The Efficacy of the US Safe Harbor Agreement

Jesse Sowell

Technology and Policy Program
Engineering Systems Division
MIT

Question

Online Privacy

Are online privacy policies and terms of service compliant with the EU Data Protection Directive?

Characterize

If so, characterize the compliance . . .

Policy Compliance

- Different countries (cultures, societies, groups, regions, *ad nauseum*) have different privacy paradigms (Westin, Bennett, Solove, Nissenbaum)
  - Europe: socially protective (read *proactive*)
  - US: normatively liberal (read *reactive*)
- EU Data Protection Directive (EU-DPD) is an attempt at policy convergence (Bennett)
  - Harmonize EU member states' privacy regulations
  - Non-EU states must have "adequate" regulations

Policy Compliance

- Different countries (cultures, societies, groups, regions, *ad nauseum*) have different privacy paradigms (Westin, Bennett, Solove, Nissenbaum)
  - Europe: socially protective (read *proactive*)
  - US: normatively liberal (read *reactive*)
- EU Data Protection Directive (EU-DPD) is an attempt at policy convergence (Bennett)
  - Harmonize EU member states' privacy regulations
  - Non-EU states must have "adequate" regulations

Policy Convergence Externality

EU states not allowed to play with "inadequate" states . . .

Externality and "Solution"

- Externality
  - EU cannot share with US
  - Potentially halt trans-Atlantic dataflows
- Resolution - US Safe Harbor (US-SH)
  - Hybrid (Farrell) compromise between EU and US Dept. of Commerce
  - Self-regulation via participation in the US-SH
    - EU: data authorities
    - US: self-regulation enforced by market and reputation

Externality and "Solution"

- Externality
  - EU cannot share with US
  - Potentially halt trans-Atlantic dataflows
- Resolution - US Safe Harbor (US-SH)
  - Hybrid (Farrell) compromise between EU and US Dept. of Commerce
  - Self-regulation via participation in the US-SH
    - EU: data authorities
    - US: self-regulation enforced by market and reputation

Efficacy of Policy Convergence

Do the US-SH's market-based enforcement mechanisms give the same guarantees as the EU-DPD data authorities?

Privacy is Difficult to Define

Westin's Definition of Privacy

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

- Vague, abstract conceptual definition
- When operationalized, typically becomes too narrow for general application (Solove)

Legal and Political Perspectives on Privacy Regulation

- Units of Analysis
  - Governance Paradigm (Reidenberg)
  - Sovereignty and Jurisdiction (Kobrin, Long, Regan)
  - Organization (Reidenberg, Regan)
  - Individual, Contextual Integrity (Nissenbaum)

Legal and Political Perspectives on Privacy Regulation

- Units of Analysis
  - Governance Paradigm (Reidenberg) (socially-constructed)
  - Sovereignty and Jurisdiction (Kobrin, Long, Regan)
  - Organization (Reidenberg, Regan)
  - Individual, Contextual Integrity (Nissenbaum)

Legal and Political Perspectives on Privacy Regulation

- Units of Analysis
  - Governance Paradigm (Reidenberg) (socially-constructed)
  - Sovereignty and Jurisdiction (Kobrin, Long, Regan)
  - Organization (Reidenberg, Regan)
  - Individual, Contextual Integrity (Nissenbaum)

Organizations and Regulators

The explanatory component focuses on the tension between **economic efficiency** and **individual privacy**

Literature: US-SH is Empty Formalism

Information in American Business

The very idea that a simple transfer of information between a parent company and its affiliates can be subject to restrictions seems unthinkable to U.S. executives, most of whom have grown up in a society where information has always flowed freely across thousands of miles. (Buss)

Literature: US-SH is Empty Formalism

Information in American Business

The very idea that a simple transfer of information between a parent company and its affiliates can be subject to restrictions seems unthinkable to U.S. executives, most of whom have grown up in a society where information has always flowed freely across thousands of miles. (Buss)

US-SH Effects

- Exacerbates tension between US and EU governance paradigms
- US-SH actively obstructs progress toward resolving privacy issues (Reidenberg)

Two Analysis Phases

- Textual Analysis (Cases)
  - Read and annotate privacy policies and terms of service
  - Evaluate compliance with EU-DPD and US-SH
- Implications
  - Stakeholders involved in developing EU-DPD and US-SH
  - Differences in enforcement mechanisms
  - Source of conceptual refinement

Hypotheses

Null Hypothesis H_0

Privacy policies are compliant with the intentions of the EU-DPD and US-SH.

Hypotheses

Null Hypothesis H_0

Privacy policies are compliant with the intentions of the EU-DPD and US-SH.

Alternative Hypothesis H_{a1}

Privacy policies are not compliant with the intentions of the EU-DPD and US-SH.

Hypotheses

Null Hypothesis H_0

Privacy policies are compliant with the intentions of the EU-DPD and US-SH.

Alternative Hypothesis H_{a1}

Privacy policies are not compliant with the intentions of the EU-DPD and US-SH.

Alternative Hypothesis H_{a2}

Privacy policies are compliant with the **black letter** of the US-SH, but derogate the intentions of the EU-DPD.

Hypotheses

Alternative Hypothesis H_{a2}

Privacy policies are compliant with the **black letter** of the US-SH, but derogate the intentions of the EU-DPD.

Stated Another Way . . .

The US-SH is an empty formalism.

Exchanging Information for Services

- Businesses $\longrightarrow$ online service providers
  - Google, Amazon, Facebook, Ebay, etc.
  - In exchange for your valuable information, OSPs give you valuable services
  - Bounded rationality and rational ignorance

Exchanging Information for Services

- Businesses $\longrightarrow$ online service providers
  - Google, Amazon, Facebook, Ebay, etc.
  - In exchange for your valuable information, OSPs give you valuable services
  - Bounded rationality and rational ignorance
- EU Commission and States
  - Privacy is a human right
  - Enforce privacy regulations

Exchanging Information for Services

- Businesses $\longrightarrow$ online service providers
  - Google, Amazon, Facebook, Ebay, etc.
  - In exchange for your valuable information, OSPs give you valuable services
  - Bounded rationality and rational ignorance
- EU Commission and States
  - Privacy is a human right
  - Enforce privacy regulations

Result:

Businesses consider strict privacy regulation “onerous”

Significant Conflicts

Information Hiding (Asymmetries)

- Coarse-grained data purposes
- Nearly as conceptual as FIPs
- Difficult to differentiate or imbue with reputation

All-or-nothing tactics

- Accept existing data collection or get service elsewhere
- Serves to lock users in to distorted privacy preferences
- Exacerbates utility privacy trade-off

Significant Conflicts

Information Hiding (Asymmetries)

- Coarse-grained data purposes
- Nearly as conceptual as FIPs
- Difficult to differentiate or imbue with reputation

All-or-nothing tactics

- Accept existing data collection or get service elsewhere
- Serves to lock users in to distorted privacy preferences
- Exacerbates utility privacy trade-off

Significant Conflicts

Information Hiding (Asymmetries)

- Coarse-grained data purposes
- Nearly as conceptual as FIPs
- Difficult to differentiate or imbue with reputation

All-or-nothing tactics

- Accept existing data collection or get service elsewhere
- Serves to lock users in to distorted privacy preferences
- Exacerbates utility privacy trade-off

Implications

Implications

- US-SH confirmed as an empty formalism
- Organizations protect their privacy interests
- *Current* hybrid regulation does not work
  - Information hiding retards development of reputation
  - Market mechanisms cannot bind
  - No clear means to verify
  - Licensing mechanisms are simply rubber stamps
- Obstructs ongoing development (all-or-nothing)