Reconciling Personal Information in the United States and European Union

Paul M. Schwartz, Berkeley Law School
1st Annual Digital Economy Congress
San Diego
November 15, 2013
A Tale of Two Papers

**The PII Problem: Privacy and a New Concept of Personally Identifiable Information**

Paul M. Schwartz† & Daniel J. Solove‡

Personally identifiable information (PII) is one of the most central concepts in information privacy regulation. The scope of privacy laws typically turns on whether PII is involved. The basic assumption behind the applicable laws is that if PII is not involved, then there can be no privacy harm. At the same time, there is no uniform definition of PII in information privacy law. Moreover, computer science has shown that in many circumstances non-PII can be linked to individuals, and that de-identified data can be re-identified. PII and non-PII are thus not immutable categories, and there is a risk that information deemed non-PII at one time can be transformed into PII at a later juncture. Due to the malleable nature of what constitutes PII, some commentators have even suggested that PII be abandoned as the

---

RECONCILING PERSONAL INFORMATION IN THE UNITED STATES AND EUROPEAN UNION

By

Paul M. Schwartz*
Daniel J. Solove**


September 6, 2013

I. INTRODUCTION .................................................................................................................. 3

II. DEFINING PII ON BOTH SIDES OF THE ATLANTIC .............................................. 5

   A. The European Union: From the Directive to the Proposed Regulation 6
      1. The EU Data Protection Directive ................................................................. 6
      2. The Proposed Regulation ............................................................................ 9
   B. The United States: A Lack of a Uniform Standard .............................................. 11
   C. Personal Information: A Problem on Both Sides of the Atlantic ............... 14

   1. Evaluating the EU Approach .......................................................................... 14
   2. Evaluating the U.S. Approach ........................................................................ 19
   3. The Disjunction Between the U.S. and EU Definitions of PII ..................... 22

III. PII 2.0 ........................................................................................................................... 26

   A. An Explanation of PII 2.0 ................................................................................... 26
Three Approaches to PII in US Law

1. Tautological Approach

2. Non-Public Approach

3. Specific Types Approach
EU Approach

- EU defines PII to encompass all information identifiable to a person.
- Directive: “identifiable” person is one who can be “identified, directly or indirectly”

- Proposed Regulation: personal data is “any information relating to a data subject”
- Data subject is person who “can be identified, directly or indirectly, by means likely to be used”
No uniform international definition of PII

- PIPEDA uses term “identifiable” data
- Tendency is for broad definition of PII: PIPEDA reflects EU perspective
Risk of Identification

- Zero Risk
- Very low risk
- Nontrivial risk
- Moderate risk
- Very high risk

Identified
Abandon PII?
Abandon PII?
PII 2.0: Three categories

Identified
Identifiable
Non-Identifiable
PII 2.0: Three categories

Identified

• plus identifiable data when significant probability of linkage to specific person

Identifiable

Non-Identifiable
A Bridge to Europe?

- At times, EU law does acknowledge that the full rigor of EU data protection law need not apply to all types of personal information.
- Article 10, Proposed Regulation: data controllers need not control more personal information to comply with Regulation.
- 2011 opinion on geolocational data: all information does not merit same set of FIPs.
• Identifiability is a continuum of risk

• Not a hard “off-on” switch, but tailored Fair Information Practices (FIPs)
PII 2.0

- Full FIP’s for **identified information**
- Identifiable information: data security, transparency and data quality
- No FIP’s for non-identifiable information
Bottom line

• Need for a harm-based approach to information privacy law
• Identifiable data does deserve some protection