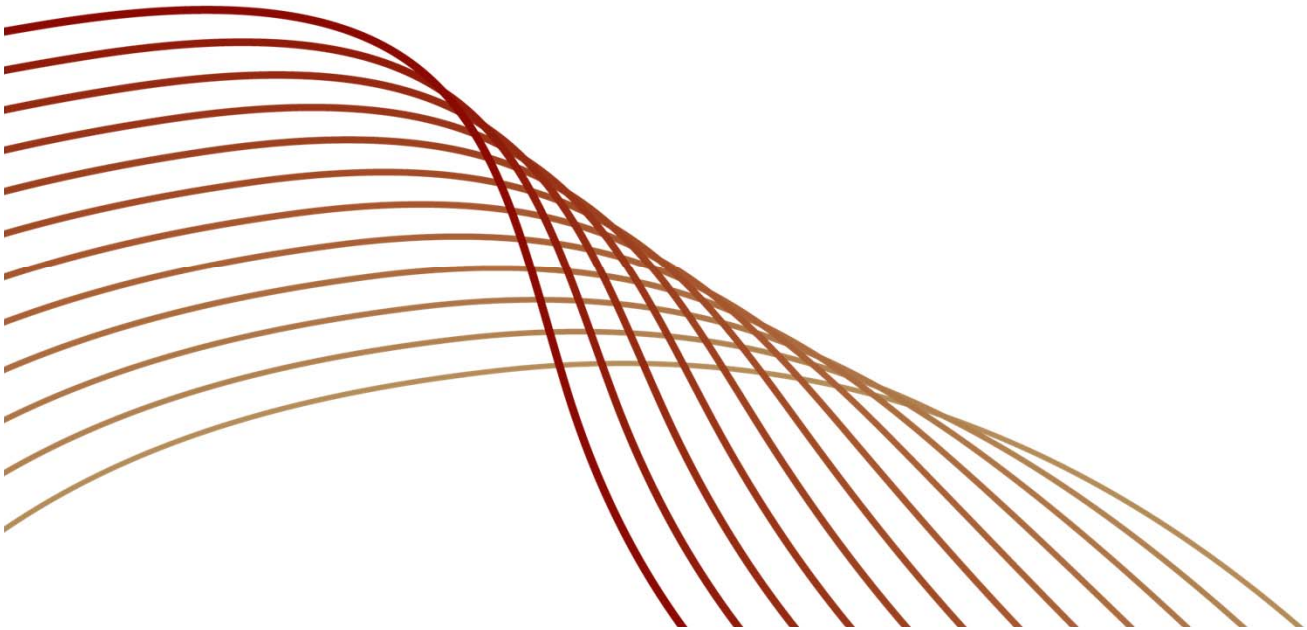
# PRACTICAL CONSEQUENCES OF THE EU DECISION ON SAFE HARBOR

Tuesday,
October 13, 2015

## 10 OPTIONS TO CONSIDER MOVING FORWARD NOW



PAUL
HASTINGS

# PROGRAM AGENDA



- **Introducing Paul Hastings Privacy & Cybersecurity Experts**
- **U.S.-EU Safe Harbor: Brief Background**
- ***Schrems v. Data Protection Commissioner***
  - Background
  - Two Key Holdings
  - Unanswered Questions
- **Ten Steps to Consider Moving Forward Now**
  - Focus on Model Contract Clauses and Options
- **Questions and Answers**

PAUL HASTINGS

# PAUL HASTINGS PRIVACY & CYBERSECURITY EXPERTS

**Behnam Dayanim**
Washington, D.C.

**James Koenig**
New York, NY

**Sherrese Smith**
Washington, D.C.

**Ashley Winton**
London

PAUL
HASTINGS

# U.S.-EU SAFE HARBOR: BRIEF BACKGROUND



- **Trans-Border Data Flow Provisions.** EU Data Protection Directive 95/46/EC, which went into effect in October 1998, prohibits transfers of personal data to third countries that do not ensure an "adequate level of protection."
- **EU-US Safe Harbor Accord.** The Clinton Administration negotiated the U.S.-EU Safe Harbor program, enabling U.S. organizations to transfer data from the EU to the United States based on their declared compliance with seven privacy principles: notice, choice, onward transfer, security, data integrity, access and enforcement.
- **Safe Harbor Program Determined Adequate.** In 2000, the European Commission ("EC") found the Safe Harbor program provided adequate protection, in line with the Data Protection Directive. Many companies depended on Safe Harbor to transfer data from the EU to the U.S. (or as the backbone of global transfers).

**Change of Opinion.** The European Court of Justice ("ECJ") invalidated that decision last week.

PAUL HASTINGS

# *SCHREMS v. DATA PROTECTION COMMISSIONER*



- **Background**: Maximillian Schrems, an Austrian national, filed a complaint with the Irish Data Protection Commissioner challenging the transfer of his personal data from Facebook Ireland to servers of Facebook, Inc. located in the United States.

**Impact of Snowden and Surveillance.** Citing revelations by Edward Snowden, Mr. Schrems alleged that the United States did not ensure adequate protection of personal data against surveillance by public authorities.

- **Irish Commissioner POV.** The Irish Commissioner believed he was not required to investigate the matter, in light of the EC's 2000 decision regarding the adequacy of the Safe Harbor program.
- **Appeal to ECJ.** Mr. Schrems appealed to the High Court of Ireland, which stayed the proceedings to seek guidance from the ECJ.

# *SCHREMS*: ECJ DECISION - TWO KEY HOLDINGS:



1) **EC's 2000 Decision Overturned.** ECJ overturned EC's 15-year old decision that U.S.-EU Safe Harbor Accord provide an adequate level of protection of the personal data of EU citizens.
   - **ECJ Focus #1 -** Public authorities' generalized access to the content of electronic communications; and
   - **ECJ Focus #2 -** The lack of legal remedies available for individuals to access, correct or erase their personal data.
2) **DPAs to Review/Investigate Complaints.** National data protection authorities ("DPAs") in the European Economic Area ("EEA") to hear/investigate individual complaints regarding the transfer of their personal data outside of the EEA (regardless of whether the EC has issued an adequacy decision).

**Net Effect – Complexity and Need to know Your Data and Flows!** This may significantly disrupt existing company global data flows, or at a minimum, add layers of complexity as it will put some premium on knowing which national authorities will have what jurisdiction over various types of data and IT operations (e.g., over servers, information, etc.).

# UNANSWERED QUESTIONS



- Is the Safe Harbor truly annulled?
- When does the decision take effect? Does it apply retroactively?
- Whom does this impact? (If I am not Safe Harbor-certified, should I care?)
- Are there options to obtain guidance?
- What does this mean for the negotiations for a more robust Safe Harbor?
  - The Umbrella agreement has just been approved (but the Judicial Redress Bill needs to be put in place).
- What about model contracts? Does the decision affect them?

# TEN STEPS TO CONSIDER MOVING FORWARD NOW



## *Ideas Others Are Pursuing . . . Risk Management*

1. **Review Data Flows and Prioritize Remediation.** Inventorying what personal data are being stored and transferred and prioritize key data transfer activities that must remain intact (business or operationally critical).
2. **Consider Legal and IT Solutions.** Focusing efforts toward ensuring data transfer and storage solutions are in place or can be rerouted or stored in a way to minimize risks (or avoid using a Safe Harbor-supported pathway).
3. **Review Vendor Contracts that Rely on Safe Harbor Transfers.** Assessing vendor potential non-compliance and if supplier was Safe Harbor certified (they may be in breach of reps and warranties as to compliance with applicable law; yet, you, as data controller, may be liable under data protection law).
4. **Consider EU Country-by-Country Leeway.** Identifying where servers in the EU are located, and the specific local requirements and privacy protections, as national authorities will have greater leeway (and offer more flexibility). Some countries permit self-determination of "adequacy."

## *. . . Internal Flows*

5. **Put Model Contracts in Place.** Putting in place Model Contracts/Intra-Group Agreements to cover any data transfer or access gaps they feel they may have.

# TEN STEPS TO CONSIDER MOVING FORWARD NOW [9]

## *. . . Internal Flows (continued)*

6. **BCRs and Consent Longer Term.** Considering binding corporate rules as one additional data transfer mechanism to also put in place.
   - Note: BCR audit and DPA approval requirements; Consent must be explicit, fully informed, may not be conditional and may be revoked).

## *. . . Vendor and Other Third Party Flows*

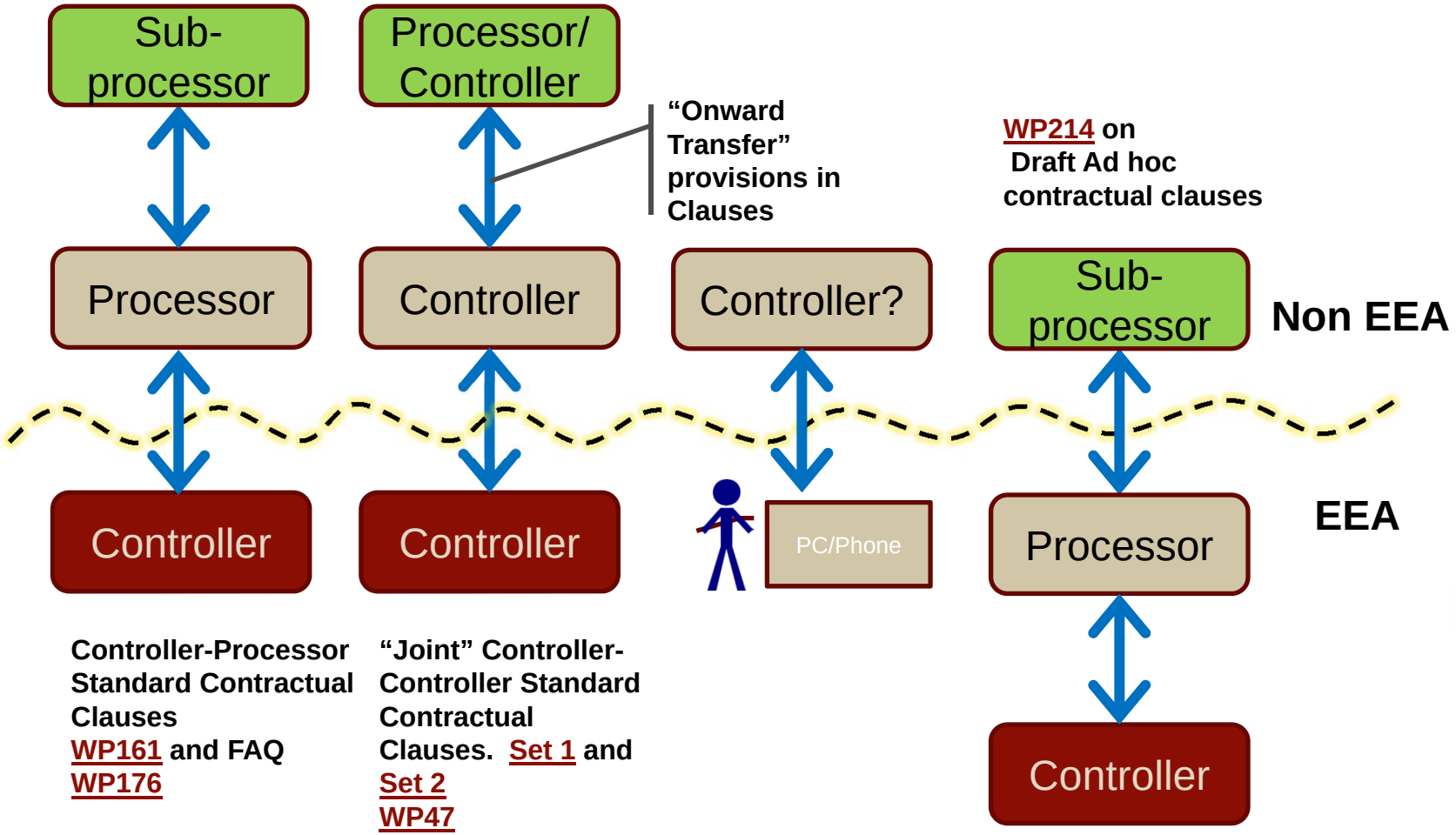
7. **Model Contracts, BCRs or IT Solutions.** Putting in place Model Contracts (or BCRs for processors or "hybrid BCRs") to cover any data transfer or access gaps. If amending contracts with suppliers, ensure that you know who will pay for the cost of future changes to law – e.g. the General Data Protection Regulation is due in 2-3 years.
8. **Outsource or Data Flow Pathways Modifications.** Outsourcing data storage or certain IT operations to vendors with data transfer mechanisms in place.

## *. . . Other Good Ideas*

9. **DPA Outreach.** Reaching out to Data Protection Authorities to build relationships and trust.
10. **Monitor Consumer Complaints Process.** Updating consumer complaint and redress procedures to heighten alert to any specific requests or complaints as we expect more individuals to raise issues.

PAUL HASTINGS

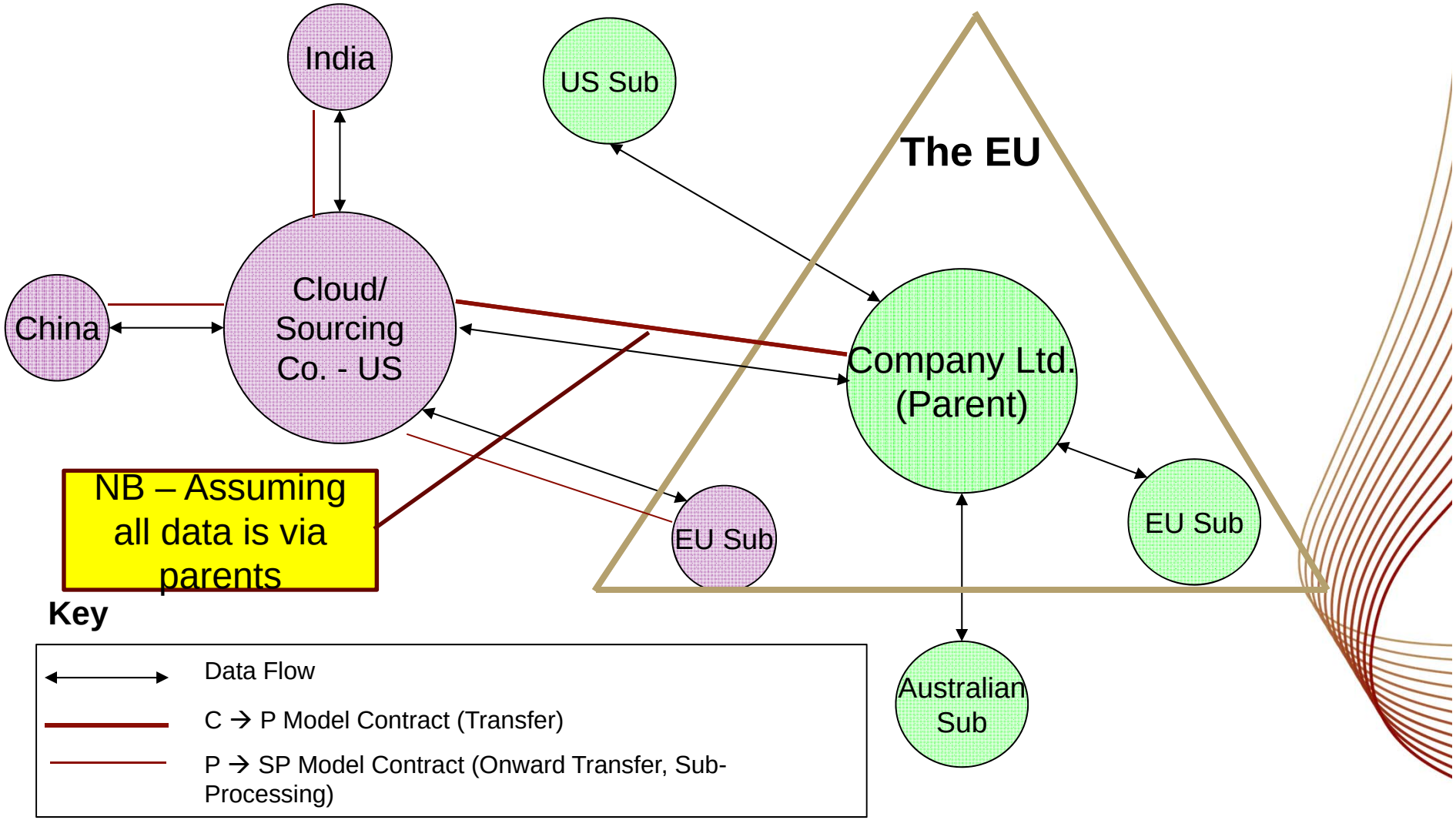
# MODEL CONTRACT CLAUSES - TYPES




**Understanding how data are being used and identifying the right type of contract are essential.**

PAUL HASTINGS

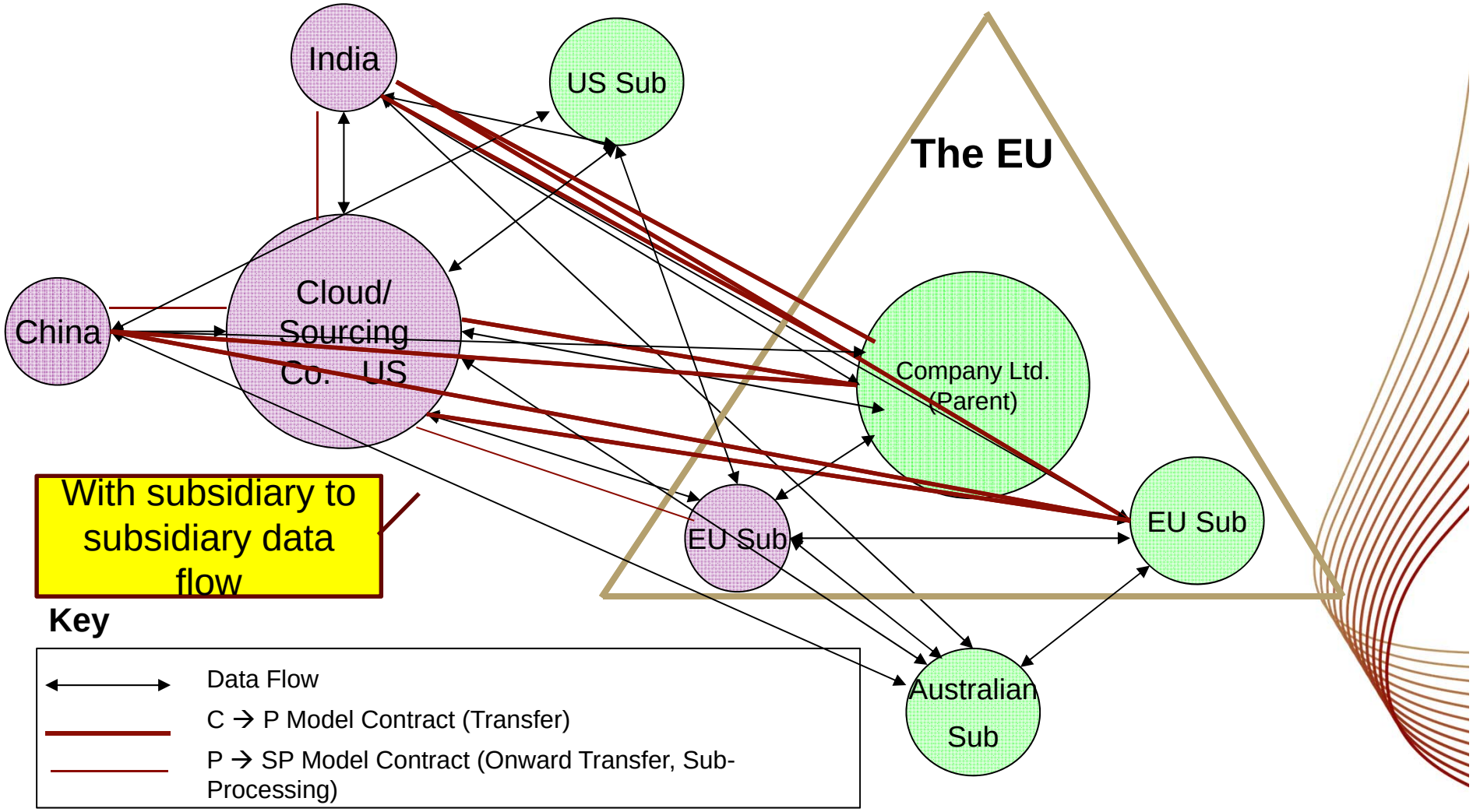
# EU DP LAW – MODEL CONTRACT STRUCTURE




**Mapping the data flow is important (Yes, it's complicated.)**

PAUL HASTINGS

# EU DP LAW – MODEL CONTRACT STRUCTURE




**Lack of careful thought and experienced advice can result in unnecessary complexity.**

PAUL HASTINGS

# QUESTIONS


Behnam Dayanim
+1.202.551.1737
bdayanim@paulhastings.com

Jim Koenig
+1.610.246.4426
jimkoenig@paulhastings.com

Sherrese Smith
+1.202.551.1965
sherresesmith@paulhastings.com

Ashley Winton
+44 (0)20.3023.5121
ashleywinton@paulhastings.com

Our Twitter: @PHPrivacy
Our blog: www.caveat-vendor.com

PAUL HASTINGS