The European Court of Justice Invalidated EU/US Safe Harbor: What Does the Future Hold?

November 20, 2015

Presented by:

Mary J. Hildebrand, CIPP/US/EU
Partner, Chair, Privacy and Information Security Practice
Lowenstein Sandler LLP

Mark Faber
Vice President, Senior Regulatory Counsel - Privacy
Prudential Financial
Overview

- US and the EU: Different Philosophies Regarding Privacy and Data Protection
- EU/US Data Transfer: Pre-Schrems
- Schrems Decision
- The Impact of Schrems: Recent Developments
- Business Challenge: Alternatives to Safe Harbor
- What Does the Future Hold?
- Recommendations
US and the EU: Different Philosophies Regarding Privacy and Data Protection
“What worries me. . . is that [Americans are] patting [themselves] on the back every morning and thanking God for the Atlantic Ocean ... Things move with such terrific speed these days, that it is really essential to us to think in broader terms and, ... the American people ... should think of possible ultimate results in Europe[.]

Franklin D. Roosevelt,
December 14, 1939 letter to William Allen White
US and EU: Different Philosophies

- United States
  - Sectoral Model
  - Federal/State
  - “Privacy” does not appear in the US Constitution

- European Union
  - Comprehensive Model
  - Privacy is a fundamental human right (EU Charter of Fundamental Rights)
EU Privacy Directive (95/46/EC)
- Adopted by the European Commission (EC) in 1995, effective in 1998
- Aimed at public and private sector
- Governs the collection, processing, and disclosure of personal data on individuals including citizens, employees, and consumers
- Each member state of the EU permitted to implement the Directive differently

Currently, there is little uniformity of structure, laws, or regulations across the EU
EU/US Data Transfer: Pre-Schrems
Under the Directive, very few countries are deemed to provide an “adequate” level of protection for the personal data of EU citizens

The US is not on the list of approved countries

In 2000, the EC and the US Dept. of Commerce completed negotiation of the EU/US Safe Harbor framework to permit the transfer of personal data from the EU to the US

Safe Harbor:
- Is available to companies subject to jurisdiction by the FTC or the Department of Transportation
- Not readily available to insurers or financial services firms
EU/US Data Transfer: Pre-Schrems

- Eligible US companies must “self certify” annually to the US Department of Commerce that they comply with the seven Safe Harbor principles
- The FTC is responsible for enforcing Safe Harbor
- Safe Harbor was approved by the EC and is binding on each of the EU member states
- By 2015, 5,000 US companies relied on Safe Harbor
The *Schrems* decision was announced in the midst of other significant developments.

In 2012, the EC introduced the General Data Protection Regulation (GDPR) to replace the Directive.

- GDPR is intended to standardize data protection laws across the EU.
- Currently preserves existing methods of transferring personal data from EU to US.
- GDPR is currently in final stages of negotiation, and will become effective 24 months after final approval.

In 2013, Edward Snowden made massive disclosures regarding NSA surveillance programs.
In 2013, the EU recommended 13 modifications to Safe Harbor, and commenced negotiations with the US.

In September 2015, the US and the EC finalized negotiation of the “Umbrella Agreement”

- Provides a framework governing transfer and protection of personal data for law enforcement purposes.
- Becomes effective when Congress adopts a law granting EU citizens the right to seek legal redress in the US for misuse of personal data.
Schrems Decision
Maximilian Schrems asked the Irish Data Protection Authority (DPA) to prohibit Facebook from transferring his personal data to the US because it was subject to NSA surveillance.

Irish DPA refused to investigate because the EC determined in 2000 that Safe Harbor provided an adequate level of protection for data transferred to the US.

The High Court of Ireland requested guidance from the European Court of Justice (ECJ):
- Does the EC’s decision on Safe Harbor in 2000 prevent a DPA from investigating a complaint alleging that a third country (i.e., the US) does not ensure an adequate level of protection and, where appropriate, suspending the contested transfer of data?
Each EU Member State DPA may examine whether the transfer of personal data complies with the requirements of the Directive and may suspend transfers to countries outside EU if it finds data protection laws inadequate.

Safe Harbor does not:
- Adequately protect personal data from interference from US government on national security or public interest grounds
- Safe Harbor does not provide EU citizens with protection or the ability to obtain redress in the US

The Safe Harbor framework fails to comply with the requirement to protect personal data to the standards required by the Directive and is, therefore, invalid.
The Impact of Schrems: Recent Developments
Impact of Schrems

- Safe Harbor was deemed inadequate and invalid as a means to transfer data from the EU to the US
- Immediate panic and uncertainty for US companies and EU entities relying on Safe Harbor
- The decision created additional uncertainty because its reasoning could be applied to other data transfer methods such as model contracts and binding corporate rules
- Opened the door for EU DPAs to evaluate adequacy of other transfer methods and transfers to other countries deemed inadequate by EC
Impact of *Schrems*: Recent Developments

- Early October – the European Commission issued a communication
- The EC emphasized:
  - Safe Harbor can no longer serve as a legal basis for transfers of personal data to the US
  - Model Contracts and BCRs are still valid
  - A new Safe Harbor framework was essential and needed to be renegotiated with the US in light of *Schrems*
  - There would be no enforcement by DPAs against data transfers that are not in compliance until late January 2016
Impact of *Schrems*: Recent Developments

- October 19 – The Israeli Law, Information and Technology Authority (ILITA):
  - Revoked its authorization regarding transfers of personal data from Israel to the US based on the Safe Harbor
  - Required that transfers of personal data from Israel to the United States be based on model contract clauses, binding corporate rules, or other valid legal arrangements or derogations under the Directive

- October 21 – the US House passed the Judicial Redress Act giving EU residents the right to bring suit in US courts for privacy violations. The Bill is on its way to the Senate
Impact of *Schrems*: Recent Developments

- October 26 – the German DPAs issue position paper:
  - Questioning the legitimacy of Model Contracts and BCRs as data transfer methods to the US
  - No new permissions will be issued for data transfers to the US based on Model Contracts or BCRs

- October 27 – the UK ICO releases statement acknowledging uncertainty created by *Schrems*, but takes a more liberal view
Impact of Schrems: Recent Developments

- October 28 – the EC announces that an agreement in principle was reached with the US on a new Safe Harbor framework – Safe Harbor 2.0
- Details to be determined and further negotiated in the coming weeks with a goal for completion before the end of January 2016
- Emphasized need for strong oversight of new program
- US government surveillance/national security issues are still the biggest obstacle to overcome
Impact of Schrems: Recent Developments

November 6 – the EC issued a guidance emphasizing:

- Data transfers to the US through Safe Harbor are unlawful as of October 6, 2015
- There would be no enforcement actions against companies failing to implement alternative data transfer mechanisms until January 2016
- Reaffirmed that model contracts and BCRs are still effective, but stated that the EC will analyze the impact of Schrems on the validity of these transfer methods
- EC will continue with and finalize negotiations for Safe Harbor 2.0, provided it provides a “renewed and sound framework for transatlantic transfers of personal data, which must meet the requirements identified in the Court ruling, notably as regards limitations and safeguards on access to personal data by US public authorities”
- Any adequacy decision by a DPA must be based on a broad analysis
- No mention of EU surveillance laws
Business Challenge: Alternatives to Safe Harbor
Business Challenge: Alternatives to Safe Harbor

- As part of the Guidance issued on November 6, 2015, the EC set forth alternative bases for transfers of personal data to the US
- EC commented that discussion regarding alternatives is “without prejudice to the independence and powers of the DPAs to examine the lawfulness of such transfers”
  - Model Contract Clauses
  - Binding Corporate Rules
  - Derogations
Model Contracts

Model Contracts:
Standard language contract clauses, which can be inserted into contracts with data controllers/processers to meet EC adequacy requirements

Appropriate for:
- Management of HR data.
- Alternative to time, cost, and effort needed for BCR implementation
- Interim solution preceding BCR implementation
- Organizations needing one-off data transfers

Advantages
- Speed
- Readily available and Pre-Approved
- Straightforward

Disadvantages
- Cannot be amended
- Cumbersome for complex transfers with multiple parties
- May require regulatory approval in some countries
## Binding Corporate Rules

**BCRs:**
Legally binding internal corporate privacy rules for transferring personal information within a corporation or corporate group.

**Appropriate For:**
- Intra-group data transfers
- Large companies with time, money and resources
- Companies making many data transfers from the EU

### Advantages
- Less burden once implemented
- Preferred method of Transfer by EU Regulators
- Provides for comprehensive level of privacy and data protection
- Avoids the need for separate contracts for each limited data transfer

### Disadvantages
- Time – process takes 12-18 months
- Requires resources and expenses to prepare
- Requires regulatory approval
Derogations:
Explicitly identified in the Directive, including:

- Unambiguous consent
- When transfer is necessary or legally required for:
  - the performance of a contract
  - on important public-interest grounds or for the establishment, exercise or defense of legal claims
  - to protect the vital interests of the data subject.

Suited for:

- Limited use
- When “necessary” and there are no other options available
- B2C websites targeting discrete transactions by EU consumers

Advantages

- Provided for in the Directive
- Extremely beneficial if they apply

Disadvantages

- Unambiguous consent must be freely given, specific, and informed
- The contractual derogations are narrowly construed, and subject to a strict “necessity test”
- Use of the data limited to the stated purpose
- Not suited for wholesale transfers of data
What Does the Future Hold?
What Does the Future Hold?

- Post-Schrems, DPAs are empowered to conduct independent investigations of data transfers to any country deemed not to provide “adequate” security under the Directive.

- Alternatives to Safe Harbor are subject to challenge by DPAs on a case-by-case basis.

- DPAs may elect to exercise audit rights under existing Model Contracts, Binding Corporate Rules or other derogations (e.g., Germany).

- Each DPA may select a different approach.
What Does the Future Hold?

- Legitimate and pressing concern on timing
- The European Commission and the Article 29 Working Party identified January 31, 2016 as a critical date for decisions regarding enforcement actions
- Can – or should – business rely on the promise of a “buffer” period?
- In the midst of all the uncertainty and speculation, data continues to flow from the EU to the US, and there are strong economic incentives to continue
- Concern that abrupt moves by the DPAs would have severe economic consequences
Safe Harbor 2.0 may not be negotiated or agreement is reached, it could face the same fate as the original Safe Harbor.

The European Commissioner for Justice, Consumers and Gender Equality, Vera Jourova, told MEPs in Brussels:

- "There is agreement on these matters in principle, but we are still discussing how to ensure that these commitments are binding enough to fully meet the requirements of the [CJEU ruling]."

Based on Schrems, this would appear to require US authorities to give assurances that the data of EU citizens held in the US will not be subject to surveillance by government agencies.
What Does the Future Hold?

- The GDPR is likely on the horizon
- There is a legitimate and sincere desire on the part of EU and US to find a solution
- Practicality/economic reality prevails over ideology
- Trillions at stake
- Security vs Privacy debate in light of recent tragic events in Paris, Beirut, and Egypt: Wild Cards
Recommendations
While there is no guarantee that DPAs will refrain from enforcement actions until the end of January, 2016, thus far post-*Schrems* activity has been limited.

Businesses should use this window productively:

- Conduct an assessment of your EU/US data transfer practices and data flows
- Evaluate EU-approved alternatives to Safe Harbor in the context of your business
- Develop a realistic plan to implement an appropriate alternative to Safe Harbor
- Assess your vendor contracts
- Be prepared to implement your plan without undue delay

Monitor judicial, legislative, and diplomatic initiatives closely, and keep an eye on current events.