

EU-US Privacy Shield is a success, so far

First year was a good year, but review findings due soon. **Robert Belair** of Arnall Golden Gregory LLP offers his insights on how the arrangement is working.

It has now been over a year since the 12 July 2016 decision by the EU Commission that the Privacy Shield Accord is adequate to enable transfers of personally identifiable information (PII) from EU member nations to the US. On 1 August 2016, the US Department of Commerce began accepting self-certifications from US companies for participation in Privacy Shield.

During the week of 18 September 2017, the European Commission, along with eight members of the Article 29 Working Party, and the US Department of Commerce and the Federal Trade Commission, conducted a review of Privacy Shield's effectiveness. *Věra Jourová*, the EU's Justice Commissioner, called the review, to be followed by a late October report, a "moment of truth" for Privacy Shield.

Is it? Both the EU and the US have too much invested in, and at stake in, the Privacy Shield Accord. It is conservatively estimated that Privacy Shield supports about \$300 billion in EU-US trade annually. What's more, there are very few attractive alternatives to Privacy Shield. Simply stated, Privacy Shield must succeed – and, therefore, will succeed.

PRIVACY SHIELD – A THUMBNAIL SKETCH

Privacy Shield is the successor to Safe Harbor. Like Safe Harbor, Privacy

practice" principles found in Safe Harbor – notice, choice, onward transfer protection, security, data quality/integrity, subject access and enforcement.

But, Privacy Shield enhances controller accountability; creates greater responsibility for controllers for onward transfers; makes controllers more responsible for the actions of their processors and service providers; emphasizes data minimization; provides more accountability through binding arbitration; creates a Privacy Ombudsman in the US Department of State; and enhances and expands several other privacy protections.

As was the case for Safe Harbor, Privacy Shield is available only to organizations subject to Federal Trade Commission (FTC) and Department of Transportation jurisdiction. Thus, depository institutions and many other financial service providers, telecommunications providers, trade unions and many not-for-profits, as well as certain other types of organizations, are not eligible. In common with Safe Harbor, Privacy Shield does not cost very much. Organizations are spending about \$1,000 per self-certification submission.

So far, more than 2,500 organizations have self-certified. Admittedly, this compares poorly to the over 5,000 organizations which self-certified in the roughly ten-year period beginning

revenues over 500 million dollars. But, there are some behemoths, as well, including Google and Facebook.

So far, no one in the US seems to be complaining. In fact, the US Department of Commerce reports that they have not received even one valid complaint about Privacy Shield. The FTC tells a similar story. Furthermore, there have been no referrals of complaints from any EU data protection authorities.

So, why haven't more companies signed up? Mostly, it seems that US companies are watching and waiting – watching to see how the September review turns out; watching to see what the EU courts do; watching to see how actively the FTC will enforce Privacy Shield; and watching to see what the Trump Administration will do.

Notwithstanding the privacy sector's caution, US Secretary of Commerce *Wilbur Ross* has emphasized US support for Privacy Shield by urging the Congress, the Administration and the business community to, "work hard to support Privacy Shield".

EUROPE REMAINS SCEPTICAL

In the US, Privacy Shield is well liked – albeit not yet well understood by the Administration or by Congress. But, the story's different in Europe. The Article 29 Working Party, which is participating in the September review, has expressed their concerns on several occasions. The EU Civil Liberties Committee has also been critical. And, EU Data Protection Supervisor *Giovanni Buttarelli* said in August 2017 that Privacy Shield is "an interim instrument for the short term; something more robust needs to be conceived".

The crux of the EU concern is twofold: (1) the failure of the US to meet all of its Privacy Shield commitments; and (2) whether Privacy Shield will do enough to safeguard Europeans from US intelligence agencies' bulk collection.

So, why haven't more companies signed up?
Mostly, it seems that US companies are
watching and waiting.

Shield is intended to facilitate, on a privacy compliant basis, the transfer of personally identifiable information from EU Member States to the US. As such, Privacy Shield incorporates the same key seven "fair information

October 25, 1998 that Safe Harbor was in place. Who are these organizations? They are mostly small businesses and tech and consulting companies, with 70 percent having fewer than 500 employees. Only 15 percent have

A number of lawsuits are already pending, including by the Irish Digital Rights Coalition in the EU's General Court (the same court which struck down Safe Harbor in the *Schrems* decision) and a similar French suit. Most recently, Privacy Shield supporters on both sides of the Atlantic were alarmed by a decision by an EU court that the EU-Canada airline passenger name record transfer agreement failed to meet adequacy concerns.

On the other hand, it is expected that the EU will be encouraged by FTC Consent Orders in September against three companies.¹ The FTC charged that these companies violated US law by falsely claiming that they are Privacy Shield certified. Decusoft, a human resources software company, Tru Communication, a printing company, and Md7, a manager of real estate leases, all entered into consent orders after the FTC charged that they misled consumers about their participation in Privacy Shield. In fact, all three companies had failed to complete the Privacy Shield certification process after starting that process.

Maureen Ohlhausen, Acting FTC Chairperson, said that, "companies that want to benefit from these agreements [Privacy Shield] must keep their promises or we will hold them accountable". These consent orders, which are not yet finalized pending the FTC analysis of public comments (which closed on 10 October), are the first FTC Privacy Shield enforcement orders. Over the approximately ten-year history of the US-EU Safe Harbor Framework, the FTC brought 39 enforcement actions.

It also should not be overlooked that many EU based companies greatly benefit from Privacy Shield. The US based Future of Privacy Forum (FPF) recently completed a study of 114 European headquartered companies that are active Privacy Shield participants. The FPF study concluded that "although no system is perfect there is substantial value for many stakeholders, including leading European companies, in maintaining Privacy Shield protections for companies and consumers in both the United States and Europe."

THE ONLY VIABLE OPTION

The bottom line is that, if Privacy Shield fails, neither the EU nor the US

have good options to facilitate the transfer of personal information. Binding corporate rules work only for the very largest companies. Standard clauses are under an adequacy attack for the same reasons that Safe Harbor failed. Indeed, an October 3, 2017 decision by the Irish High Court in "Schrems II" referred the standard clause framework to the Court of Justice of the European Union – the same doomed path taken by the Safe Harbor accords. A "naked" consent from the record subject doesn't work very well, either, particularly in the employment context where the EU and, especially, the Article 29 Working Party, question the volitional quality of the consent.

This doesn't mean that Privacy Shield is untouchable. While the Europeans are unlikely to cast Privacy Shield aside, they may seek to strengthen Privacy Shield in the wake of the September review. This is particularly true, given the continuing US failure to appoint a permanent Privacy Shield Ombudsman and a failure to name a permanent FTC chairperson (or fill other FTC commissioner vacancies) or to fund the White House Civil Liberties Oversight Board. Further, everyone is mindful that on 25 May 2018 the GDPR goes into effect. This comprehensive reform of the 1995 EU Data Privacy Directive seems certain to cast some shadow on Privacy Shield.

Finally, the collection of personal information from European citizens by US agencies for law enforcement and intelligence purposes is not going away. Certainly, the Trump Administration continues to make Europeans nervous. In January of this year, for example, the Trump Administration issued an Executive Order, "Border Security and Immigration Enforcement Improvements", which stated, "ensure that agency privacy policies exclude persons who are not US citizens from the protection of the Privacy Act to the extent consistent with applicable law". Edward Snowden promptly tweeted that Section 14 of this Executive Order marks the end of Privacy Shield. More importantly, several members of the EU Parliament reacted with alarm.

But, it turns out that the phrase, "consistent with applicable law", is not meaningless. The Judicial Redress Act

extends Privacy Act remedies to non-US citizens. That Act, being a matter of statute law, cannot be repealed or changed by Trump's Executive Order.

A bigger threat is the pending expiration of Section 702 of the Foreign Intelligence Surveillance Act (FISA). That statute prohibits the bulk collecting of communications engaged in by foreign targets without a warrant. If Congress fails to renew this law, the EU is certain to question the extent to which Privacy Shield will protect EU citizens.

CAUTIOUS OPTIMISM

But, the press release at the close of the Privacy Shield review in September, while not substantive, expressed support on both sides of the Atlantic for Privacy Shield. Bruno Gencarelli, Head of EU Commission's Data Protection Unit, said the September review left both sides with, "cautious optimism".

On the US side there is certainly optimism. Were Privacy Shield to unexpectedly fail, and thereby interrupt EU-US trade, the reaction in the Congress and the White House would undoubtedly be a combination of astonishment and anger.

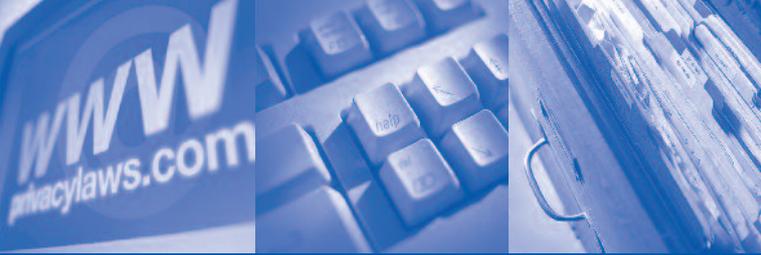
Robert Litt, former General Counsel of the Office of the Director of National Intelligence and no friend of the President, summed it up this way: "While the President's ignorance, incompetence and vanity have no doubt damaged relations with our European allies, it is important to be assured that Privacy Shield will be unaffected."

REFERENCE

1. See www.privacylaws.com/Publications/enews/International-Enews/Dates/2017/9/First-enforcement-actions-against-non-compliant-Privacy-Shield-participants)

AUTHOR

Robert Belair is a Partner at Arnall Golden Gregory in Washington DC, US. Email: Robert.Belair@AGG.com



www.privacylaws.com



ESTABLISHED
1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS

DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

East meets West: Converging regimes, different approaches

Data Protection Authorities discussed legislative frameworks, data transfers and new technologies at their 39th International Conference. **Laura Linkomies** reports from Hong Kong.

The conference was attended by more than 750 representatives from Data Protection Authorities, policymakers, government and business leaders. The DPAs, in their closed session, accepted as new members the Data Protection Authorities of Japan,

Montenegro, South Africa and Turkey, and Belgium's Supervisory Authority for Police Information Management.

The DPAs adopted resolutions on automated vehicles (p.30),

Continued on p.3

Poland takes further steps to adjust to the GDPR

DPA to conduct inspections without prior notification. Specific rules for processing of employee data. By **Joanna Tomaszewska** and **Filip Drgas** of Spaczyński, Szczepaniak & Wspólnicy, Warsaw.

After a few months of silence (following the announcement of the partial draft of the new data protection law in March 2017 – the “March Proposal”), Poland's Ministry of Digital Affairs has finally published the draft of the

new act on data protection and the draft of a separate act seeking to implement the GDPR into Polish law in sectoral provisions (both proposals are referred to as the “Draft”).

Continued on p.5

Issue 149

October 2017

NEWS

- 2 - **Comment**
Can the GDPR create a new global standard?
- 12 - **EU-US Privacy Shield – success so far**
- 27 - **'Speaking the inconvenient truth': UN Special Rapporteur on privacy**
- 29 - **Asian privacy scholars meet**

ANALYSIS

- 18 - **Privacy in eight South Asian States**
- 21 - **European data privacy standards in laws outside Europe**
- 25 - **Industrial Internet of Things: Data privacy and intellectual property**

LEGISLATION

- 10 - **Austria amends DP law to comply with GDPR provisions**
- 16 - **Iceland shows how an EEA country steers parallel to the EU**
- 23 - **South Korea faces GDPR hurdles**

MANAGEMENT

- 7 - **Belgian DPA publishes guidance on DPOs and internal records**
- 14 - **Think tank says DPAs should fine only seriously negligent conduct**

NEWS IN BRIEF

- 9 - **CNIL publishes processor guidance**
- 9 - **EU DPAs issue GDPR guidance**
- 11 - **Human Rights court rules to limit monitoring of employee emails**
- 11 - **Luxembourg issues GDPR Bill**
- 17 - **UK ICO welcomes draft DP Bill**
- 26 - **Hungary moves on with the GDPR**
- 28 - **Uber settles with US FTC**
- 30 - **Guidance on driverless vehicles**
- 31 - **EU to tackle data localisation**
- 31 - **Canada's DPA to step up enforcement**
- 31 - **Call records ruling in Portugal**

Online search available www.privacylaws.com

Subscribers to paper and electronic editions can access the following:

- Back Issues since 1987
- Special Reports
- Materials from PL&B events
- Videos and audio recordings

See the back page or www.privacylaws.com/subscription_info

To check your type of subscription, contact kan.thomas@privacylaws.com or telephone +44 (0)20 8868 9200.

PL&B Services: Publications • Conferences • Consulting • Recruitment
Training • Compliance Audits • Privacy Officers Networks • Roundtables • Research

INTERNATIONAL
report

ISSUE NO 149

OCTOBER 2017

PUBLISHER**Stewart H Dresner**
stewart.dresner@privacylaws.com**EDITOR****Laura Linkomies**
laura.linkomies@privacylaws.com**DEPUTY EDITOR****Tom Cooper**
tom.cooper@privacylaws.com**ASIA-PACIFIC EDITOR****Professor Graham Greenleaf**
graham@austlii.edu.au**REPORT SUBSCRIPTIONS****K'an Thomas**
kan.thomas@privacylaws.com**CONTRIBUTORS****Robert Belair**
Arnall Golden Gregory LLP, US**Sarah Cadiot**
Wilson Sonsini Goodrich & Rosati, Belgium**Rainer Knyrim**
Knyrim Trieb Attorneys at Law, Austria**Whon-il Park**
Kyung Hee University, South Korea**John Selby**
Macquarie University, Australia**Joanna Tomaszewska and Filip Drgas**
Spaczyński, Szczepaniak & Wspólnicy, Poland**Patricia Gelabert**
PL&B Correspondent**Published by**Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom**Tel: +44 (0)20 8868 9200****Fax: +44 (0)20 8868 5215****Email: info@privacylaws.com****Website: www.privacylaws.com****Subscriptions:** The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.

Design by ProCreative +44 (0)845 3003753

Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2046-844X

Copyright: No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior written permission of the publisher.

© 2017 Privacy Laws & Business

“ comment ”

Can the GDPR create a new global standard?

European privacy principles and the GDPR have a huge impact outside of Europe (p.21). In the US, companies are signing up to the EU-US Privacy Shield to ensure continued data flows, but the arrangement's future is still not certain, although the first year looks promising (p.12). The first annual review started 18 September, and the EU Commission should release its assessment any day now, to be followed by a separate report by the EU Data Protection Authorities (p.9).

At the Data Protection Authorities' 39th International Conference in Hong Kong in September which I attended with *PL&B* publisher Stewart Dresner and Asia-Pacific Editor, Professor Graham Greenleaf, many speakers from Asian countries told the participants how they are preparing for the GDPR. The Hong Kong Privacy Commissioner's Office has developed a Privacy Management Programme to mark a strategic shift from compliance to accountability. This is one of the examples of how the thinking in the East meets West (p.1), even if there is not a common regulatory framework.

South Korea has applied for an EU adequacy decision but our correspondent says that it may have to be satisfied with a partial adequacy assessment in the area of information and communications networks (p.23). Read an overview of privacy developments in South Asian countries on p.18, and a short summary of the Asian Privacy Scholars Network conference which discussed a wide range of topical privacy issues (p.29).

Country-specific reports in this issue discuss GDPR implementation in Poland (p.1) and Austria (p.10), and how it also affects data protection in a European Economic Area country, Iceland (p.16). In addition, we report on the Belgian DPA's recommendation on the role of Data Protection Officers (p.7). Progress is being made with GDPR implementation in Spain and Ireland, and we will report on them in a future issue. We are also following closely in our UK Report (to be published next month) progress on the UK's draft DP law which will implement both the GDPR and the so-called Police Directive (p.17). If you would like to inform us of GDPR implementation in your country, please contact me.

In this issue, we also report for the first time on the work of the United Nations Special Rapporteur on the Right to Privacy (p.27), and data privacy and intellectual property challenges with the Industrial Internet of Things (p.25).

Laura Linkomies, Editor

PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 100+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality

Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access

We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

3. E-Mail Updates

E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues

Access all the *PL&B International Report* back issues since 1987.

5. Special Reports

Access *PL&B* special reports on Data Privacy Laws in 100+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation

Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service

Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

“*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Global Data Protection Officer, Dentsu Aegis Network**”

Subscription Fees

Single User Access

International Edition £550 + VAT*

UK Edition £440 + VAT*

UK & *International* Combined Edition £880 + VAT*

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-10 users. Enterprise licence for 11+ users.

Subscription Discounts

Introductory 50% discount. Use code HPSUB (first year only) for DPAs, public sector, charities, academic institutions and small and medium companies.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):

Individual *International* or UK Edition

Rest of Europe = £22, Outside Europe = £30

Combined *International* and UK Editions

Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.

www.privacylaws.com/UK