Cross-border Data Privacy

vis-à-vis The False Tradeoff Between Privacy and Security

Trevor Miranda       Jonathan Scrivanich
Table of Contents

1. Introduction
   a. Raison d'être

2. Current Policies
   a. EU-US Privacy Shield
   b. APEC Privacy Framework
Introduction
“Transfers of personal data are an important and necessary part of the transatlantic relationship, especially in today’s global digital economy.”[1]
Raison d'être

● Every country has their own standards of privacy
  ○ And securing data
● Countries want to guarantee some standard to citizens
● Ability to regulate/prosecute across borders
  ○ Guidelines are cute, meaningless without enforcement
● Differing policies are confusing and dangerous
● Standardize practice, protect consumer data and privacy
Current Policies
EU-US Privacy Shield

Overview

● Replacement for the “Safe Harbour” framework
  ○ Previous agreement between EU and US (15 years of use)
  ○ Invalidated by Maximilian Schrems v. Data Protection Commissioner

● Requirements decided in case now matched by “Privacy Shield”
  ○ European Commission approved in 12 July 2016
  ○ Operational since 1 August 2016

● More than 2,400 companies certified as being in compliance in 2017\(^2\)
  ○ Enforced by many US Federal departments and EU courts
EU-US Privacy Shield

1. Consumer right to be informed
2. Limitations on company for use of data for different purposes
3. Obligation of company to minimize required data and time stored
4. Obligation of company to secure data
5. Obligation of company to protect data when transferred to another company
6. Consumer right to access and correct data
7. Consumer right to lodge a complaint and obtain remedy against company
8. Redress for consumer if data accessed by US public authorities
Privacy Shield And Solove

- US companies have begun to self-certify and transfer data under the agreement.
  - Self-certification inherited from the Safe Harbor framework meaning that to verify compliance the company can either do a self-assessment or get outside compliance review.

- Ombudsman
  - The office would be situated an part of a government (The US) that supervises government agencies
  - The unbiased ombudsman would be regulated and controlled by US laws.

- “The executive branch could veil its actions in secrecy, preventing any accountability to the people” (Solove 90)
US Law Inadequacies Still Remain

- Specifically, the US continues to deny the relevance and application of internationally-accepted standards of necessity and proportionality in its surveillance operations.
- Solove makes similar remarks about the US and its surveillance when he references the Church Committee’s report on US surveillance where they declared:

  “Too many people have been spied upon by too many Government agencies and [too] much information has [been] collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power.”

- US has no national laws regulating the collection and use of personal data. Only federal privacy-related laws in particular categories: HIPAA, FTC Act, etc.
APEC Privacy Framework

- Asia-Pacific Economic Cooperation
  - Collection of economic partners in the Asia-Pacific
    - China, Peru, Russia, United States, Australia, Korea, etc.
  - Combined with the “Cross-border Privacy Rules” (CBPR)
    - Relies on organizations’ self-assessments[^3]
    - APEC must certify organizations in compliance initially[^3]
- Enforcement by “Accountability Agents”
- Framework endorsed all 21 members in November 2004, CBPR in 2011
- Far fewer actually intend to participate (5 members)[^3]
APEC Privacy Framework

Privacy Principles

1. Information should be protected from misuse
2. Information collectors should make their practices/policies known
3. Collection should be limited to specific purposes
4. Information collected should only fulfill those purposes
5. Individuals should be given a choice in collection
6. Information should be accurate and timely
7. Collectors should adequately protect information
8. Individuals should be able to access and correct data about them
9. Collectors should be held accountable to these principles
APEC Strengths

- Organizations submit a self-assessment questionnaire along with relevant documentation to an APEC-recognised accountability agent. The agent then decides if the organization is in compliance.

- Enforces remedies for infringement on an organization’s proposed CBPR plan.
Principle 2 Notice

● Data controller must include a notice to individuals when collecting their Personal Information (PI)

● Weaknesses: “Reasonably practical steps shall be taken to ensure notice is provided”
  ○ Recognizes circumstances may be impractical to give notice:
    ■ Automatic collection such as cookies
    ■ ex/ a third party insurance company collecting employees information from an employer in order to provide medical insurance services.

● Leaving the discretion of defining what is reasonable to the organizations.
  ○ “The executive branch may be the appropriate branch for developing security measures, but that does not make it the most adept branch at establishing a balance between security and liberty.” (Solove 41)
Principle 3 Collection Limitation

- Lawful and fair collection of PI limited to what is relevant to the purpose of collection
- Weakness: Provides exceptions “where providing notice would be inappropriate”
  - In an outbreak of food poisoning, it would be appropriate for the relevant health authorities to collect the PI of patrons from restaurants without providing notice to or obtaining the consent of individuals in order to inform them of the potential health risk.
  - “Transparency is what keeps the government accountable to the people”(Solove).
Principle 4 use of PI

- PI should be used only to fulfill the purposes of collection and other compatible or related purposes except for:
  - The individual provides consent for the information to be used for other purposes
  - When necessary to provide a service or product requested by the individual
  - By the authority of law and other legal instruments, proclamations and pronouncement of legal effect

- Weakness 3rd exception:
  - Encourages organizations to blindly accept government acquisitions as they are protected from this exception.
  - “The dire claims the government made about national security were bogus, just a way to cover up what the Pentagon Papers revealed—that the government had made deceptive claims about the Vietnam War.” Solove (67).
Overall Weaknesses

- Many exceptions for each principle
- Organizations are given discretion which is a dangerous power.
Thanks for listening!

Any questions?
References


