DATA PRIVACY & SECURITY
SPECIAL REPORT
SEPT. 24, 2020

Making the Cut?

After EU judges struck down the Privacy Shield data-transfer agreement, what's next for US tech giants, thousands of other companies and regulatory regimes around the world?

mlex
a LexisNexis company

INSIGHT | COMMENTARY | ANALYSIS

Editor's Letter

Lewis Crofts
MLex Editor-in-Chief

A headache. A bombshell. A seismic shift. However dramatic you might like your metaphors, there is little doubt that EU judges delivered an extraordinarily significant ruling on July 16. In striking down Privacy Shield, the EU-US data-transfer framework, they instantly threw into doubt the operations of more than 5,000 US companies that relied on it.

The ruling — essentially based on the failure of the mechanism to protect EU citizens' data from US government snooping — doesn't prevent companies transferring data between the EU and other foreign countries under "standard contractual clauses." But these can't protect data in countries, including the US, that don't have protections for citizens' rights and privacy as tough as those in the EU. That drives a cart and horses through the procedures of thousands more US and European companies, notably Facebook and other tech giants.

This special report is a collection of key stories published by MLex in recent weeks making sense of this muddle, highlighting the areas of greatest regulatory risk for businesses and looking ahead, where possible, to spot emerging fixes.

We have arranged it in three thematic sections to reflect the multiple moving parts of the topic: 1) the EU court's decision and immediate effects on Facebook and other companies; 2) the scramble by the US and EU to work out what to do about replacing the binned agreement and making SCCs more robust; and 3) the concerns and responses by other affected countries around the world — including the UK, Japan and Australia.

We trust you enjoy reading this report and find it a useful guide to a complex, evolving issue. The reporting here is a brief example of the insight and predictive analysis that MLex brings subscribers to our data privacy and security service every day.

The stories included were all published as events unfolded, bringing our subscribers unrivalled insight into the significance of developments and the likely next steps in an issue that will affect the operations of many thousands of businesses around the world.

Data privacy and security represent a new major front in regulation, enforcement and compliance worldwide. MLex has been at the forefront of providing forensic and predictive insight, commentary and analysis on this emerging area of regulatory risk for years.

To find out more about our range of areas of interest and subscriber services — and to ask for a trial — see the contact details on the back page of this report or visit our website directly at mlexmarketinsight.com. ■

Contributors

Mike Swift

Chief Global Digital Risk Correspondent

Formerly chief Internet reporter for the San Jose Mercury News and SiliconValley.com, Mike has covered Google, Facebook, Apple and other major Silicon Valley companies closely as he followed trends in search, the mobile web and online social networks. He helps coordinate MLex coverage of privacy and data security worldwide. A former John S. Knight Fellow at Stanford University, he is a graduate of Colby College. He is an award-winning journalist with expertise ranging from the business of professional sports to computer-assisted reporting.

Matthew Newman

Chief Correspondent, Europe

Matthew writes about mergers, antitrust and cartel investigations as well as digital risk. Matthew began covering competition at the Luxembourg courts in 2004 and then moved to Brussels. After working as a spokesman for the European Commission until April 2012, he spent several months in Washington, DC writing about mergers for MLex. He spent a year studying French, history and communications in Grenoble, France and is a graduate of Boston University with degrees in history and journalism.

Vesela Gladicheva

Senior Technology, Media and Telecom Correspondent

Vesela reports on topics including telecom regulation, privacy, cybersecurity and copyright, focusing on EU regulatory and legal risk in the telecoms, media and technology (TMT) sectors. She holds a Master's degree in journalism from City University London, and works in English, Spanish, French and Bulgarian.

Sachiko Sakamaki

Senior Correspondent, Tokyo

Sachiko covers antitrust, anti-bribery & corruption, and privacy & cyber security. She has an undergraduate degree from Waseda University in Tokyo and a master's degree in communications from United States International (now Alliant International) University in California. She previously worked as a journalist for Time magazine, the Far Eastern Economic Review, Bloomberg News, and the Washington Post in Japan.

Dave Perera

Data Security & Privacy Reporter

Dave joined the Washington DC office as our new technology reporter as we built out that part of our coverage. He is a veteran cybersecurity reporter for Politico and a former editor for FierceMarkets publications. Dave studied Spanish and Italian literature at the University of Colorado, and has a Master's degree from the Columbia University School of International and Public Affairs.

Joanna Sopinska

Trade Correspondent

Joanna covers trade in Brussels. Formerly trade editor of EU Trade Insights, she has many years' experience reporting on trade, investment policy and foreign affairs. Before that, she spent nine years at Europolitics news agency writing on trade, agriculture policy and foreign affairs. Before moving to Brussels in 2006, Joanna worked as an analyst at the Polish Institute of International Relations (PISM) in Warsaw. She holds a postgraduate diploma in the European public affairs from Maastricht University in the Netherlands and an MA in international relations from University of Lódź in Poland.

Laurel Henning

Senior Correspondent, Sydney

Laurel is a senior correspondent covering data privacy and security, antitrust and mergers and acquisitions across Australia and New Zealand. Prior to that, Laurel spent a year spearheading MLex's activist investment coverage, looking at boardroom disputes and shareholder campaigns agitating for changes to company strategy. Laurel joined MLex in 2013 and reported for five years on European energy and climate policies from Brussels. In that time, Laurel covered the regulation of emissions and technological developments pertaining to the energy sector within the EU. A graduate of the University of Liverpool, Laurel studied English and French before beginning a career in journalism with MLex.

Jakub Krupa

Digital Risk Correspondent

Jakub joined MLex's London team in August 2020 to handle data privacy and security. Based in the UK since 2012, he previously worked as the UK correspondent for the Polish Press Agency, leading the coverage on Brexit, UK politics and relations with the EU. His stories also featured in other leading outlets, including The Guardian and the Evening Standard. He is also a regular commentator on Poles in the UK.

Introduction

Mike Swift
Chief Digital Risk Correspondent

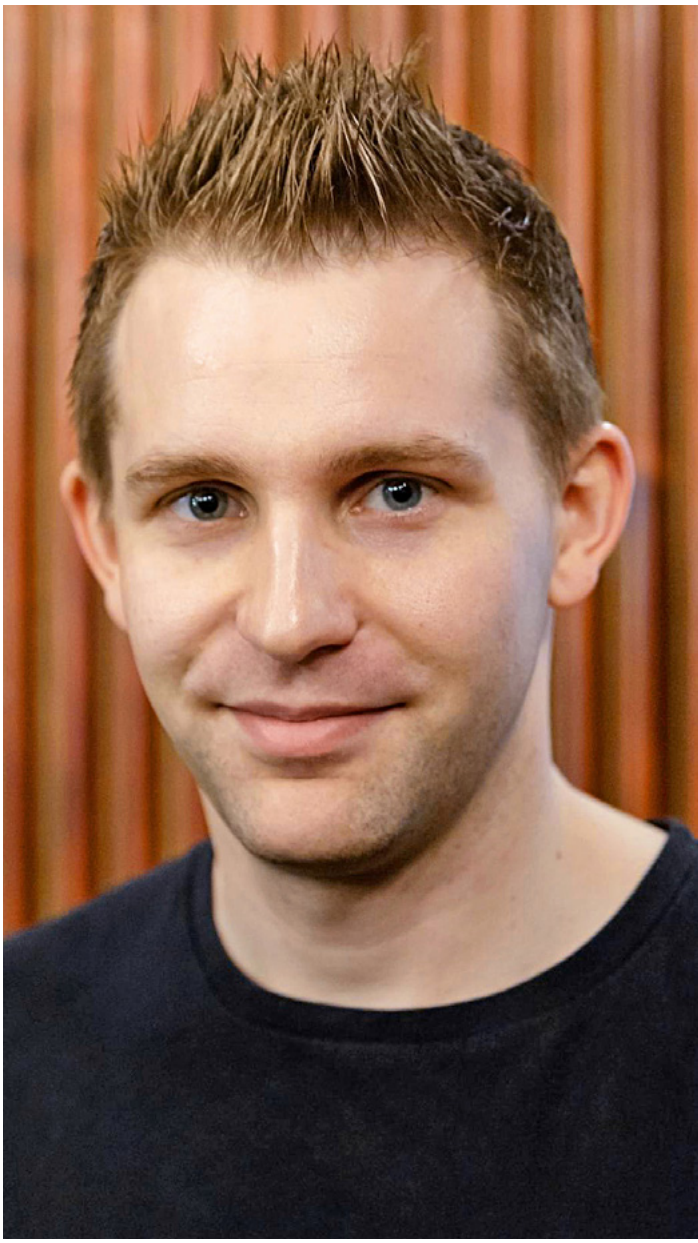
A data crisis erupted in July, when EU judges annulled the EU-US Privacy Shield and raised doubts about cross-border transfer mechanisms used by the likes of Facebook and other big Internet platforms. What happens next?

Max Schrems just won't go away. For the second time in five years, the legal basis for much of the world's data transfers has been thrown into question as a consequence of the Austrian privacy advocate's relentless efforts; after EU judges' invalidation in 2015 of the EU-US Safe Harbor trans-Atlantic data transfer framework in what became known as the "Schrems I" decision, this July came "Schrems II" that annulled that machanism's successor, Privacy Shield.

As EU and US officials this autumn negotiate a response to the EU Court of Justice's latest decision, which also dented the viability of "standard contractual clauses," or SCCs, as an international data transfer mechanism, their hope is to avoid experiencing déjà vu all over again, as baseball player Yogi Berra once put it in a trademark malapropism.

"I don't want to speak about a 'Schrems III' decision after another five years," EU justice commissioner Didier Reynders said ruefully during a recent video conference organized by the Brookings Institution in Washington. "Please not a Schrems III! So we need to find solutions."

Goodwill and rueful joking aside, crafting a trans-Atlantic data transfer system that will defeat or avoid a third challenge by Schrems won't be easy. It certainly won't be as



Double trouble: Austrian privacy campaigner Max Schrems.
Photo: Manfred Werner

straightforward as negotiations following the EU Court of Justice's Schrems I decision five years ago. That's in part because of the timing of the US national elections this fall, the likely need for US legislation to create a more durable solution this time around, and the potential handover of power in the White House and Congress.

The stakes are particularly high for US Internet giants such as Facebook that rely on contractual clauses as the legal basis to transfer the personal data of Europeans between the EU and US. Earlier this month, the Irish Data Protection Commission said that in the wake of the EU Court of Justice decision, Facebook couldn't use SCCs for trans-Atlantic data transfers. But within days, the social-media giant had won a reprieve when an Irish court on Sept. 14 suspended the Irish regulator's preliminary decision, granting Facebook the right to challenge it by judicial review. Other companies that rely on SCCs will be watching Facebook's defense with worried eyes.

Because SCCs are used to transfer Europeans' data worldwide, the ramifications of Schrems II are global. The continuing rounds of uncertainty in data transfers that are the basis for trillions of dollars of digital commerce are a powerful reminder of the value for a nation to permanently harmonize its local privacy laws with Europe's General Data Protection Regulation.

That goal has in recent years been on the minds of lawmakers and regulators in Japan, Canada, New Zealand, South Korea and Brazil — countries that have passed or are in the process of updating national privacy laws to be more in harmony with GDPR, with an eye to gaining an adequacy ruling with the EU.

Brexit, meanwhile, has thrown the UK into the realm of data-transfer uncertainty, as British negotiators race to get an adequacy deal with the EU before the end of the Brexit transition on Dec. 31. There, fault lines have emerged over the UK's intelligence surveillance regime and concerns about onward data transfers to the US. The Schrems II ruling has also caused uncertainty for Australia, which lacks adequacy status with the EU.

Whatever happens with Schrems' future court challenges, he can lay claim to one lasting victory from his multiple challenges to international data transfer systems. The more than 500 million affluent citizens of the European Union are a big, juicy carrot, drawing the rest of the world toward the strong privacy standard of the GDPR as they seek unfettered data transfers with the EU. ■

Because standard contractual clauses are used to transfer Europeans' data worldwide, the ramifications of Schrems II are global. The continuing rounds of uncertainty in data transfers — the basis for trillions of dollars of digital commerce — are a powerful reminder of the value for a nation to permanently harmonize its local privacy laws with the EU's General Data Protection Regulation.

Contents

Facebook and others' EU-US data transfers are valid, but Privacy Shield is invalid, top EU court says

INSIGHT

By Matthew Newman

Published on July 16, 2020

The mechanism used by Facebook and thousands of other companies to transfer EU citizens' data to the US has been ruled valid by the EU's top judges. There is "nothing to affect the validity of that decision" in the EU's Charter of Fundamental Rights, the Court of Justice said today. But the US-EU Privacy Shield is invalid, the court said.

The case stems from a lawsuit against Facebook by Austrian privacy activist Max Schrems, who is challenging Facebook's use of so-called standard contractual clauses, or SCCs, and the Privacy Shield agreement to transfer Europeans' data to the US. The Irish High Court referred questions on EU law to the EU Court of Justice in 2017.

Beyond Facebook, SCCs underpin data transfers for businesses in almost all sectors, from financial services and insurance companies to social-media platforms and cloud-computer server providers. Almost nine out of 10 companies used SCCs in 2019, according to a survey by the International Association of Privacy Professionals.

SCCs are sets of template contract clauses that comply with the EU's strict data-protection rules and have been approved by the European Commission. »»

Companies that export data and those that receive it sign these contracts, which bind them to certain commitments that protect the privacy rights of individuals whose data are transferred.

The clauses are needed because under the EU's General Data Protection Regulation, data can only be transferred to countries that provide "adequate" protection of EU citizens' privacy rights. The EU has adequacy decisions with only 13 countries, so SCCs are the most common way to legally transfer data.

Now that the EU court has validated SCCs, businesses in the bloc will be able to continue their international data transfers.

Regarding the EU's decision to approve the Privacy Shield, the court said "the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union ... are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programs based on those provisions are not limited to what is strictly necessary."

SCHREMS CASE

Schrems is the activist whose initial complaints about Facebook led to a landmark ruling in 2015 by the EU Court of Justice, where judges found that transfers of personal data to the US under the old regime, Safe Harbor, didn't provide an adequate level of protection.

Facebook moved from relying on Safe Harbor to using SCCs for personal data transfers to the US. Schrems mounted another complaint at the Irish Data Protection Commission, which referred the case to the Irish High Court. The Irish court then referred 11 questions to the EU Court of Justice.

The case reference number is C-311/18. ■

Beyond Facebook, SCCs underpin data transfers for businesses in almost all sectors, from financial services and insurance companies to social-media platforms and cloud-computer server providers. Almost nine out of 10 companies used SCCs in 2019, according to a survey by the International Association of Privacy Professionals.

EU-US digital trade 'in limbo' after Privacy Shield strikedown, with sudden risks for SMEs

A vast swath of trans-Atlantic digital trade has fallen into legal limbo after the EU's top court today invalidated the Privacy Shield, which enabled the transfer of personal data between the EU and the US.

Brussels and Washington will now have to negotiate a new adequacy agreement, which is almost certain not to happen before the US presidential elections in November and could take well into next year.

In the meantime, in order to continue transferring personal data across the Atlantic without the threat of significant sanctions and civil compensation claims, more than 5,000 companies registered with the Privacy Shield mechanism will have to rely on alternatives such as standard contractual clauses, or SCCs, as are already used by many large companies.

The court ruling puts at risk any digitally enabled transactions of trade in goods and services between the EU and the US — such as consumers' online purchases of books, tickets or holidays, as well as services such as cloud computing or Internet-connected devices — which involve the movement of data under the provisions of the Privacy Shield.

"We have to find an intermediate solution for the companies" to remove them from the legal limbo, said BusinessEurope director general Markus Beyrer. "We need some kind of moratorium on application of penalties" to offset the "heavy blow" that today's decision dealt to trans-Atlantic trade, he added.

The EU Court of Justice ruling today stemmed from privacy activist Max Schrems' challenge to Facebook's use of SCCs and the Privacy Shield to transfer data to the US. Judges said Privacy Shield doesn't provide adequate protection to European citizens, but they did uphold the SCCs used by thousands of companies to transfer EU citizens' data to the US as valid.

Since its launch in 2016, the Privacy Shield has been an essential tool for the smooth transfer of personal data across the Atlantic. About 70 percent of the framework's users are small or medium-size businesses, according to the US Department of Commerce, which oversees it with the Federal Trade Commission.

Its invalidation creates another trade hurdle, at a time when the US administration is threatening to hit the EU with billions of dollars in tariffs over digital taxes.

The EU Court of Justice struck down a previous framework, Safe Harbor, in October 2015, also as a result of a challenge by Austrian activist Schrems. The EU and US sides took until February 2016 to reach a tentative deal on a replacement — Privacy Shield — but this didn't come into force until July of that year.

The European Commission said it would open talks with the US on updating the Privacy Shield in line with today's ruling. Officials would be working "closely and constructively with our American counterparts with an aim of ensuring safe trans-Atlantic data flows," said V□ra Jourová, the bloc's rights commissioner.

But striking a new deal might be very difficult with US President Donald Trump's administration, which has proved hostile to privacy safeguards and has refused to limit its surveillance powers.

"We would like to see on the American side the federal law on data protection that would be equivalent or similar to the [General Data Protection Regulation], which would stipulate strong safeguards for the protection of private data of the citizens," Jourová said. "But we cannot do magic and change American laws from Europe."

Wilbur Ross, US Commerce Secretary, said the ruling was "deeply disappointing," but stressed that his department would "continue to administer the Privacy Shield program … Today's decision does not relieve participating organizations of their Privacy Shield obligations". ■

INSIGHT

By Joanna Sopinska

Published on July 16, 2020

US vows to limit fallout from European Privacy Shield dissolution

US officials say they will work to limit fallout caused by an EU Court of Justice ruling jeopardizing the flow of commercial data across the Atlantic, while acknowledging they are still analyzing the ruling's full ramifications.

The Luxembourg-based court today invalidated, for a second time in five years, the primary legal framework underpinning trans-Atlantic data flows, in a ruling holding wide-ranging effects for US companies with European customers.

Nearly 5,400 American businesses rely on the current mechanism, dubbed Privacy Shield, which is meant to guarantee European residents equivalent protection for their data even when held inside US data centers. Privacy Shield, now defunct in its current form, is the successor to the EU-US Safe Harbor Framework, which the court invalidated in 2015.

In both cases, the court doubted the mechanism's ability to protect Europeans' data from intelligence agency surveillance. "We are deeply disappointed," a senior US government official told reporters during a press call, speaking on condition of anonymity. The US is already in discussions with the European Commission and the European Data Protection Board on how to proceed, the official said, vowing that the two sides will be able to reach a new agreement.

INSIGHT

By Dave Perera

Published on July 16, 2020

"We're both democratic societies. We both value privacy, and so, we do have shared values," the official said when asked if the repeated EU Court of Justice rulings reveal fundamental trans-Atlantic incompatibility on handling data.

"We do have somewhat different approaches," the official acknowledged. But just as Privacy Shield succeeded the Safe Harbor Framework, another accord will succeed Privacy Shield, the official added. Asked when that might occur, the official declined to speculate. "I think it would be premature and irresponsible to provide any timeline at this point," he said.

EU Justice Commissioner Didier Reynders and the commission's vice president for values and transparency, Věra Jourová, told reporters they will discuss the next steps tomorrow with US Commerce Secretary Wilbur Ross.

In a statement, the Department of Commerce, which administers Privacy Shield, said it will continue to process certification submissions. The US hopes "to limit the negative consequences to the $7.1 trillion transatlantic economic relationship that is so vital to our respective citizens, companies, and governments," Ross said.

The court's ruling also throws into doubt whether a more tailored approach to trans-Atlantic data-sharing, dubbed "standard contractual clauses," remain an option for American companies. The Irish Data Protection Commission says use of contractual clauses is now "questionable" in the wake of the court's opinion.

The US official said he doesn't yet have an answer on that front. "We're still digesting the ruling."

Facebook, whose data-transfer practices lie at the heart of the European court case, said in a statement that it will "ensure that our advertisers, customers and partners can continue to enjoy Facebook services while keeping their data safe and secure."

A Google spokesman said the company has no statement. Twitter didn't respond to a request for comment. A Microsoft representative pointed to a blog post from its chief privacy officer asserting that today's ruling "does not change data flows for our consumer services." ■

Facebook's EU-US data transfers should be suspended, Irish regulator says in draft decision

Facebook Ireland shouldn't be allowed to use standard contractual clauses for trans-Atlantic transfers, the Irish Data Protection Commission has said in a draft decision. The move may force the tech giant to suspend the transfers and could dramatically affect how companies conduct business in a data-driven economy.

INSIGHT / COMMENTARY

By Matthew Newman

Published on Sept. 10, 2020

Facebook Ireland shouldn't be allowed to use "standard contractual clauses" for trans-Atlantic transfers, the Irish Data Protection Commission said in a draft decision, in a move that may force the tech giant to suspend the transfers and dramatically affect how companies conduct business in a data-driven economy.

After a landmark EU court ruling that annulled the EU-US Privacy Shield — a trans-Atlantic data transfer agreement — the Irish DPC began looking at the ruling's implications on Facebook's use of standard contractual clauses, which are model contracts guaranteeing that companies uphold data-protection rules, and whether they're a legal way to transfer users' data to the US.

The regulator told Facebook Ireland last month that its "preliminary view" is that the use of SCCs for trans-Atlantic transfers isn't lawful under the EU's strict General Data Protection Regulation, MLex understands. "I can confirm that … the Commission has now written to Facebook Ireland Limited, identifying the issues [that are] the subject of the inquiry," Ireland's duty data protection commissioner said in the letter, which was made public by Max Schrems, an Austrian privacy activist.

Schrems complained more than seven years ago about the legality of Facebook's data transfers to the US. His complaint followed revelations about US security agency's siphoning of data from US tech companies.

Facebook acknowledged the Irish probe, and said in a blog post yesterday that the authority "has suggested that SCCs cannot in practice be used for EU-US data transfers". "While this approach is subject to further process, if followed, it could have a far-reaching effect on businesses that rely on SCCs and on the online services many people and businesses rely on," a spokesman for the social-media company said.

The lack of legal certainty on data transfers "would damage the economy and hamper the growth of data-driven businesses in the EU," Facebook said. "The impact would be felt by businesses large and small, across multiple sectors."

STANDARD CONTRACTUAL CLAUSES

The issue of SCCs' legality is critical for multinational companies because after the Privacy Shield's annulment, they have been relying on SCCs and binding corporate rules to transfer EU citizens' data to the US. A ruling against Facebook's use of SCCs could cast doubt on their viability for other companies' transfers.

The Irish authority has given Facebook 21 days to »»

respond to the draft decision. After that, the authority will take on board Facebook's comments and circulate its draft to the EU's data-protection authorities. The DPC will then issue a final decision, which could be an order for Facebook to stop data transfers based on SCCs as a legal basis, as well as possible fines.

The Irish DPC, which began probing Facebook's use of SCCs in 2015, led to questions at the EU's highest court on the validity of SCCs and the Privacy Shield.

While the EU Court of Justice declared that SCCs are still valid, EU judges said data exporters must assess whether the countries to which data is sent offer adequate data protection under the EU's data-protection rules.

> *The Irish authority has given Facebook 21 days to respond to the draft decision ...The DPC will later issue a final decision, which could be an order for Facebook to stop data transfers based on SCCs as a legal basis, as well as possible fines.*

For Schrems, the ruling means the Irish DPC should declare that Facebook's data transfers are illegal and should be stopped. It doesn't need to conduct another probe into their legality, he said, and should focus on his original complaint. He complained that the inquiry will lead to further delays in ruling against Facebook. "The scope of the inquiry is insufficient and irrational," Schrems' lawyers said in a letter to the Irish DPC made public by his advocacy group, None Of Your Business.

The lawyers asked Facebook what legal basis it's using following the EU court's decision. The company said that the legal basis is "contractual services" as outlined in the company's data policy. Under Article 49 of the GDPR, companies can transfer data if the transfer "is necessary for the conclusion or performance of a contract concluded in the interest of the data subject."

Schrems' lawyers told the DPC that its inquiry into Facebook's current data transfer methods "will only cover a small aspect of the case before you." As a result, the lawyers asked the DPC to stop its inquiry and to focus on Schrems' complaint.

Noyb said in a statement that it's planning to file an interlocutory injunction to ensure that the DPC takes action on the entire alleged legal basis relied upon for data transfers by Facebook. The DPC said it will respond to the request on Friday, Noyb said. ■

Facebook's Irish court win eases pressure on privacy regulators over SCCs

Facebook's Irish court win over US data transfers this week has given other European privacy authorities some breathing room. Regulators are facing a barrage of complaints from privacy activist Max Schrems against companies' use of standard contractual clauses to transfer Europeans' data to the US, following a landmark EU court ruling in July. Central guidance is still urgently needed to ensure they handle the cases in a coherent way.

COMMENTARY

By Matthew Newman & Jakub Krupa

Published on Sept. 16, 2020

Facebook's Irish court win over US data transfers this week has given other European privacy authorities some breathing room to deal with a barrage of complaints that similar transfers are illegal under EU data-protection rules.

The Irish Data Protection Commission had drafted an order for Facebook to stop transferring Europeans' data to the US with immediate effect. But Facebook challenged the order on procedural grounds, and an Irish judge ruled on Monday that the company could pursue a judicial review against the decision.

In the meantime, Facebook can continue to transfer data to the US under a popular mechanism known as standard-contractual clauses, or SCCs. The judge set a new hearing for November, meaning that a final decision on Facebook's data transfers is months away at least.

That should ease the pressure on other European data-protection authorities, which last week formed two task forces to come up with guidelines on how to deal with complaints against the use of SCCs. The guidelines are essential to avoid contradictory approaches by different national authorities.

The uncertainty stems from a landmark ruling in July by the EU's top court. The primary effect of the judgment was to invalidate the EU-US Privacy Shield, a data-transfer tool used by more than 5,000 companies. But it also placed strict conditions on the use of SCCs, despite ruling that they are legal in principle.

That created an urgent need for clarity: More than 90 percent of multinational companies rely on SCCs for data transfers. And complaints have flooded in since the Court of Justice ruling: Austrian group Noyb, led by privacy activist Max Schrems — a protagonist in the EU court case — has alone filed 101 complaints against companies across Europe.

GUIDANCE NEEDED

Authorities across Europe will need clear guidance from their umbrella group, the European Data Protection Board, if they are to tackle these and other complaints in a coherent way.

David Stevens, the head of Belgium's data-protection authority, said that it's not "realistic" for companies to assess the appropriateness of a country's law enforcement and surveillance laws. Authorities could however develop codes of conduct for companies so that they can continue to transfer data, he said at a press conference* yesterday. »»

In July, a group of German regional data-protection authorities said additional safeguards are needed when organizations rely on SCCs or Binding Corporate Rules for the transfer of personal data outside Europe. Berlin's data-protection authority suggested that personal data should no longer be transferred to the US at all.

Switzerland, which is outside the EU but has its own data-transfer deal with the US, said that companies can no longer rely on the Swiss-US Privacy Shield. Companies that rely on SCCs need to carry out a risk assessment on a case-by-case basis and appropriate safeguards should be put in place.

COMMISSION MOVE

The European Commission is also under pressure to act quickly to ease companies' anxiety about the use of SCCs.

Following the entry into force of the GDPR in 2018, the commission had to update and modernize SCCs to take into account new ways of transferring data. For example, new model contracts were needed for transfer between an EU-based data processor and a non-EU-based sub-processor.

Ideally, the commission should be integrating advice from the EDPB on adequate measures when it updates the SCCs. However, it's not clear that the EU's data-protection authorities will reach an agreement quickly enough for the commission to amend its new model contracts.

Ideally, the commission should be integrating advice from the EDPB on adequate measures when it updates the SCCs. However, it's not clear that the EU's data-protection authorities will reach an agreement quickly enough for the commission to amend its new model contracts.

The commission will soon circulate its draft SCCs internally, MLex understands. The EDPB will then issue an opinion on them. Justice Commissioner Didier Reynders has vowed that they'll be ready by the end of the year.

These new SCCs will come some way to ease companies' concerns about new kinds of data transfers, but they won't answer the overarching problem of whether SCCs need to be amended, and how they should be changed to conform with the EU court's decision.

That guidance can only come from the EDPB or following a ruling by a data-protection authority. For now, it seems the authorities will hold off taking quick action, but they will eventually have to address Schrems' dozens of complaints. ■

**Scope Europe, Schrems II — Cloud Industry Unites to Create Global Standard for Transfer of Personal Data, Sept. 15, 2020.*

EU court's ruling may mean US must reckon with commercial impact of intelligence gathering

Today's decision by the EU's top court to void Privacy Shield and limit standard contractual clauses for international data transfers is arguably the most important data-protection ruling in years. As the second time that judges have struck down a key EU-US data transfer system, it may force the US at last to make a choice: spying or commerce?

COMMENTARY

By Mike Swift

Published on July 16, 2020

Today's decision by the EU Court of Justice to nullify the EU-US Privacy Shield and to limit standard contractual clauses for international data transfers is arguably the most important data-protection ruling in years, a decision that scrambles the existing global data-transfer order.

It's a ruling that raises plenty of questions, but few answers. For the US, the ruling places economic interests in stark conflict with national security, given the European court finding that American intelligence surveillance oversight is "not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law".

While there will be no immediate interruption of the digital trade between the US and EU that the US Chamber of Commerce values at $7.1 trillion a year, the EU Court of Justice ruling means the more-than-5,300 smaller and mid-sized companies that use Privacy Shield, as well as many companies that use standard contractual clauses to transfer data, can't continue with business as usual. »»

EU and US officials now will have to decide whether to propose more limited changes to Privacy Shield — a questionable strategy given that the EU Court of Justice has struck down both the Shield and the previous Safe Harbor data transfer scheme in October 2015 — or to pursue a completely different, as-yet unknown data-transfer approach.

The ruling could prompt US companies to store more of their data in Europe, perhaps by building data centers there. But that would also raise concerns about the growing global problem of data localization, as nations impose costs, limit access to new markets and potentially trigger more privacy problems as they increasingly assert their sovereignty over the international flow of data.

While the ruling highlights the glaring lack of a US national privacy law among developed nations, that wasn't the basis of the EU Court of Justice ruling, which was focused on the oversight of US spy agencies under the Foreign Intelligence Surveillance Act and US Executive Order 12333.

"The problem with the US is that there is no omnibus privacy law," privacy activist Max Schrems, who brought the case against Facebook that led to today's decision, told reporters at a briefing yesterday. But even if Congress were to pass a national privacy law, unless it also covered the bulk collection of data of non-US citizens by US intelligence agencies as well as commercial privacy practices, it wouldn't fix the problem identified by today's EU Court of Justice ruling.

For now, senior US officials acknowledge they don't really know what comes next, although they will work to limit fallout caused by the ruling. But there could also be opportunity for California, where voters will decide this year whether to move an existing state comprehensive privacy law even closer to the EU's General Data Protection Regulation.

Today's ruling also has ramifications for the UK, which as a result of Brexit is trying to negotiate a data-protection adequacy deal with the EU. Like the US, Britain has an active international intelligence network.

Caroline Louveaux, the chief privacy officer for Mastercard, compared her feelings after the ruling today to showing up for a university final exam having not done any preparation for the course. "There is total uncertainty," Louveaux said on a webinar organized by OneTrust that drew more than 2,000 worried participants.

WATER UNDER TROUBLED BRIDGES

There are three commonly used "bridges" to transfer the personal data of EU citizens to other jurisdictions with other privacy laws: Privacy Shield, contractual clauses and Binding Corporate Rules. "I have never been as happy as today that we went for BCRs," Louveaux said.

Lara Liss, the chief global privacy officer for the Walgreens Boots Alliance, likened the EU Court of Justice decision to a structural engineer who finds problems with the integrity of two train bridges — Privacy Shield and standard contractual clauses — although in this case, the "trains" carry personal data.

While the ruling highlights the glaring lack of a US national privacy law among developed nations, that wasn't the basis of the EU Court of Justice ruling, which was focused on the oversight of US spy agencies under the Foreign Intelligence Surveillance Act and US Executive Order 12333.

"What we heard this morning was that the Privacy Shield bridge is no longer structurally sound," Liss said. But even with the SCC bridge, companies will have to carefully check the destination and intervening stops of the data, Liss said, because the EU Court of Justice ruling means companies will have to decide whether the national laws where the data is exported are in conflict with the data-protection obligations in the SCCs.

"It creates more of an obligation on companies to really look at this very closely" when using SCCs, Liss said.

For California, where enforcement of the privacy provisions of the California Consumer Privacy Act began just this month, EU officials have said the CCPA could allow California and the EU to negotiate an »»

adequacy deal that would allow the free transfer of data without a mechanism such as Privacy Shield.

For California and Europe, "there are no obstacles to have adequacy," Bruno Gencarelli, head of the European Commission's international data flows and protection unit, said in 2018.

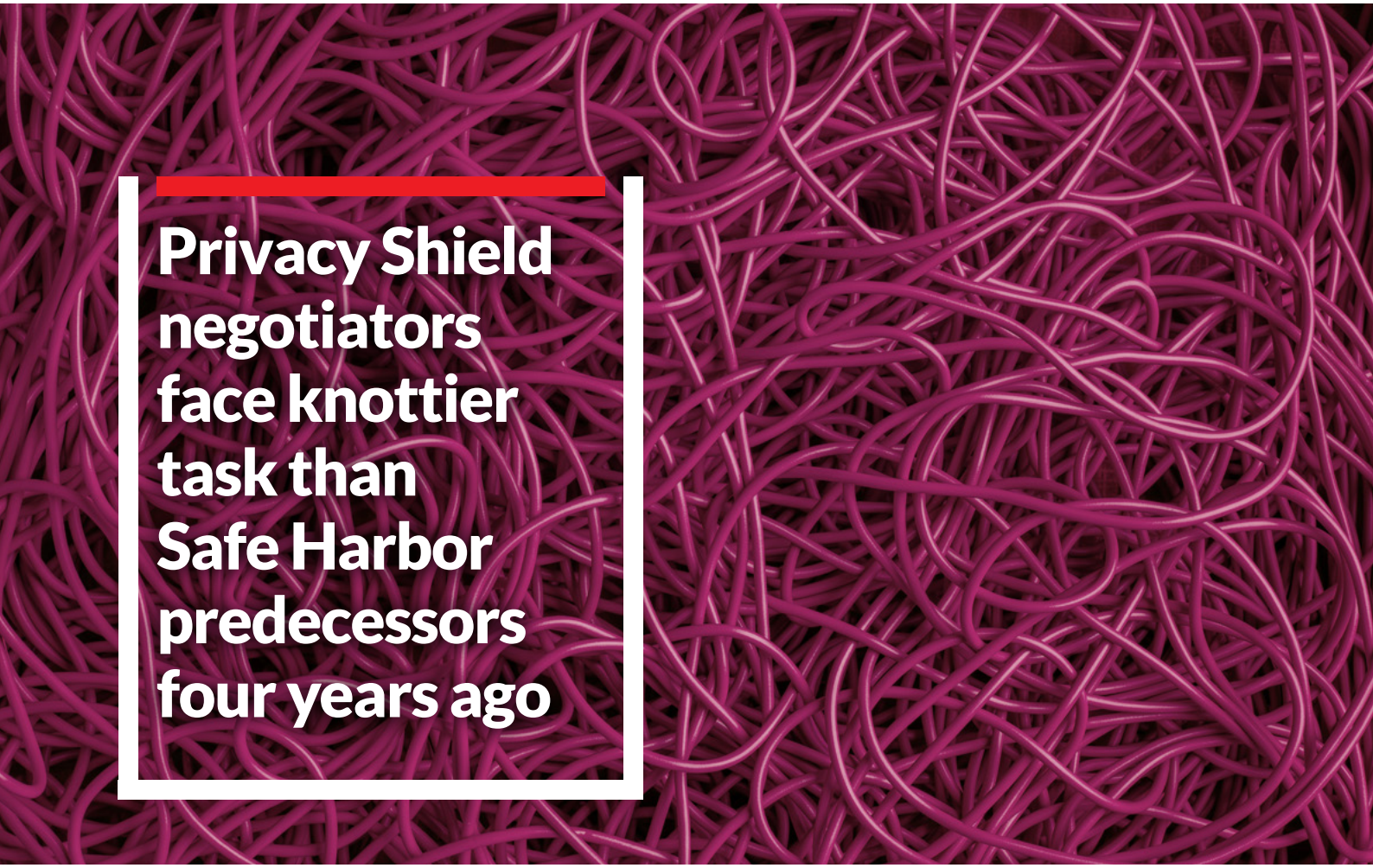
An adequacy ruling could be even more feasible if California voters pass the California Privacy Rights Act as part of a ballot initiative that will be decided in November. The CPRA would move the largest US state even closer to Europe's GDPR on privacy regulation, and even surpass its protections and sanctions in terms of the privacy of location and children's data.

Even back in 2015 when the EU Court of Justice nullified Safe Harbor, the predecessor of Privacy Shield, it appeared the US would have to make a choice — spying or commerce? And five years later, a key element of today's EU Court of Justice decision had to do with the "Ombudsperson" mechanism set up in Privacy Shield to deal with privacy complaints by Europeans about US intelligence activities.

The court found that the Ombudsperson mechanism lacks actionable rights before the courts against the US authorities, ruling that it "does not provide data subjects with any cause of action before a body which offers guarantees substantially equivalent to those required by EU law," according to a court summary of the decision.

For the US, the decision will likely mean federal officials must at last confront the question of whether bulk collection of data from non-Americans by US intelligence services is worth the economic harm of US companies being handicapped from selling their digital services in the 500 million-person European market.

In the confusing aftermath of today's position, it's impossible to predict how the winner of November's US presidential election will judge that question. ■



Privacy Shield negotiators face knottier task than Safe Harbor predecessors four years ago

When the EU Court of Justice invalided the "Safe Harbor" trans-Atlantic data transfer scheme in 2015, uncertainty about the legality of EU-US data transfers lasted several months. This time, the uncertainty following the court's decision to invalidate its successor could last longer, due to a list of complications that negotiators didn't have after the Safe Harbor decision.

COMMENTARY

By Mike Swift

Published on Aug. 26, 2020

US and European negotiators working on a successor to the now-invalid Privacy Shield face a difficult task, a problem that in several ways is significantly thornier than when they negotiated the last trans-Atlantic data transfer framework four years ago.

US and EU officials started talks about two weeks ago to replace the a trans-Atlantic data-bridge that is crucial to the data-driven economy on both continents, launching a process that appears likely to overlap the US presidential election in November and a potential transition of power in Washington.

That is one significant problem negotiators didn't face in 2016, when the Privacy Shield agreement that replaced the previous "Safe Harbor" framework was finalized nine months before that year's election. But it's not the only difficulty that negotiators must grapple with that they didn't have in 2016.

More than 5,000 companies rely on the EU-US Privacy Shield, which was declared invalid by the EU Court of Justice on July 16.

The EU Court of Justice had also invalidated the Privacy Shield's predecessor, Safe Harbor, in October 2015. At the time, there was significant concern about the sudden uncertainty regarding trans-Atlantic data transfers, but the uncertainty didn't last long. Within two months, officials were predicting a deal on a successor to Safe Harbor could be close. And just four months after the EU Court of Justice decision, in February 2016, EU and US negotiators had a deal on Privacy Shield.

This time around, the period of uncertainty could last longer. It has already been a month and a half since the EU Court of Justice's Privacy Shield decision, but there are no visible signs that a successor deal could be close. Asked for any details or other news about the current talks, a US Department of Commerce spokesperson today only referred MLex to the Aug. 10 joint statement from US Commerce Secretary Wilbur Ross and European Commissioner for Justice Didier Reynders that talks were getting started.

The coming months will be a fraught period in US politics, with US national elections just 10 weeks away. Congress, like the White House, will be distracted by the demands of the 2020 election. Every seat in the US House of Representatives is up for election, along with 33 of the 100 members of the US Senate.

The uncertainty and distraction generated by the election could slow down the data transfer talks. And even if a deal is reached before Election Day on Nov. 3, different people could be running the White House and the Commerce Department by the end of January. Those people could have different views on a deal reached their predecessors.

And Max Schrems, the Austrian privacy advocate who launched the two court actions that ultimately led to the invalidation of Safe Harbor and Privacy Shield, is not going away. Schrems' civil-rights group Noyb in recent days has filed a total of 101 complaints against EU-US data transfers, alleging violations of the EU General Data Protection Regulation in 30 European countries, including by Google and Facebook in the US.

The uncertainty and distraction generated by the US election could slow down the data transfer talks. And even if a deal is reached before Nov. 3, different people could be running the White House and the Commerce Department by the end of January. Those people could have different views on a deal reached their predecessors.

Privacy Shield, which created an ombudsperson role within the US State Department to field complaints from Europeans about privacy violations by US intelligence agencies, didn't require the involvement of the US Congress to put in place. But this year, the cupboard is somewhat bare for US options that don't require Congressional action.

One idea that has gotten some attention, for example, is to expand the role of the US Privacy and Civil Liberties Oversight Board. The five-member PCLOB investigates and evaluates the privacy risks of US intelligence programs, but its role is strictly advisory. Those familiar with the PCLOB agree that any change that would give it a more significant role in a new Privacy Shield say that would almost certainly require action by Congress.

After the successful challenges Schrems brought against Safe Harbor and Privacy Shield, it's clear that any deal cut between EU and US negotiators for a Privacy Shield successor will need to be able to withstand a European court review — a fact that just makes the job of the current negotiators tougher.

"The challenge is not the counterpart in the negotiation. It's that it will be ultimately tested in the courts," said a former US official close to the 2016 Privacy Shield talks, who spoke to MLex on condition of anonymity. "The complication is that it's not just solved by a political agreement where if a group of people get into a room, they can come up with something. It's that what those people come up with gets tested in a court by a different standard." ■

EU justice chief says standard contractual clause revisions will be complete by year's end

EU Justice Commissioner Didier Reynders predicted European officials will complete their post-Schrems II upgrade of standard contractual clauses by the end of 2020, even as he laid out three specific conditions for US officials to meet as the two sides negotiate a data transfer successor to the EU-US Privacy Shield.

INSIGHT / COMMENTARY

By Mike Swift & Matthew Newman

Published on Sept. 10, 2020

EU Justice Commissioner Didier Reynders predicted European officials will complete their post-Schrems II upgrade of standard contractual clauses, or SCCs, by the end of 2020, even as he laid out three specific conditions for US officials to meet as the two sides negotiate a data-transfer successor to the Privacy Shield.

Speaking on a webinar with the Washington-based Brookings Institution, Reynders urged US lawmakers to pass a comprehensive national privacy law, to have it include a court-redress system for both US and European citizens to address intelligence services' privacy violations, and for the US to move forward with an e-evidence deal with the EU, in order to come up with a durable and lasting solution for EU-US data transfers.

The EU had held off revising SCCs — model contracts guaranteeing that companies uphold data-protection rules — until the outcome of a landmark EU court ruling in July, known as "Schrems II," that annulled the US-EU Privacy Shield, the basis used by more than 5,000 companies to transfer data across the Atlantic.

While the EU Court of Justice declared that SCCs are still valid, judges said data exporters must assess whether the countries to which data is sent offer adequate data protection under the EU's data-protection rules. Once the revisions are complete by the end of this year, Reynders said, "we believe SCCs can continue to provide companies with an easy-to-implement tool to meet data transfer requirements."

He also acknowledged that the start of an Irish Data Protection Commission inquiry about the validity of Facebook's trans-Atlantic data transfers adds to the urgency of the SCC revisions.

The US and the EU have started talks on how to replace the Privacy Shield. The outcome of those negotiations is uncertain because of the complexity of conforming to the EU court's decision, which suggested the US revamp its surveillance laws to give EU citizens more rights to contest the unauthorized collection of their personal data.

Under the EU's strict General Data Protection Regulation, the bloc allows transfers of its citizens' data to foreign countries only if they provide an "adequate" level of protection. The original EU-US agreement, known as Safe Harbor, was annulled in 2015 after a challenge by Austrian privacy activist Max Schrems, who argued that the agreement should be invalidated following revelations of surveillance by intelligence agencies of US tech companies' data transfers.

Referencing the global trend toward nations passing comprehensive privacy laws, Reynders said it will be 'important that the US also goes in this direction ... It is clear that this increasing convergence in privacy laws around the world offers new opportunities to facilitate data flows.'

Photo courtesy of CTBTO

Reynders projected a sense of optimism about the EU-US talks to find a trans-Atlantic data-transfer solution after the EU Court of Justice's Schrems II decision invalidated Safe Harbor's successor, Privacy Shield, on July 16. But because US legislation will probably be necessary to accomplish the goals Reynders outlined today, EU and US negotiators face a more difficult environment then in 2015 and 2017, when the EU Court of Justice invalidated Safe Harbor.

Referencing the global trend toward nations passing comprehensive privacy laws, "it will be important that the US also goes in this direction," Reynders said. "It is clear that this increasing convergence in privacy laws around the world offers new opportunities to facilitate data flows."

Reynders said that if the US changes its privacy rules to give its citizens more rights to contest the use of their data by intelligence service and law enforcement, then it would be important to give those same rights to EU citizens. "If you give a new protection to US citizens it would be easier to give the same protection to the EU citizens, and it will be more of problem of the enforcement of the rights then something else," he said.

"If we are doing that, it would be possible to avoid a Schrems III decision and to work with an adequacy decision and solid basis for all the companies," he said, referring to a possible challenge of a new EU-US data-sharing agreement that would wind up at the EU courts again in future years.

Offering redress to EU citizens over intelligence agency privacy violations is a key requirement for a new agreement, he said. "The most difficult issue is in relation to the national security," he said. "It is there we have some things to do."

Reynders also highlighted the importance of the EU and US to complete their negotiation of an e-evidence agreement that would allow law enforcement agencies in the EU or US to directly access electronic crime evidence from online platforms in the other jurisdiction.

"The Commission is committed to work on an international agreement with the US that would eliminate conflicts of law," he said, acknowledging that the European Parliament needs to complete its own work on proposed e-evidence legislation first.

Reynders said that based on privacy laws either proposed or passed in the states of California and Washington, he's optimistic the US is already moving in the same direction as the rest of the world to codify fundamental privacy rights for its citizens.

Challenged by an American questioner about whether the EU is imposing its own privacy values over the needs for systems to be interoperable across international boundaries, Reynders suggested that both are possible, and highlighted ongoing data-transfer adequacy talks with South Korea and the UK as he argued that privacy values are converging globally.

"We try to make sure the protection is traveling with the data," he said. "So it's not first a trade issue, it's first a protection for fundamental rights for citizens."

The EU, he added, "is very open to exchanging data with other partners, but again, we want to make sure the protection is traveling with the data." ■

UK uncertainty over EU data-transfer deal grows as Brexit deadline nears

The UK's prospects of maintaining a free flow of data with the EU after Brexit by clinching a deal with the bloc this year are looking increasingly shaky as the clock ticks down. Fault lines have emerged over the UK's surveillance regime and concerns about onward data transfers to the US, as well as around likely plans for a more business-friendly data privacy framework. And the recent EU court ruling that blew up the EU-US Privacy Shield transfer mechanism has only complicated matters.

COMMENTARY

By Matthew Newman & Vesela Gladicheva

Published on July 31, 2020

The UK's prospects of maintaining a free flow of data with the EU after Brexit by clinching a deal with the bloc this year are looking increasingly shaky as the clock ticks down.

Both sides aim for a deal before the Brexit transition period ends on Dec. 31, but they will have to overcome fault lines that have emerged over the UK's surveillance regime and concerns about onward data transfers to the US. Likely plans for a more business-friendly data privacy framework are also a sticking point.

Without an EU decision that UK data-protection rules provide "adequate" protection for the bloc's citizens, EU companies and EU-based affiliates of UK companies will have to find another legal basis for data exports to the UK. It's worth noting that flow helped drive economic activity worth about 42 billion pounds ($54 billion) in 2018, according to the UK government.

In a data-driven economy, any hindrance to the free flow of information from social media, retail, insurance and financial-services companies would significantly hike costs and give rise to legal uncertainty.

All these factors underscore the size of the task the UK faces, and the importance of the outcome, as it strives to secure a data adequacy deal. And more: if the British government can't get this deal done, that could deliver a setback to the country's standing just as it is positioning itself to take a new global role.

SURVEILLANCE REGIME

Broadly, to secure an adequacy agreement, countries must ensure that their data-protection laws are "essentially equivalent" to the EU's General Data Protection Regulation.

The UK is confident that its data-protection rules meet EU standards and that nothing stands in the way of an adequacy decision. After all, its main privacy law, the Data Protection Act 2018, is based on the GDPR; it has a world-class data-protection authority, the Information Commissioners' Office, or ICO; and it has a robust judicial system that could handle surveillance-abuse complaints.

But a landmark EU court ruling that annulled a key trans-Atlantic data-transfer mechanism has put the spotlight on a delicate and potentially problematic aspect of the UK's privacy and security regime: Its intelligence-gathering may be too similar to that of the US, particularly when it comes to mass surveillance of citizens.

The EU Court of Justice on July 16 struck down »»

The UK remains vulnerable to the same concerns that prompted Schrems to challenge Facebook's Ireland-to-US data transfers ... With a real prospect of a UK adequacy decision coming under legal attack, the European Commission may want to hold off and save itself from another embarrassing court reversal.

the EU-US Privacy Shield, saying it doesn't provide citizens with protection equivalent to the GDPR. Judges considering a challenge by privacy activist Max Schrems over Facebook's Ireland-to-US transfers of data said they were concerned that US "surveillance programs ... are not limited to what is "strictly necessary".

This Schrems II ruling has amplified concerns that UK surveillance practices could get caught in legal and political headwinds similar to those in the US. These strengthened after Edward Snowden's revelations in 2013 that US intelligence services harvest private data from big tech companies such as Facebook.

Worries about the UK's close intelligence ties to the US and its security laws might end up delaying and politicizing the European Commission's adequacy decision.

Rights advocacy groups have challenged the UK's surveillance regime, enshrined in the Investigatory Powers Act 2016, which allows the mass collection and retention of citizens' data. This is a breach of fundamental EU privacy rights, the groups argue.

A case* brought by Privacy International and sent to the EU Court of Justice for clarification bolstered those arguments. A legal opinion for the court said in January that "general and indiscriminate" data retention of all users is "disproportionate," and it recommended that judges prescribe limits. A ruling is expected later this year.

The UK has said that its regime is in line with EU court rulings, particularly 2016's landmark Tele2/ Watson judgment**. This laid down that blanket data collection was unlawful and that only the data of those suspected of serious crimes should be accessed.

ONWARD DATA TRANSFERS

Nevertheless, the UK remains vulnerable to the same concerns that prompted Schrems to challenge Facebook's Ireland-to-US data transfers. Talks are now likely to focus on onward data transfers from the UK to the US.

With a real prospect of a UK adequacy decision coming under legal attack — especially if the EU court backs Privacy International later this year — the European Commission may want to hold off and save itself from another embarrassing court reversal.

Meanwhile, privacy activists may target the UK's role in the Five Eyes intelligence sharing group, alongside the US, Canada, New Zealand and Australia. They are concerned the UK may become a backdoor to the US. »»

If the UK does get an adequacy deal, it could take much longer than the rest of this year to seal it. It could also come with strict conditions, such as on onward transfers — highlighting a post-Brexit period of legal uncertainty for companies. What's more, any deal will likely depend on how the EU and the US agree to patch up or replace Privacy Shield, to ensure UK companies can transfer data to both Europe and America.

BUSINESS-FRIENDLY REGIME

A major focus for the talks will be on how the UK may amend its version of the GDPR to make it a more business-friendly framework. As it looks for its post-Brexit place in the world, Britain may well aim to attract US and other global companies by trimming red tape.

Proponents of an EU-UK deal and lobbyists from the business community will say that a slight move away from the GDPR shouldn't be pose problems for Brussels. That's because Britain would still be in a better adequacy position than countries granted EU adequacy but that don't apply the GDPR, such as Canada, New Zealand and Japan.

At the same time, some will point to a UK-US accord last year on sharing electronic data for criminal investigations, while others highlight a failure by the ICO to show its muscle with prompt and punitive fines on British Airways and Marriott International over customer data breaches. Fine decisions there have been delayed by up to a year, and are expected to be a fraction of what the regulator had originally proposed.

WHAT IF THERE'S NO DEAL?

If the EU refuses to grant the UK a data adequacy agreement, that will mean a new level of difficulty for companies. That's especially true for those based in the EU, which would have to find another legal basis to transfer data to the UK. In reality, that most likely means they'll need to rely on "standard contractual clauses," or SCCs — model contracts guaranteeing that companies will uphold data-protection rules.

In the Schrems II ruling, EU judges said SCCs were still valid but cast doubt on their continued use. They said SCCs can only be used where the law of the non-EU country to which a company is importing data provides protection that is "essentially equivalent" to the GDPR.

Transfers to the UK under SCCs thus face a greater risk of disruption, if local data-protection authorities in EU countries decide to question and even suspend them.

The nightmare scenario will be where Britain doesn't get an adequacy deal and SCCs are invalidated —something companies now see as a real prospect following the Schrems II ruling. That would effectively remove any realistic legal basis for data transfers from the EU to the UK.

Some lawyers are advising clients to take a wait-and-see approach. SCCs will have to be amended on the basis of commission revisions flowing from the ruling.

The European Data Protection Board, which brings together EU privacy enforcers, has said it will provide more guidance on data-transfer tools, including SCCs, as well as binding corporate rules, or BCRs, for intra-group transfers. It's looking into what kind of "supplementary measures" — whether legal, technical or organizational — could be put in place so that companies could continue to rely on SCCs and BCRs.

All things being equal, the UK should — in the end — secure an adequacy deal from the EU. But much is riding on its efforts to get over the line, as failing would be a major embarrassment to the island nation at a time when it wants to be seen as a reliable, even pioneering global partner. ■

**Case C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service*

***Case C-203/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*

Privacy Shield ruling sparks uncertainty in Australia and New Zealand

The invalidation of the mechanism used by thousands of companies to transfer EU citizens' data to the US is causing uncertainty as far afield as Australia and New Zealand. The ruling is causing particular concern in Australia, which doesn't enjoy adequacy status with the EU's landmark General Data Protection Regulation for its national-privacy law.

INSIGHT

By Laurel Henning

Published on Aug. 5, 2020

The invalidation of the mechanism used by Facebook and thousands of other companies to transfer EU citizens' data to the US is causing concern as far afield as Australia and New Zealand.

With Europe's top court nullifying the EU-US Privacy Shield last week, Australian and New Zealand companies and subsidiaries of US businesses that were relying on the Privacy Shield certification have been thrown into uncertainty.

AUSTRALIA

The ruling by the EU's top judges is causing particular concern in Australia, which doesn't enjoy adequacy status with Europe's landmark General Data Protection Regulation, or GDPR, for its national-privacy law.

Businesses in Australia and New Zealand can still put in place standard contractual clauses, or SCCs, to govern data transfers but should expect these to face closer scrutiny following the ruling.

Robyn Chatwood, a partner at Melbourne law firm Dentons, told MLex companies could face some disruption to putting the SCCs in place if they aren't already in use.

But more pressing for Australia, Chatwood said, is the bloc's consideration of personal-data transfers in the context of surveillance activities.

"The [EU Court of Justice's] view is that surveillance programs need to grant EU data subjects rights that are actionable in the courts against the authorities in order to provide an effective remedy," Chatwood said.

That's a problem for Australian legislation designed to grant law-enforcement agencies the right to request access to encrypted data from messaging services such as Viber and Whatsapp.

A parliamentary inquiry into Australia's law, which dates to late 2018, recently heard that the measures are prompting concerns from EU customers of Australian software who are worried they could face access orders that will make products less secure and weaken global supply chains.

The Australian law has limited or no redress for data subjects, Chatwood says. That means that even if Australian companies rely on SCCs for data transfers, there is a risk these would be deemed invalid by the EU, because the protections for individuals would remain inadequate.

Australia's privacy watchdog did not respond to a request for comment.

NEW ZEALAND

Over the Tasman Sea, New Zealand's Privacy Commissioner told MLex it is closely monitoring the situation following the EU ruling.

New Zealand's adequacy status with the EU's GDPR means data flows for now are done relatively easily.

"While New Zealand's EU adequacy status means the EU-NZ data flows are not directly affected … by the decision, we are considering the broader implications," a spokesperson for the Office of the Privacy Commissioner said.

> *A parliamentary inquiry into Australia's law recently heard that the measures are prompting concerns from EU customers of Australian software who are worried they could face access orders that will make products less secure and weaken global supply chains.*

The EU is currently reviewing New Zealand's adequacy status, with the country's updated privacy law set to enter into force on Dec. 1.

The privacy watchdog is planning to publish a blog post shortly to give an overview of the decision to New Zealand businesses.

Kristin Wilson, a senior associate at New Zealand law firm Bell Gully, told MLex the updates to New Zealand's privacy law "should move us further towards retaining adequacy status."

"But [the EU ruling] signals a heightened concern from Europe and, in particular, the Court of Justice to ensure that third-party countries actually do have the proper standards in place that are essentially equivalent to GDPR," Wilson said.

Wilson added that when the GDPR entered into force there was a lot of concern in New Zealand about its extraterritorial aspect that could see companies in New Zealand facing 20 million-euro fines.

"One issue that's still unclear is how exactly GDPR is enforced in organizations that are outside of the EU in practice," she said. "This is an area where we're still waiting [to see how it plays out]." ■

Breakdown of Privacy Shield raises Japan's concerns about impact on its data-flow review with EU

As Japan's data-transfer deal with the EU approaches its first review four months from now, Japanese privacy specialists and regulators are alarmed about the impact of the landmark European court decision nullifying the EU-US Privacy Shield.

INSIGHT

By Sachiko Sakamaki & Mike Swift

Published on Sept. 16, 2020

As Japan's data-transfer deal with the EU approaches its first review four months from now, Japanese privacy specialists and regulators are alarmed about the impact of the landmark European court decision nullifying the EU-US Privacy Shield.

Japan's efforts over the past two years to provide stronger privacy protections by amending the main national privacy law and increasing enforcement efforts by Japan's Personal Information Protection Commission, or PPC, have prompted a degree of optimism about the durability of the EU data-transfer deal.

But the July 16 decision by the EU Court of Justice underscores the EU's strict stance on the privacy and transfer of personal data, a stance that some officials and experts fear may make the review of the EU-Japan adequacy deal more challenging.

"The European Union may scrutinize government access to personal data more strictly, and we're prepared to explain fully, when asked," Kiyoshi Sawaki, the PPC's deputy secretary general, told MLex, adding that Japan's overall situation regarding government access hasn't much changed in the past two years.

GOVERNMENT ACCESS AND REDRESS

Hiroshi Miyashita, associate law professor at Chuo University, told MLex that the EU Court of Justice's clarification of three conditions for data flows under the EU's General Data Protection Regulation, or GDPR — appropriate safeguard, enforceable rights and effective legal remedies — affects Japan.

"Japan should take measures before an incident surfaces to secure effective legal remedies," said Miyashita, who added that he's not worried about the maintenance of the Japan-EU adequacy decision.

He predicted, however, that these conditions will be looked at when mutual adequacy decisions between the EU and Japan will be reviewed in January.

To respond to the EU's concerns about a redress system in Japan for European citizens with privacy complaints about their data imported to Japan, the PPC has set up an English phone line to handle the concerns of European individuals. Those concerns were expressed during the negotiations for the first agreement.

The PPC hasn't published how many complaints from European citizens it has received regarding how their privacy rights were handled by Japanese companies and other entities.

The lack of a redress system within the US courts »»

for European citizens with complaints about privacy violations by American intelligence services or other government agencies was a significant reason why the EU Court of Justice nullified the Privacy Shield. That same decision also cast doubt over the use of standard contractual clauses as the basis to transfer data internationally.

Yoichiro Itakura, a lawyer specializing in data protection at Hikari Sogo Law Offices, said Japan may face questions and requests from the European Data Protection Board and the European Parliament about the Japanese government's access to personal data.

Voluntary disclosures by private entities of personal data to the public authorities in response to their requests through an "enquiry sheet" are still going on, while EU scrutiny is rising. This raises a concern, he said.

EU'S DATA-FLOW DEALS

Japan is one of 12 countries whose laws have been recognized by the European Commission as providing data protection "adequate" to EU citizens, a list that includes Argentina, Israel, Canada, Switzerland and New Zealand. EU adequacy talks are also ongoing with South Korea.

The US lacks a national privacy law, and it has not qualified for an adequacy deal with the EU. But prior to July 16, the Privacy Shield allowed more than 5,000 companies to make trans-Atlantic data transfers by certifying they would adhere to EU privacy principles.

Japan's PPC and its European counterpart are currently working on the review of the data-flow agreement between Japan and the EU, based on mutual adequacy decisions regarding data protections, due in January 2021.

After Japan won the EU's first adequacy finding following the GDPR's 2018 effective date, optimism has prevailed. Japan's main privacy law — the Act on the Protection of Personal Information — was amended in June to strengthen individuals' privacy rights, and the PPC has stepped up enforcement against data misuses.

"I don't think the Japan-EU data-transfer mechanism will be nullified, but Japan should work to curb government access [to data], and the PPC should continue to work on active enforcement," said Itakura.

The PPC's Sawaki also said the legal amendment, seen by Europe as coming closer to the GDPR, may have created a favorable environment for continuing the data-transfer agreement with the EU.

JAPAN, THE EU AND THE US

Japan, meanwhile, has been promoting trilateral talks with the EU and the US on free and secure data flows since last year. Japan occupies a middle ground on personal data between the EU, which highly values the privacy rights of individuals and the US, which prefers freer data trade.

Sawaki said the trilateral framework talks are moving forward, unaffected by the Privacy Shield's invalidation. Regulators in the three jurisdictions are also cooperating at the Organization for Economic Co-operation and Development, or OECD, to restrict excessive government access to personal data and data localization, he said. "Cross-border data transfer between the EU and the US is important for Japan and the world. The two sides will somehow overcome [the current situation], and Japan is ready to offer support for that." Sawaki added that some Japanese companies may be inconvenienced by the Privacy Shield's invalidation.

As part of the work related to the trilateral framework, the PPC is conducting a survey on the need for onward transfers of data among the private sector, he added.

While the US is intensifying its campaign to promote a cross-border mechanism under the Asia-Pacific Economic Cooperation, or APEC, forum as a better data flow mechanism than the GDPR, in Japan, lawmakers are joining the US to restrict Chinese apps like TikTok over concerns about data security and national security.

Miyashita of Chuo University said Japan should take the middle ground between the US, which values national security, and the EU, which emphasizes privacy rights, and take an intermediary position.

"This could be a chance for Japan to play an intermediary role between the two," Miyashita said. ■

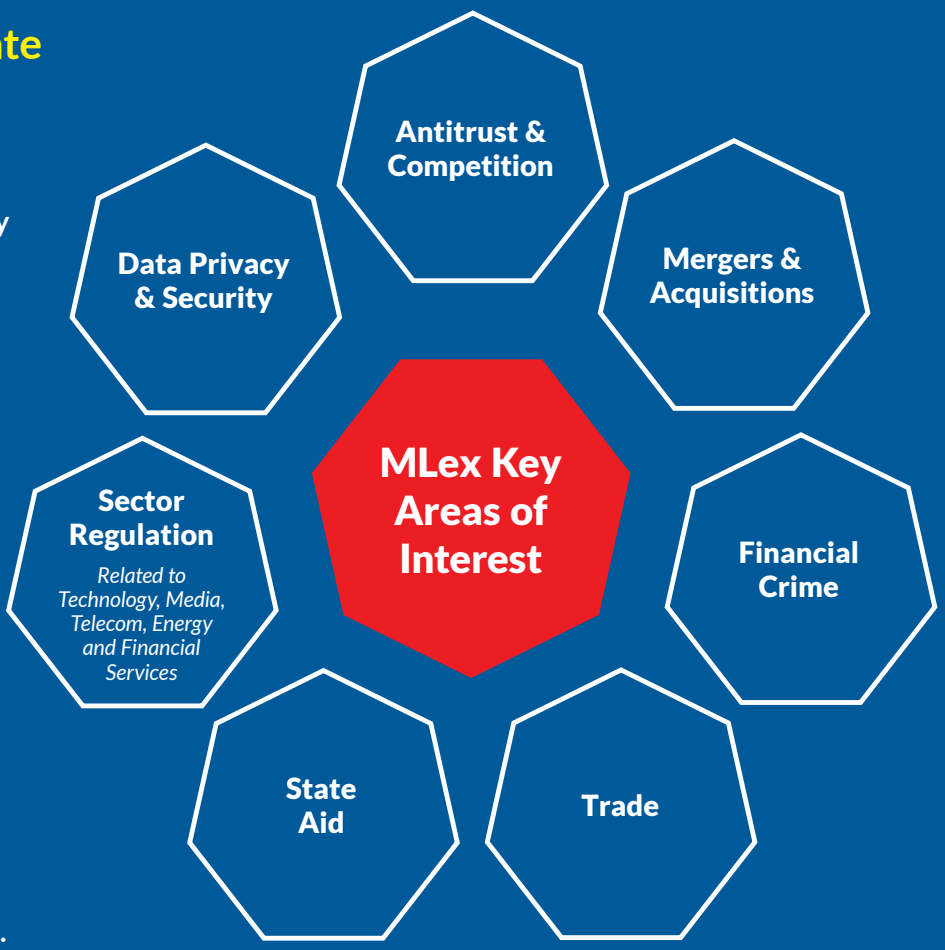
MLex Insight • Commentary • Analysis

Confidently Navigate and Respond to Regulatory Risk

Stay ahead of key regulatory issues with expert insight, commentary and analysis to ensure you are advising your clients on how to best navigate complex, global enforcement environments.

MLex is on the cutting edge of reporting on global regulations, both in effect and proposed.

Our exclusive, real-time coverage of probes, enforcement trends, litigation and regulator commentary help ensure you are informed and able to respond immediately to client risks and opportunities.



The MLex Difference

- We have a singular focus on regulatory risk, providing unrivalled expertise across our team of 80+ reporters around the world.
- Through longstanding relationships with regulatory communities we keep you informed of developments ahead of mainstream media.
- We insist on the highest standards of sourcing and accuracy in our editorial process.
- Unbiased and forensic reporting ensures our clients get the information they need.

Our Global Presence

Our journalists cover the world from 14 bureaux in key jurisdictions:
EUROPE: Brussels • London **AMERICAS:** Washington • New York • San Francisco • São Paulo
ASIA: Hong Kong • Beijing • Shanghai • Seoul • Tokyo • Jakarta • Melbourne • Sydney

mlex
a LexisNexis company

UK +44 800 999 3237
US +1 800 356 6547
EU +32 2 300 8250
HK +852 2965 1424
www.mlexmarketinsight.com
customerservices@mlex.com