

Origins of Data Protection Laws,
and ramifications for
“journalistic purpose”, publicly
available data, and unique
national identifiers

kyungsinpark@korea.ac.kr

Open Net Korea

Korea University Law School

2014.7.10 Tokyo, Japan

Asian Privacy Scholars Network

Contents

1. Origins of data protection laws
2. “publicly available data”
3. “journalistic exceptions”
4. How to handle unique national identifier
(Korea situation)
5. Conclusion

Origins of “Property”-like Personal Data Right

- “Data Surveillance” Alan Westin <Privacy and Freedom> (1967)
- Traditional surveillance – obtaining of data about another against his will from-within his private boundaries
- Data surveillance – obtaining of data voluntarily made available by data subjects
- What is wrong w/ voluntary transfer ? – incomplete agreement on scope of use and transfer upon turning over the data
 - equivalent to UNCONSENTED use and transfer and therefore SURVEILLANCE
- Solution: Contract law not sufficient, need a Property right!
→ Peculiar Concept that One owns data about himself or herself.

free speech v. data protection

- Speech = exchange of data
- Data protection = “property-like” right on data about oneself
 - Right to consent for collection, use, transfer
 - Right to inspect and correct
- Data subject controlling flow of data →
Data subject as a Censorer

Publicly Available Information

- Publicly available information:
 - (1) involves no unique point of 'turning over'
 - NO "incomplete agreement" problem
 - Rebuttal?: "All personal data are originally from data subjects." Is this true?
 - (2) Is it surveillance to collect information that everyone knows?
 - ___ I know that you know X about me
 - ___ I don't know that you know X about me

Solution

- 1980 OECD “data with no privacy-infringing risk” exception
- 2000 EU-US Safe Harbor excluding publicly available data
- 2004 APEC’s “publicly available data” exception (Canada, Australia, Belgium, etc.)

“Journalistic Purpose” exception

- Definition of “journalistic purpose” – all publication intending for all readers ECJ (Case 73/07 Satakunnan Markkinapörssi and Satamedia)
- Does publication of information for everyone to read constitute ‘data surveillance’?
 - no data imbalance
 - 1995 EU Directive’s “journalistic purpose”

Unique National Identifiers

- “function creep”, it is bad but what does it really mean? = (1) Dependence on UNI + (2) High Risk of data breach due to availability → hacking and surveillance (3) made even easier b/c of uniformity
- “Paradox of Trust” explains how Reliability causes Both Dependence and Data Breachability, destroying Reliability
- → all national identifiers come with restriction on collection **cf.** Korea has 866 exceptions!

Conclusion

- UNI cannot be collected with or without consent. Strict liability! No consideration for potential for data surveillance → publicly available or not, no processing allowed.
- But, UNI is never deemed publicly available data → Therefore, no conflict?
- How about face image? Facial image can become publicly available and uniquely identifying at the same time. Where do you draw the line?