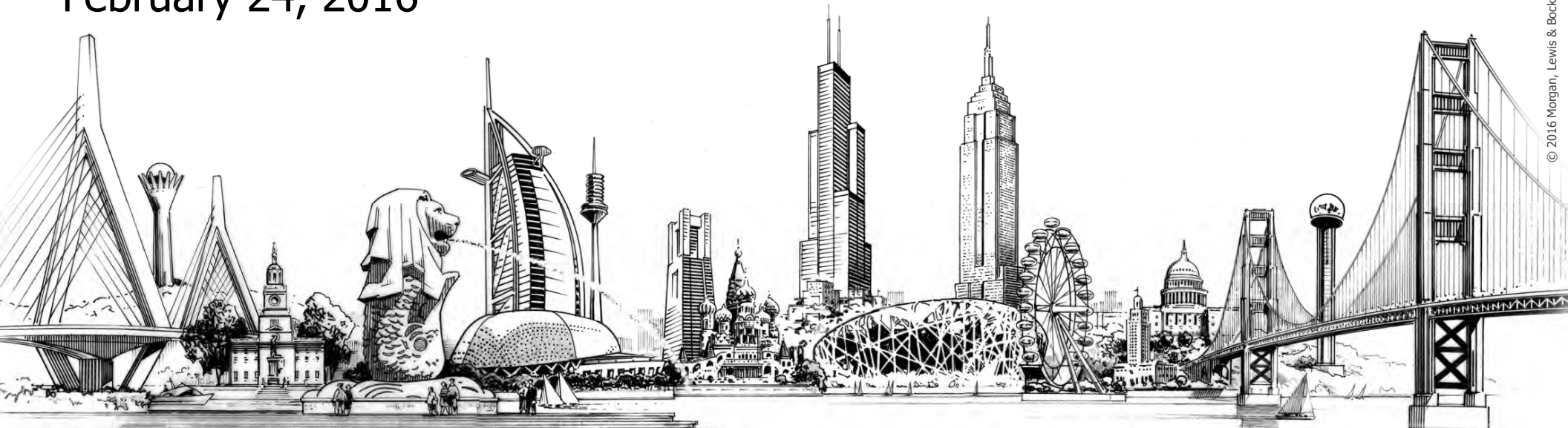


Morgan Lewis

THE EU-US PRIVACY SHIELD

Pulina Whitaker, Mark Krotoski, and Gregory Parks
February 24, 2016



Welcome and Introductions



Pulina Whitaker
London
+44.20.3201.550
pwhitaker@morganlewis.com



Mark L. Krotoski
Silicon Valley
+1.650.843.7212
mkrotoski@morganlewis.com



Gregory T Parks
Philadelphia
+1.215.963.5170
gparks@morganlewis.com

Overview of Safe Harbor and Privacy Shield

1. EU/US Privacy Framework Agreement in 2000
2. Over 4,000 US organizations certified by 2015
3. EU Court of Justice issued a ruling in *Schrems* which ruled that the EU-US Safe Harbor program was invalid on October 6th, 2015
4. New EU-US Privacy Shield to replace Safe Harbor announced on February 2, 2016
5. Judicial Redress Act of 2015 – enables EU citizens to enforce privacy rights in US courts
6. Awaiting Article 29 WP guidance on EU-US Privacy Shield

The *Schrems* Decision

- In October 2015, EU Court of Justice invalidated the EU-US Safe Harbor Agreement
- Key findings of decision:
 - Organizations self-certified under the Safe Harbor program are permitted to “disregard” the Safe Harbor principles to comply with US national security, public interest or law enforcement requirements
 - There is no provision in the Safe Harbor program for protection for EU citizens against US authorities who gain access to their personal data transferred to the US pursuant to the Safe Harbor program. There is only a provision for commercial dispute resolution
 - “The guarantee of independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals”
 - The powers of supervisory authorities include “effective powers of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings”
 - The Safe Harbor program “cannot prevent persons whose personal data has been or could be transferred to a third country from lodging with the national supervisory authorities a claim....concerning the protection of their rights and freedoms”

The *Schrems* Decision (continued)

- Where the national data protection authorities find that complaints regarding the protection of personal data by Safe Harbor-certified companies are well founded, they “must...be able to engage in legal proceedings”
- The EU Data Protection Directive “requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary” but there is no such requirement applicable in the US following the transfer of personal data pursuant to the Safe Harbor program
- The Safe Harbor program “fails to comply with the requirements” to protect personal data to the “adequate” standard required by the EU Data Protection Directive and is, “accordingly invalid”

New EU-US Privacy Shield

- EU Commission announced new “EU-US Privacy Shield” for US organizations, replacing the Safe Harbor program on February 2, 2016:
 - Limitations imposed on US authorities accessing personal data for national security purposes and an oversight mechanism
 - Annual review of these principles
 - EU citizens to have same civil rights of enforcement as US citizens under proposed new Judicial Redress Act
 - EU citizens and EU DPAs can complain to FTC and DoC
 - Needs to be formally adopted by EU Commission (after advice from Article 29 Working Party)

US Perspective on Privacy Shield

- Confusion post-*Schrems* left many companies without options
- There was much hope for a “Safe Harbor 2.0” n/k/a “Privacy Shield”
- Data transfers need to happen
- US Government, regulators and companies support ultimate adoption
 - FTC promising “robust” enforcement and co-operation with EU authorities
 - Commerce Department pushing for necessary legislative changes

What US Companies Must Do to Use Privacy Shield Protections

- Details currently sparse, but will involve more than simple self certification that existed under Safe Harbor.
- More of an approval process that will involve both declaring and demonstrating commitment to the principles of the EU Data Privacy Directive:
 - Notice – information collected and use
 - Choice – must give opt out for third party transfer or alternative use; must have opt-in for sensitive information.
 - Onward Transfer – third party must comply with adequacy standards
 - Access – individuals can learn what information is held, correct or delete
 - Security – “reasonable precautions” to protect from loss or misuse; de-identify data
 - Data Integrity – reliability of data
- Final principle of enforcement will be significantly increased. Must submit to:
 - Jurisdiction by EU data protection authorities
 - Responding to complaints of EU citizens through Privacy Ombudsman
 - Be bound by decisions of EU authorities on data handling
 - Continued FTC enforcement

EU Commission approved “adequate” Countries

- Countries providing "adequate level of protection":
 - EEA countries – EU, Iceland, Liechtenstein, Norway
 - Andorra
 - Argentina
 - Canada
 - The Faroe Islands
 - Guernsey
 - Isle of Man
 - Israel
 - Jersey
 - New Zealand
 - Switzerland
 - Uruguay

Judicial Redress Act of 2015

Key Legislative Objectives

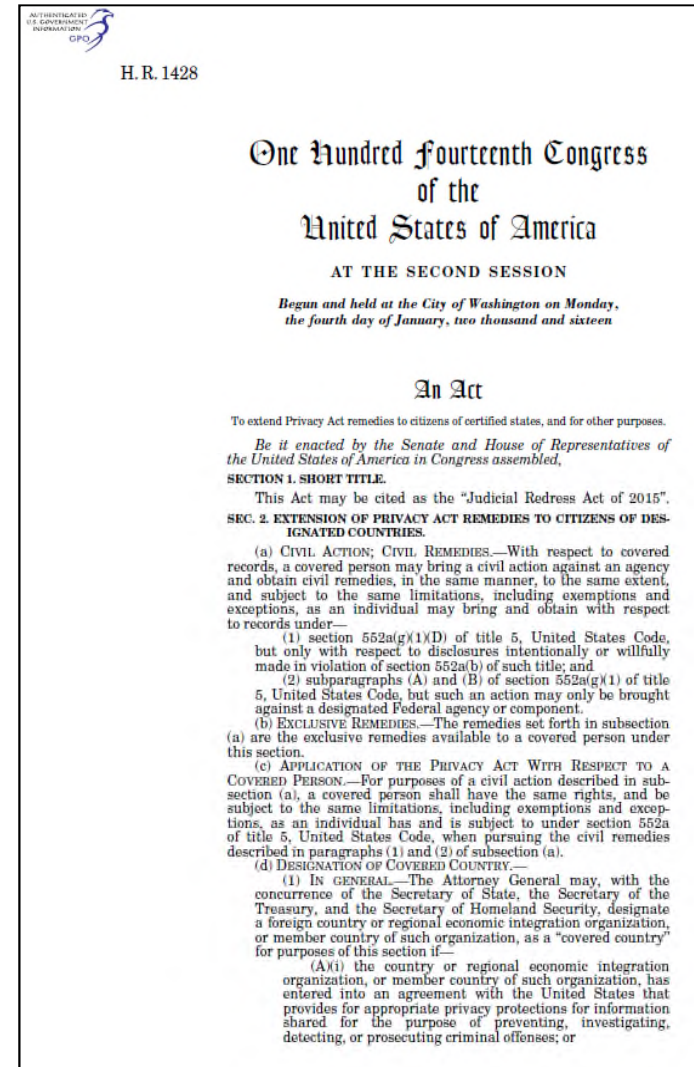
- “According to the Department of Justice, the Judicial Redress Act is critical [1] to reestablishing a trusting relationship between the European Union and the United States, [2] to ensuring continued strong law enforcement cooperation between the United States and Europe, and [3] to preserving the ability of American companies to do business internationally.” [Cong. Goodlatte]
- “Restore public trust in US privacy protections” [Cong. Goodlatte] [Cong. Collins]
- “[R]ebuild strained relationships with our allies and to ensure privacy and security for both American and European Union citizens” [Cong. Sensenbrenner]
- Promote adoption of the Data Privacy and Protection Agreement [Cong. Goodlatte]

Judicial Redress Act of 2015

- Enables EU citizens from designated countries to enforce privacy rights in US courts
 - Extends same rights under the 1974 Privacy Act to citizens from designated countries
 - AG will designate covered foreign countries
 - Applies to information obtained through international law enforcement channels
- Right of civil action in US court
 - Right to sue the United States Government to access, amend, or redress unlawful disclosures of personal information transferred for law enforcement purposes
 - Redress Federal Government failures to grant access to records or to amend incorrect records

Judicial Redress Act of 2015

- Legislative Action
 - March 18, 2015
 - Introduced in the House of Representatives [H.R. 1428]
 - Oct. 20, 2015
 - Passed House of Representatives on voice vote
 - Feb. 9, 2016
 - Passed Senate as amended on voice vote
 - Feb. 10, 2016
 - Amended measure passed House of Representatives on voice vote
 - Feb. 12, 2016:
 - Presented to President



International Data Transfer Options

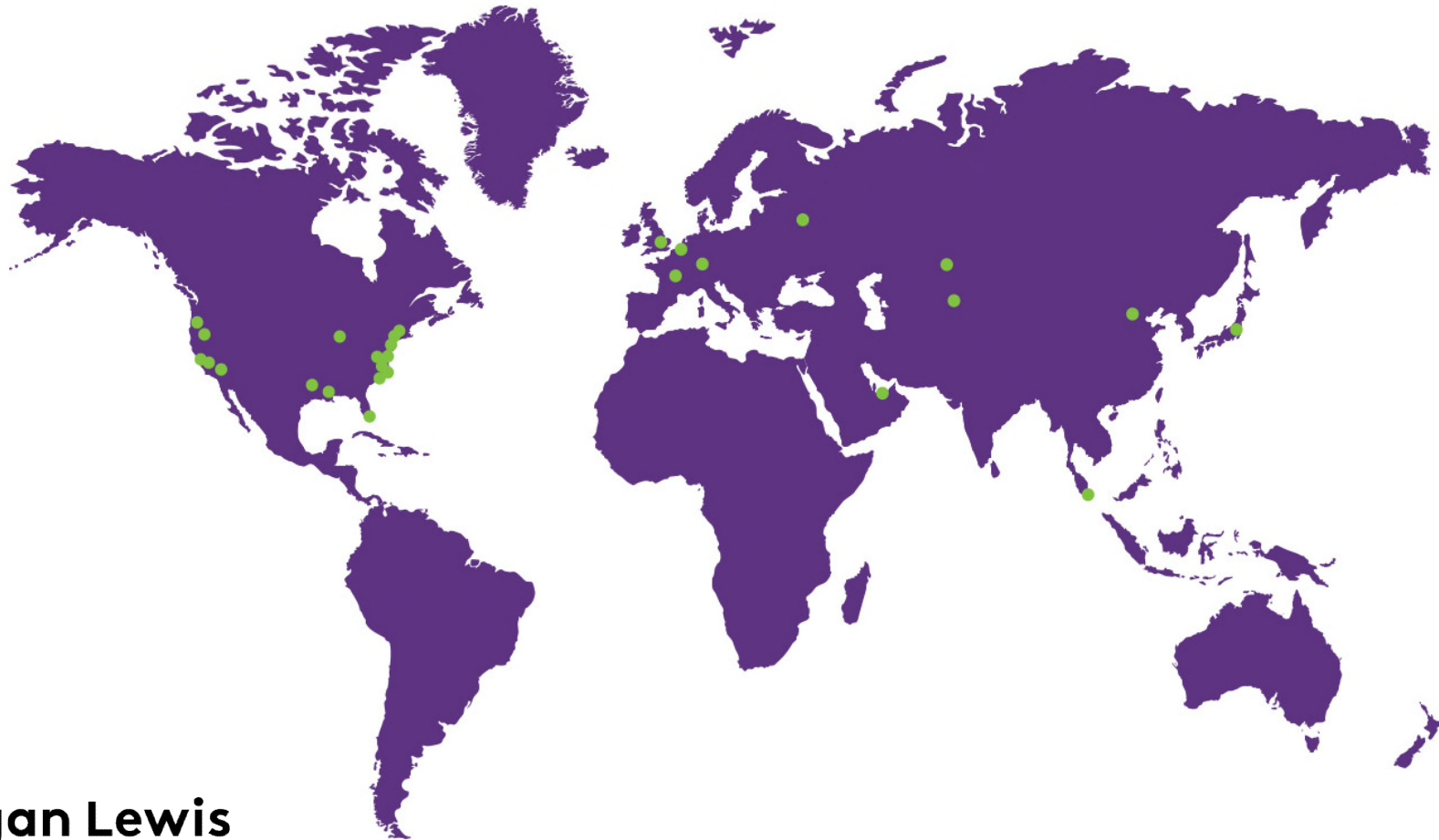
- Although some confusion post-*Schrems*, transfers outside EEA also lawful where:
 - parties have signed model contractual clauses approved by EU Commission
 - approved binding corporate rules
 - data subject expressly consented to transfer – freely given and informed
 - other statutory exceptions include:
 - necessary to perform a contractual obligation to the individual
 - necessary for company's compliance with a legal obligation
 - necessary for company to establish or defend its legal rights or
 - necessary for reasons of substantial public interest

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty	Dallas	Los Angeles	Philadelphia	Singapore
Astana	Dubai	Miami	Pittsburgh	Tokyo
Beijing	Frankfurt	Moscow	Princeton	Washington, DC
Boston	Hartford	New York	San Francisco	Wilmington
Brussels	Houston	Orange County	Santa Monica	
Chicago	London	Paris	Silicon Valley	



Morgan Lewis

THANK YOU

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Attorney Advertising. Links provided from outside sources are subject to expiration or change.

© 2016 Morgan, Lewis & Bockius LLP

Morgan Lewis