# Lost in Privacy? How to tackle transatlantic data protection challenges

Ira Rubinstein
NYU School of Law
February 4, 2017

# Agenda

- European and US Regulatory Paths
- The *Schrems* Decision and the Privacy Shield
- Privacy Bridges

# The EU Path (1)

- Privacy as fundamental right
- Data protection law
  - Adopts precautionary principle
  - Offers comprehensive and uniform solutions
    - Under Directive, harmonization has been ongoing concern
  - Serves twin goals of achieving high level of data protection and free flow of data w/i EU
    - NB: Adequacy requirement and "Brussels effect"
    - Exemption for law enforcement and intelligence activities, which are largely reserved for Member States
      - Surveillance laws vary greatly and some are very problematic

# EU Path (2)

- GDPR
  - Increased harmony and consistency
  - Shift of power to the central government
  - Larger penalties and fines
  - Most notably, a "belt and suspenders" approach to regulating private firms

# EU Path (3)

- Example of belts and suspenders: Big data
  - Core requirements-arts. 5 and 6
  - Transparency-art. 13-15
  - Right to object/not be subject to automated decision-making/profiling-arts. 21-22
  - Data protection by design and default-art. 25
  - Data protection impact assessments-art. 35
  - Prior consultation-art. 36
- Two views of these substantive & procedural requirements
  - They will engender trust and create a level playing field thereby enabling big data services in Europe
  - They will restrict numerous well-established & effective practices and may obstruct new deployments of big data

# The US Path (1)

- Privacy has a constitutional, common law and statutory basis
- The FIPs originated in the US and find expression in mostly sectoral statutes, which reflect a harms-based approach to privacy regulation
- Consumer protection law also plays a key role with the FTC engaging in robust enforcement efforts
- States also play a significant role in developing privacy laws and enforcing consumer protection laws
- Gaps in US law remain but the Obama White House took several steps to close them; early steps by the new Admin. have raised serious concerns

# The US Path (2)

- A complete picture of the US path requires mention of three additional factors:
  - Private lawsuits enforcing federal and state privacy laws
  - "Privacy on the ground" (i.e., CPOs, PETs, industry codes, soft law, strong NGOs, media pressure)
  - Federalism
    - States as first movers and policy labs for privacy law
    - State-federal interaction, especially over sectoral regulation, avoids problems of inflexibility and ossification that plague omnibus laws

# The US Path (3)

- The Snowden revelations
  - Widespread data collection and analysis without adequate accountability and transparency running counter to constitutional and statutory protections against unwarranted surveillance
  - But also vigorous debate in the US about the proper balance between privacy and security.
  - And new studies, proposals, revised policies, new laws
    - PRG and PCLOB
    - PDP 28
    - USA Freedom Act
    - Email Privacy Act?

# Differences: EU vs. US

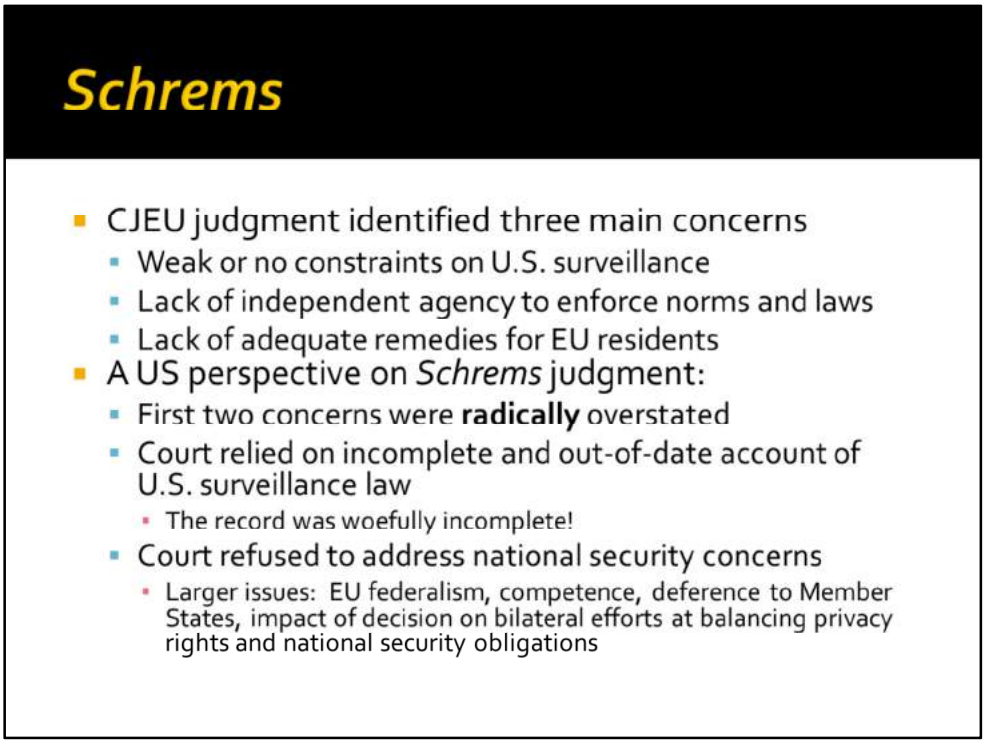
- Legitimate processing
  - No processing without legal basis vs. processing unless legal rules prevent it
- Precautionary principle vs. risk-avoidance
- Right to respect for private and family life vs. no constitutional basis in US for limiting data processing in consumer privacy context
- Different compliance cultures
  - EU: High level of protection but weak enforcement (GDPR may change this in a b$g way)
  - US: Myriad laws with varying levels of protection but aggressive enforcement by FTC and state AGs and emergence of "common law" of consumer privacy
- Different ways of balancing privacy and free expression

# Commonalities

- Democratic governments and close historical and social ties
- A common tradition of upholding human rights
  - Fundamental rights under EU instruments
  - 1st, 4th and 5th amendments to US Const.
  - Surveillance:
    - "Necessary and proportional" vs "reasonable expectation of privacy"
- Significant economic relationships

# Cross-Fertilization

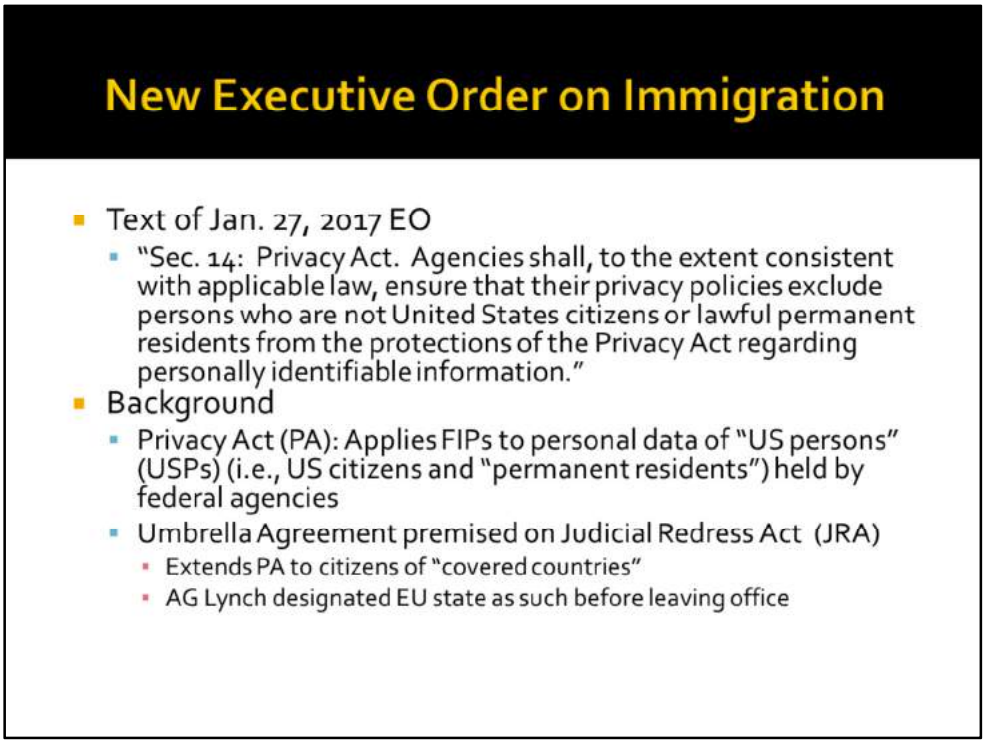
- FIPs (e.g., new emphasis on accountability)
- CPOs
- Breach notification laws
- Joint enforcement efforts
- Policy guidance reaching very similar results despite very different starting points
  - Mobile apps
- Common technological and cross-border challenges
- Recognition of need for common solutions
  - Privacy Shield, Umbrella Agreement, MLATs?



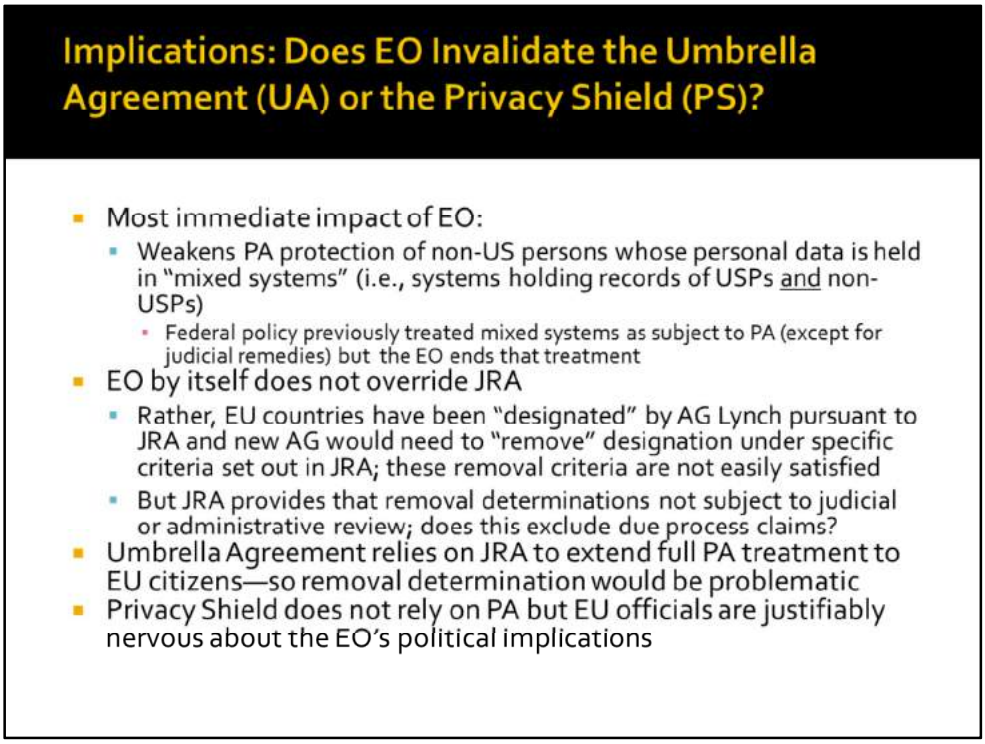

Court misunderstood/disregarded applicable US law (PPD-28, Freedom Act), role of FISC, newly enacted US laws and policies

# Privacy Shield and other transfer mechanisms

- Privacy Shield
  - Responsive findings seek to overcome *Schrems'* objections
    - Calls out new US safeguards
    - Creates new role for ombudsperson
    - Also improves protections as compared with SHA
- Ongoing concerns
  - Are US surveillance programs "mass and indiscriminate"?
  - Is the ombudsperson sufficiently independent?
- Challenges:
  - Two direct challenges to Privacy Shield filed with CJEU
  - BCRs and model clauses also coming under pressure
    - New Schrems filing against Facebook re validity of model clauses and Irish High Court will soon decide on referral to CJEU




Executive Order: Enhancing Public Safety in the Interior of the United States




DHS view on mixed system:
At the time, the Department reasoned that this extension of privacy protections to non-U.S. persons would benefit the United States in two ways. First, it addressed concerns that U.S. partners had raised in negotiations for information sharing agreements, which at that time included a negotiation with the EU over the sharing of Passenger Name Records. Second, the policy change acknowledged that privacy between countries is rooted in reciprocity, reasoning that if the U.S. made efforts to protect foreign citizen data, others would make efforts to protect the personal information of U.S. citizens.
Adopted by most agencies and IC via PPD-28
Covered country decertification if: (a) no longer effectively shares information with the United States for law enforcement purposes, (b) no longer has appropriate privacy protections for such shared information, (c) fails to permit the transfer of personal data for commercial purposes between the territory of the covered country and the territory of the United States, or (d) impedes the transfer of information (for purposes of reporting or preventing unlawful activity) to the United States by a private entity or person. 5 U.S.C. § 552a note


-This group was convened on the initiative of Jacob Kohnstamm, chairman of the Dutch Data Protection Authority, and jointly
organized by the Massachusetts Institute of Technology Cybersecurity and Internet Policy Research
Initiative, and the University of Amsterdam's Institute for Information Law.
-Published a report based on a series of in-person meetings and discussions among a group of independent EU and US experts in the field of privacy and data protection. Presented at 2015 International Conference of Privacy and Data Protection Commissioners in Amsterdam.
-Ten bridges

# Privacy bridges (2)

- Criticism: Failed to recommend needed legal reforms
- Current Activity:
  - New work commencing on Bridges 2 and 3, i.e., researching technical solutions, business models and company policies to help enhance users' control of their data as they engage with digital services, and that enable users to understand how data they provide are used and for what purposes.
  - Spur adoption by companies of innovative and privacy-protective solutions, where a condition for successful adoption of these solutions is approval and endorsement by data protection authorities.

## Questions?