EU-US Privacy Shield Update
April 21, 2016

Boris Segalis, Partner, New York
Marcus Evans, Partner, London
Jay Modrall, Partner, Brussels
Data Protection, Privacy & Cybersecurity Practice

• Global Reach
  – US, Europe, Canada, SE Asia, China, Latin America, Australia, Middle East, Africa, Russia

• Across Industries
  – Energy, Utility, Pharma, Consumer Products, Financial, Technology, New Media

dataprotectionreport.com
Agenda

• Status of Privacy Shield review and next steps
• Privacy Shield overview
• WP29 key concerns & possible resolutions
• Path forward, Privacy Shield, Model Clauses, BCRs
Status of Privacy Shield review and next steps
<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2016</td>
<td>Commission aims to adopt Privacy Shield</td>
</tr>
<tr>
<td>May 19, 2016</td>
<td>Art 31 Committee meeting to approve Privacy Shield</td>
</tr>
<tr>
<td>Apr 13, 2016</td>
<td>WP29 Privacy Shield review results</td>
</tr>
<tr>
<td>Feb 29, 2016</td>
<td>EU Commission publishes Privacy Shield documents</td>
</tr>
<tr>
<td>Feb 2, 2016</td>
<td>EU Commission and US agree on Privacy Shield</td>
</tr>
<tr>
<td>Oct 16, 2015</td>
<td>WP29 advocates Safe Harbor 2.0, enforcement “moratorium” through Jan 2016, allows Model Clause and BCR data transfers to continue</td>
</tr>
<tr>
<td>Oct 16, 2015</td>
<td>CJEU invalidates Safe Harbor in Schrems</td>
</tr>
<tr>
<td>Nov 27, 2013</td>
<td>EU Commission sets out 13 recommendations for Safe Harbor</td>
</tr>
<tr>
<td>June 2013</td>
<td>Edward Snowden discloses information about US surveillance</td>
</tr>
</tbody>
</table>
Privacy Shield review and adoption process

- **Schrems requirements**
  - Essential equivalence
  - Ability of DPAs to question Commission determinations of adequacy

- **WP29 opinion**
  - Not binding, but important in view of *Schrems*

- **Article 31 committee – next stage**
  - Reviews draft Commission decisions, may be influenced by WP29 views
  - Comprised of MS representatives not affiliated with DPAs or WP29
  - EU Commission can adopt decision in accordance with Article 31 committee opinion with immediate effect
  - EU Commission can adopt decision not in accordance with Article 31 committee opinion after giving Council 3 months to take different action
  - Committee opinion on draft Privacy Shield expected by May 19, 2016
Privacy Shield requirements
Privacy Shield Requirements

- DOC, FTC, DPAs commit to robust, proactive oversight, limiting path to check the box certification, may signal new era of scrutiny of certified companies
- Compliance may be limited for national security, public interest or law enforcement requirements, conflicting legal requirements or explicit limited/tailored authorizations, member state law exceptions or derogations
- Borrows EU definitions for PD, Sensitive PD, Processing, Controller
- De-listed companies must address cross-border compliance or can’t hold on to the data
- Companies should think about Privacy Shield as PbD element
Privacy Shield Principles

• Principles
  • Notice
  • Choice
  • Accountability for Onward Transfer
  • Security
  • Data Integrity and Purpose Limitation
  • Access
  • Recourse, Enforcement & Liability

• “FAQs”
Privacy Shield Requirements - Regulators

- **FTC and DOT** enforce the public commitment to comply with Privacy Shield Principles
- **DOC – robust oversight, scrutiny mean more emphasis on quality of certification**
  - Verify certification submissions – all requirements/checklist
  - Maintain SH list current + list of companies no longer certified
  - Inform de-listed companies they can’t retain data, follow up by questionnaire
  - Actively review privacy policies of de-listed companies to identify relevant misrepresentations, false claims
  - After warning, refer non-compliance to FTC/DOC
  - Promptly review and assess complaints
  - Actively enforce program, including by direct, substantive inquiries in the event of complaint, failure to respond to DOC inquiries, or other evidence of non-compliance with Privacy Shield
  - Better website, including Privacy Shield guide for EU audience
  - Increased DPA collaboration, including by establishing a dedicated contact
  - Facilitate resolution of complaints, 90 day deadline to respond to DPA
  - Establish arbitration procedures (Annex 2) and fund financed by certified businesses
  - Annual interagency compliance meetings
Privacy Shield Requirements - Regulators

- **DPAs** will create a panel for resolving complaints, to ensure harmonized approach to enforcement

- Independent recourse mechanisms must provide Privacy Shield-related information on claim resolution & publish annual report on aggregate stats
Privacy Shield Requirements - Regulators

• **FTC**
  - Commits to making Section 5 review of referrals from arbitrators, DOC or DPAs a priority
  - Standardizes referral process
  - Will take action against false claims of participation
  - Participates in periodic meetings and annual reviews

• **DOT** commits to enforcement

• **State** establishes an Ombudsperson position for EU authorities to submit requests on behalf of EU individuals regarding US intelligence practices
  - Commitment to facilitate, communicate, but remedies are within confines of existing legal processes
Privacy Shield Requirements - Regulators

- **Office of Director of National Intelligence**
  - Explains US signals intelligence;
  - Bulk collection permitted for detecting and countering certain activities of foreign powers, counterterrorism, counter-proliferation, cybersecurity, detecting and countering threats to armed forces, and combatting criminal threat, including sanction evasion
  - 2015 Freedom Act limited bulk collection under FISA and NSLs, requiring specific selection terms that identify a person, account, address or device to be targeted
  - Describes transparency – corporate reports, congressional reports, FISA decisions
  - Judicial redress – FISA, CFAA, ECPA, RFPA, FOIA
Privacy Shield Requirements - Regulators

- DOJ
  - Overview of tools DOJ uses to obtain commercial data from corporations in the US for criminal law enforcement or civil or regulatory public interest purposes
WP29 opinion – key concerns & possible resolutions
WP29 key concerns & possible resolutions

- WP29 sets out roadmap for future challenges to Privacy Shield
- 4 European Essential Guarantees (WP237)
- Three points of concern
  - No obligation to delete data if no longer necessary
  - Massive & indiscriminate data collection still possible
  - Ombudsperson must be independent and able to offer an effective remedy for non-compliant processing
- Recommended “clarifications”
  - Opt-out if to be used for “materially different purpose” is too broad
  - Onward transfers – not to third country unless meets European Essential Guarantees
  - Rights of access, correction and erasure too narrow/ rights not apply to publicly available information
  - Redress too complex & does not allow exercise in EU
  - Must be updated to meet GDPR requirements when applicable
  - Key-coded data must be transferred under another mechanism
  - No 9 month compliance holiday for companies that certify in first 2 months
Data transfer suspension under Shield, MCs & BCRs

Privacy Shield

- Once Commission adopts Privacy Shield decision, DPAs must allow transfers unless and until European Court of Justice invalidates it

- If Privacy Shield is adopted, WP 29 “essential guarantees” concerns could lead to suspensions under EU MCs and BCRs before Shield challenge is heard

- Same “essential guarantees” concerns could apply to transfers to other non-EEA countries with inadequate surveillance protections under EU MCs or BCRs

EU Model Clauses

- Commission Decision approving EU MCs allows DPAs to suspend transfers under them if “it is established” that surveillance does not meet EU standards in non-EEA importing country

Binding Corporate Rules

- Binding Corporate Rules are based on approvals from DPAs, not on a Commission Decision, and DPAs can withdraw approval unilaterally
Resolving WP29 concerns

Commission will not be able to resolve all the WP 29 concerns

- Even if asked, US unlikely to agree substantial revisions, especially further surveillance restrictions
- Some flexibility may be available on the Ombudsperson
- EU law on surveillance may evolve based on ongoing CJEU cases (*Tele2*, *Davis*), but unlikely to render US surveillance acceptable by loosening EU protections

Article 31 committee may diverge from WP 29

- But Commission could extend deadline to allow time for acceptable changes

If Article 31 committee does not support the decision

- Commission can still adopt in August if Council allows
  - *Schrems* II process would likely begin soon after
  - Meanwhile, DPAs likely to challenge EU MCs and BCRs on *Schrems* principles
- If Commission abandons Privacy Shield, challenges will focus exclusively on EU MCs and BCRs
Worst case scenarios – Privacy Shield, MC, BCRs

Commission adopts Shield
- Schrems II type complaint on commercial/essential guarantees grounds against Shield and CJEU rules on legality
- DPA suspends data flows on essential guarantees grounds under EU MC/ BCR and/or applies further restrictions to such transfers
- Uncertainty remains
- More data localisation

Commission does not adopt
- DPA suspends data flows on essential guarantees grounds under EU MC/ BCR and/or applies further restrictions to such transfers
- Uncertainty remains
- More data localisation
Path forward – Privacy Shield, Model Clauses, BCRs
Privacy Shield

• Privacy Shield certification is marginal effort for SH-certified companies
• Initial certification may require significant effort
• Weakness in Privacy Shield less of a factor for intracompny transfers and B2C business
• In B2B transfers, business customers in Europe may resist the Privacy Shield, requiring a hybrid approach, but Privacy Shield may work in many cases
• DPAs likely to be vocal about dislike to Privacy Shield, based on SH experience, but business customers are pragmatic
• If Privacy Shield is not adopted or fails….
Model Clauses & BCRs

• The moratorium on having no solution is over
  • No calming language in WP statements
  • EU controllers who were using Safe Harbor are receiving letters from DPAs to respond with an alternative mechanism within deadlines
  • Hamburg data protection authorities enforcement action against 3 companies in March

• Model clauses and BCRs remain valid, susceptible to challenge
Model Clauses

• Evidence of growing acceptance

• Challenges
  • Prior approval in a number of EU jurisdictions (requires registration of domestic processing first) but GDPR will abolish
  • B2B US processors accept model clauses, but not exposed to registration and approval risks themselves (but their customers are)
  • Business risk if vendors do not accept flow downs
  • Limitation of liability provisions can mitigate risk
BCRs

- Tailor made group export programme that meets EU requirements (and is DPA pre-approved)

- Challenges
  - Only cover transfers intragroup and to 3rd Parties with Processor BCRs
  - Susceptible to same suspension challenges as EU MC
  - German DPAs suspended new approvals to US on 26.10.16 so not currently an option for German exports (EU MCs will have to be used)
Recap

• Commission not obliged to address WP29 concerns, may proceed with Art 31 approval process
• Incentivised to do so to minimise grounds of challenge
• Not addressing “essential guarantee” concerns could impact transfers under EU MCs and BCRs too
• Possibility of “essential guarantee” challenges for other countries too – uncertainty unlikely to clear up quickly
• Risky to have no export solution at this point – EU Model Clause adoption likely to increase despite risk of suspension of flows
• If adopted, the Privacy Shield will remain the easiest export route for EU exporters to execute
• Weak Privacy Shield may be the right option, but hybrid approach to transfers may be required
Speaker

Marcus Evans
Partner, London

Marcus leads Norton Rose Fulbright’s Data Protection, Privacy and Cybersecurity practice group in Europe.

Marcus advises on the full range of information law issues from compliance audit programs through to cyber breach and regulatory response most often with a multijurisdictional element. He also advises on regulatory and contractual issues in the provision and procurement of IT and e-commerce services.

He works across all sectors but has particular expertise in financial services.

Marcus is ranked for his privacy work in the Legal 500 and recognised as a notable data privacy practitioner in Chambers & Partners 2014. He "brings an investigative and thorough approach to data protection mandates. Sources say: "He was very good at getting to the bottom of stuff and asking the right questions. That made a huge difference to us." He has been described as "very professional, very efficient and extremely knowledgeable in data protection". 
Boris Segalis is a US co-chair of Norton Rose Fulbright's Data Protection, Privacy and Cybersecurity practice group.

Boris counsels clients regarding a broad range of privacy, information security, cybersecurity and information management issues. The practice addresses all aspects of information management lifecycle, including its collection, use, storage, disclosure and destruction, as well as the protection of the information and the infrastructure supporting the data.

Boris advises clients on information law issues that arise in the context of data-based products and services, big data programs, smart grid operations, marketing and advertising, corporate transactions (including M&A and bankruptcy), state and federal investigations and regulatory actions, cross-border data transfer, vendor management, cloud computing, technology transactions, incident and breach response and pre-response planning. Boris represents clients in a variety of industries, ranging from start-ups to Fortune 100 companies. His clients include companies in the consumer products and services areas, online retailers and media companies, pharmaceutical companies, utilities, travel-related businesses, B2B technology providers, payment processing businesses, and non-profit organizations.

Boris is a member of Crain’s Business 40 under 40 class of 2015. He has been recognized by Chambers as an up and coming attorney in Privacy & Data Security. Boris is a Certified Information Privacy Professional (CIPP/US) through the IAPP, and serves on the IAPP’s Research Board.
Jay Modrall is a partner in Norton Rose Fulbright's Antitrust and Competition practice group based in the Brussels office. Jay counsels clients regarding a broad range of EU law issues, including not only antitrust and competition law issues but also EU aspects of privacy and data protection law.

Jay’s data protection work has included advising a wide range of clients on European data protection requirements, from the origins in the Council of Europe Convention in the 1980s to the fallout of the Court of Justice’s Schrems decision today. As one of the few Brussels-based EU lawyers with extensive experience in the financial services sector, Mr. Modrall played a key role in the drafting and early implementation of many of the key EU directives and regulations including AIFMD, Banking Union, CRD IV/CRR, Credit Agency Regulation, EMIR and MiFID, gaining extensive hands-on experience with the EU legislative process. Mr. Modrall has written extensively and is a frequent speaker at conferences on a wide range of EU financial services regulatory and Eurozone topics.

A U.S.-qualified lawyer by background, Jay is a member of the Bar in New York, Washington, D.C. and Brussels, Belgium. He joined Norton Rose Fulbright LLP in September 2013 as partner, having been a resident partner in a major US law firm since 1995. Jay’s native language is English. He is fluent in Italian, having lived and worked for several years in Italy, and proficient in Dutch and French.
Disclaimer

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients.

References to ‘Norton Rose Fulbright’, ‘the law firm’ and ‘legal practice’ are to one or more of the Norton Rose Fulbright members or to one of their respective affiliates (together ‘Norton Rose Fulbright entity/entities’). No individual who is a member, partner, shareholder, director, employee or consultant of, in or to any Norton Rose Fulbright entity (whether or not such individual is described as a ‘partner’) accepts or assumes responsibility, or has any liability, to any person in respect of this communication. Any reference to a partner or director is to a member, employee or consultant with equivalent standing and qualifications of the relevant Norton Rose Fulbright entity.

The purpose of this communication is to provide general information of a legal nature. It does not contain a full analysis of the law nor does it constitute an opinion of any Norton Rose Fulbright entity on the points of law discussed. You must take specific legal advice on any particular matter which concerns you. If you require any advice or further information, please speak to your usual contact at Norton Rose Fulbright.