criteria raised by the CJEU and analyzes whether the Privacy Shield framework adequately addresses the CJEU’s concerns. It also looks at whether the proposed framework provides EU citizens with an “essentially equivalent” level of protection when their personal data is transferred to the United States. And finally, the article explains alternative methods that in-house counsel can use to continue the legal transfer of data from the European Union.

The first concern raised by the CJEU was that the Safe Harbor agreement allowed US intelligence agencies to access the personal data of EU citizens under the guise of national security. The European Commission stated, “The personal data of EU citizens sent to the US under the Safe Harbor may be accessed and further processed by US authorities in a way incompatible with the grounds on which the data was originally collected in the European Union and the purposes for which it was transferred to the US.” This access was justified because of an exception that allowed access “to the extent necessary to meet national security, public interest, or law enforcement requirements.”

To survive a legal challenge, the new framework will need to correct this loophole. Specifically, the framework must justify the US intelligence agencys’ access and satisfy Article 52 of the EU’s Charter of Fundamental Rights by “lay[ing] down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data.” Unfortunately, the new agreement does not meet the burden stated in Article 52. In fact, the new framework contains the same language as the invalidated Safe Harbor framework: “Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements.”

However, the Privacy Shield has attempted to address this area of concern through the creation of an ombudsperson. This position’s responsibilities include dealing with individual complaints from EU citizens if they believe their personal data has been used in an unlawful manner by US intelligence agencies. The duties and responsibilities of the ombudsperson will be carried out by an undersecretary of the US Department of State. If this role was created to address complaints levied at intelligence agencies, it would have been far more pragmatic and effective for the position to be filled by an individual who has more knowledge and understanding of the intelligence community.

There is also little evidence to suggest that the ombudsperson is afforded the same level of independence as other oversight positions that the CJEU has found compliant. Moreover, political appointees in the United States can be dismissed easily, which detracts from the ombudsperson’s purported independence.

Notwithstanding the lack of required independence, the redress and investigatory powers of the ombudsperson are severely lacking. To have sufficient investigatory power, the position must have

unfettered access to all information and data exchanged in the Privacy Shield. The framework does not give the ombudsperson such access and, if a violation is detected, he or she cannot compel the violating agency to cease its illegal data processing operation. Rather, a "request alleging violation of law or other misconduct will be referred to the appropriate United States government body, including independent oversight bodies, with the power to investigate the respective request and address non-compliance as described below."

In an effort to help define the exception "necessary to protect national security," General Counsel for the Office of the Director of National Intelligence Robert Witt stated, "When data has been transferred to corporations in the United States pursuant to the Privacy Shield, or indeed by any means, US intelligence agencies can seek that data from those corporations only if the request complies with FISA [US Foreign Intelligence Surveillance Court] or is made pursuant to one of the National Security Letter statutory provisions." This is a troubling statement for Europeans to swallow when you consider the 2015 FISA Annual Report to Congress, which states that the US government filed 1,598 warrant requests and FISA did not deny a single one.

Further complicating the matter is a recent change approved by the US Supreme Court to the Federal Rules of Criminal Procedure (FRCP): The revision to Rule 41 of the FRCP now permits judges to issue warrants for access to computers located in any jurisdiction, including the European Union. Previously, judges were able to order search warrants only within their court's jurisdiction.

Nonetheless, the recent reclassification of internet service providers as a utility by the Federal Communications Commission, stripping the Federal Trade Commission (FTC) of its privacy enforcement, is perhaps the most worrisome development. Traditionally, the FTC was the privacy authority in the United States as well as the enforcer of privacy laws on which the Privacy Shield is based. Jon Leibowitz, former FTC chairman under President Barack Obama, stated, "The [Department of Commerce] and others are relying on the FTC approach, and if it's being questioned as not strong enough, I think does not potentially bode well [for] Privacy Shield." Although the European Union voted in favor despite this recent change, it will certainly be an issue the CJEU will closely examine.

As enacted, the Privacy Shield does not adequately address the CJEU's concern over US intelligence agencies accessing data exchanged through the framework. The exception given in the Privacy Shield contains the exact same language used in the Safe Harbor. It does not lay out clear guidelines as required by Article 52 and has the potential to be easily exploitable through secretive FISA courts. The creation of an ombudsperson is a step in the right direction, but the position in its proposed form does not provide a sufficient level of independence or an adequate redress to EU citizens for non-compliant data processing.

The second concern raised by the CJEU was that the Safe Harbor did not provide adequate remedies to EU citizens whose privacy rights had been violated. In the CJEU's own words, "data subjects had no administrative or judicial means of redress." Article 47 of the EU's Charter of Fundamental Rights requires EU citizens to have an effective remedy before a tribunal when their rights have been violated.

To meet this burden, the Article 29 Working Party recommended that the new framework allow EU citizens "to bring claims for damages in the EU" in addition to being "granted the right to lodge a claim before a competent EU national court." Unfortunately, the drafters of the Privacy Shield did not include any clauses or provisions to comply with this recommendation. In fact, the current arbitration framework within the Privacy Shield was proposed because the FTC has no legal duty to deal with

complaints from EU citizens. As a result, EU negotiators demanded adequate assurance that every complaint be addressed. The Privacy Shield also states that the complainant will have to cover their own attorney's fees in arbitration, creating a significant financial burden for those seeking a judicial remedy.

The United States tried to address the concerns of the CJEU by passing the Judicial Redress Act on February 24, 2016. The legislation is designed to give EU citizens standing to seek remedy for privacy right violations in US courts. However, the act is far too limited to satisfy the requirement that EU citizens be afforded an effective redress mechanism. Of note, corporations using the Privacy Shield cannot be sued under the new law, and only "certain US government agencies" will be liable. Due to the legislation's lack of clarity and staggering amount of exemptions, it is far too difficult for EU citizens to determine what federal agencies will actually be liable. This raises credible doubt that the Judicial Redress Act satisfies the Article 47 requirement of providing an "effective remedy."

Max Schrems put it succinctly:

> "There is still no court I can go to. There's still no approval by court for an individual case; there's still no redress where I can walk up and say, 'I don't want my data to end up at the National Security Agency (NSA), and I don't even want the NSA to have access to it,' which is actually the crucial point under the European Law."

The third concern raised by the CJEU was that Safe Harbor prevented the national data protection authorities (DPAs) from performing their legal obligations and duties. In its rationale, the CJEU stated that any data exchange framework "cannot eliminate or reduce the powers expressly accorded to the [data protection] Authorities." The CJEU went on to say that DPAs "must be able to examine, with complete independence, whether the transfer of that data complies with the requirements." Essentially, these supervisory agencies have an affirmative duty to investigate compliance issues and address complaints by EU citizens.

This duty was severely hindered, if not completely stripped away, through the Safe Harbor framework — allowing US organizations to choose whether to cooperate with EU Data Protection Authorities: "organizations may choose to cooperate and comply with the European Data Protection Authorities."

Unfortunately, this issue was not rectified in the new framework and, once again, the Privacy Shield ultimately contained the same language as the invalidated Safe Harbor. Businesses are allowed to decide whether they will cooperate with the DPAs: "US law will apply to questions of interpretation and compliance with the Principles and relevant privacy policies by Privacy Shield organizations, except where such organizations have committed to cooperate with European DPAs." Only companies processing HR data are required to cooperate with the DPAs. To comply with the CJEU's rationale, all organizations within the Privacy Shield must be legally obligated to cooperate with DPAs. Given these points, the new framework fails to adequately address the concerns raised by the CJEU, which only strengthens the growing sentiment that the Privacy Shield will not withstand the inevitable legal challenge.

Finally, we turn to whether the Privacy Shield meets the burden of providing an "essentially equivalent" level of protection for transferred data compared to the data protection guaranteed within the European Union. The CJEU stated that whether or not the United States could provide an equivalent level of protection would hinge on "the establishment of effective detection and supervision mechanisms."

Like the original Safe Harbor, the Privacy Shield allows businesses to self-certify their compliance with the new framework. This alone does not mean the framework is per se inadequate, but it does require that the Privacy Shield drastically improve oversight to ensure compliance with EU privacy standards. To address this issue, the Department of Commerce has committed to checking self-certification documents as well as maintaining a website that lists organizations that are certified and organizations that have been removed or that voluntarily withdrew.

Unfortunately, the letters from US federal agencies reassuring the European Union that they will enforce compliance do not include in-depth details about expanding or implementing new mechanisms to supervise organizations that have self-certified or ways to detect possible non-compliant behavior. The Department of Commerce (DoC) stated that it would be "conducting internet searches to identify where images of the Privacy Shield certification mark are being displayed … [and] monitor false claims of participation and misuse of the certification mark." So to adequately address this burden and ensure that the Privacy Shield survives legal challenges, the DoC will be "googling" companies to make sure they are not falsely using the Privacy Shield mark — how reassuring. Without stricter monitoring, it's entirely possible, if not likely, that a violation of the Privacy Shield by a US company would only be detected after irreparable harm has been inflicted on the data subject(s). As enacted, the detection and supervision mechanisms of the Privacy Shield are only "essentially equivalent" to the Safe Harbor mechanisms that were struck down late last year for being inadequate.

A key area of concern not addressed by the CJEU was brought to light by the Article 29 Working Party (WP29), which consists of regulators from all 29 member statesDPAs. In their opinion letter released April 13, 2016, the WP29 cited the inability of the framework to be amended in light of the inevitable implementation of the EU General Data Protection Regulation (GDPR). The GDPR will require a higher level of compliance than what is proposed in the Privacy Shield, yet the framework contains no provision that allows for amendments to ensure that the Privacy Shield will meet the new standard set by the GDPR when it becomes effective in April 2018. Without the ability to amend, the Privacy Shield will ultimately be found invalid when the GDPR's heightened standard becomes effective.

Clearly, there are some noticeable flaws in the Privacy Shield, but to classify the framework as a total failure is unfair given the great strides that have been made in bridging the legal gap between the European Union and the United States. However, without addressing the areas of concern highlighted within this article, it is unlikely that the Privacy Shield will survive a legal challenge in the CJEU and grow to become a long-term mechanism for in-house counsel to continue legal exchanges of data across the Atlantic. Unfortunately, it appears that these concerns will likely not be addressed, and any amendment to the now-enacted agreement is doubtful. US Undersecretary of Commerce for International Trade Stefan Selig stated that "[The US government is] very cautious about not upsetting what was a delicate balance that was achieved when we negotiated the original text, so would be chary about doing anything that would do just that."

Next steps

It is important to prepare accordingly and not completely rely on the Privacy Shield to ensure that the trans-Atlantic data flow may continue legally. Thankfully, there is a practical solution provided by the European Commission in two alternative mechanisms that will ensure the data exchange continues: standard contract clauses and binding corporate rules.

The European Commission adopted three sets of standard contract clauses that offer sufficient

safeguards as required by EU law. Essentially, use of these clauses allows organizations to legally transfer personal data outside of the European Union. These clauses are designed to ensure a sufficient level of protection, and companies that use them will benefit from favorable treatment (i.e., EU nations are legally obligated to acknowledge that the standard contract clauses fulfill the privacy requirements and therefore may not refuse the transfer except in limited circumstances).

The other mechanism, BCRs, are codes of conduct ensuring a sufficient level of data protection that organizations voluntarily adopt and follow. Companies draft the rules themselves and then submit them to the DPAs for approval. Once approved, the organization can legally transfer data between businesses that are part of the same corporate group that adopted the approved corporate rules.

It is important to remember that these alternatives are not guaranteed long-term solutions either. Since Safe Harbor's invalidation, both standard contract clauses and BCRs have come under fire and are potentially next on the chopping block for invalidation. Despite this, in-house counsel should consider adopting at least one alternative method to the Privacy Shield — ensuring a continued flow of data in the event that a method is invalidated. There are several factors to consider in an organization's decision of whether to adopt BCRs or standard contracts: among them the size of the company, the industry it does business in, and the type of data being stored. Ultimately, the best practice is to hire outside counsel who specialize in cybersecurity to provide guidance on the best alternative method to fit your organization's needs.

Determining the appropriate data exchange mechanisms is something every in-house counsel must consider, but completely relying on one mechanism, specifically the Privacy Shield, for a long-term solution is not advisable. Rather, self-certifying for the Privacy Shield along with adopting BCRs or standard contract clauses is quickly becoming the established best practice.

Further Reading

Schrems v. Data Protection Commissioner (Case C-362/14) Oct. 6, 2015.

EU-US Privacy Shield Principles Annex A: 6.

Article 29 Working Party, Opinion 01/2016 on the EU-US Privacy Shield draft adequacy decision.

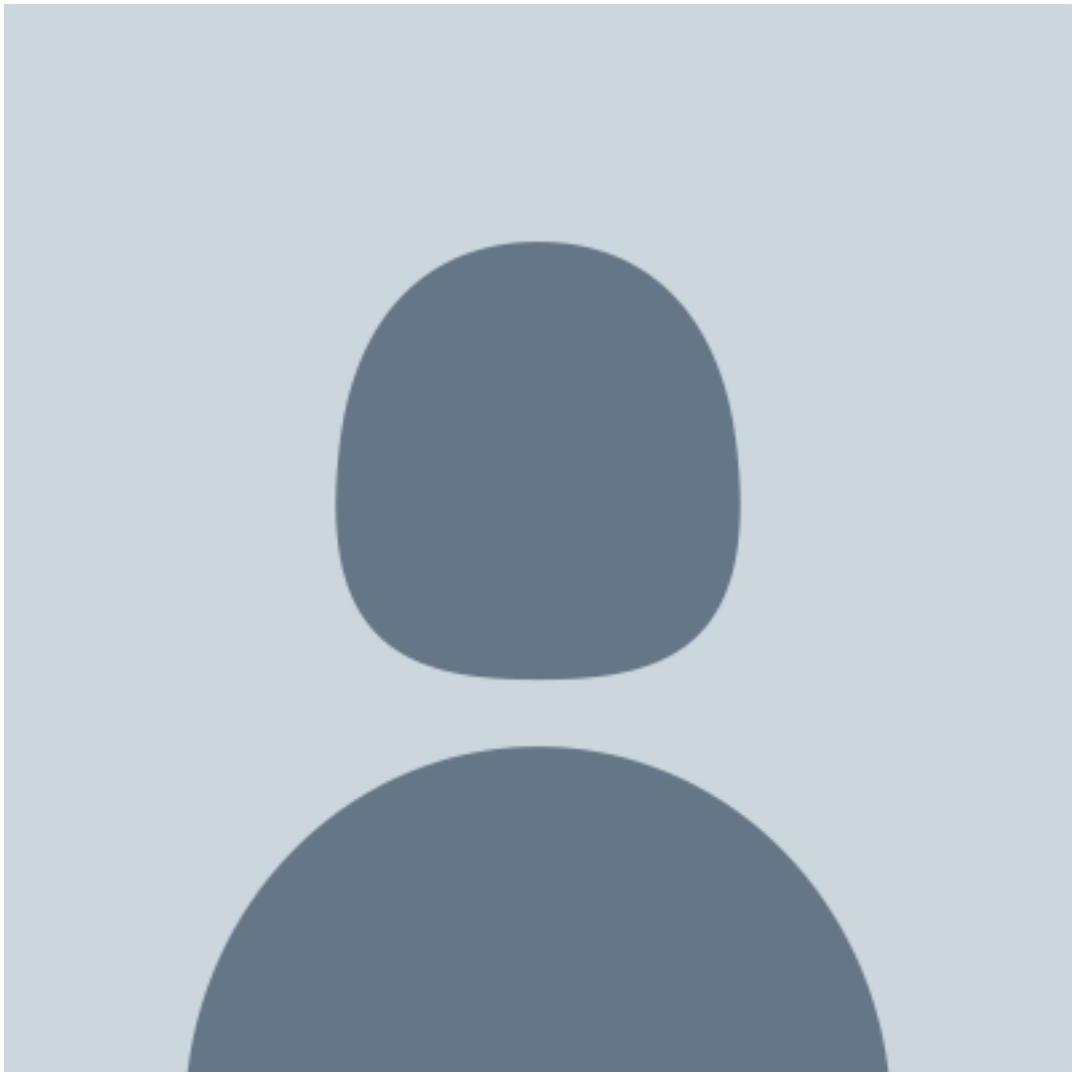
Summary: H.R. 1428 – 114th Congress (2015-16).

EU-US Safe Harbor Privacy Principles.

EU-US Privacy Shield Privacy Principles Annex II: I(7).

Letter from US Department of Commerce Undersecretary for International Trade Stefan Selig to Commissioner for Justice Vera Jourova.

[William Krouse](#)



Attorney

Iron Vine Security