

Data Protection Law and future of Malaysian data privacy

K.S. Park

Korea University Law School

kyungsinpark@korea.ac.kr

Open Net Korea

www.opennetkorea.org

Privacy - Basics

- Intrusion into privately held area OR
Revealing privately held information →
privacy infringement
- Exception: to save life, protect security,
reveal corruption
- How about "to investigate crime"? OK but
since the powerful actor, the state is
doing it, presumption of innocence
requires special procedure

Warrant Doctrine

- Special protection when State is infringing individuals' privacy for criminal punishment
 - Warrant = "Probable cause" certified in writing by a responsible official independent of and disinterested in prosecutorial progress
 - Why? Due process = no rights to be infringed before notice and hearing before neutral tribunal → how do you force hearing on unwilling individuals? - a quasi-hearing based not on conviction but on probable cause

What is private?

- US: categorical (black & white) **3rd party doctrine**
 - Supreme Court: “metadata acquisition not a “search” so not need warrant” but US Congress changed law by making some metadata subject to court order
- EU: incremental - e.g. walking in gay pride march not considered voluntary giving up of privacy
- US: becoming more incremental – **Jones** (location tracking), **Riley** (mobile phone search), **Carpenter** (cell tower location no 3rd party doctrine)
- Anyway, when it comes to criminal investigation, EU=US because of public interest –e.g. French police collecting info at gay pride march will not need warrant. **Difference is when private parties collect and use data.**

Data Protection Law

- Definitions:
 - Personal Data – all data about an identifiable person – INCLUDING PUBLIC DATA
 - Data Subject – the person whom the personal data is about
 - Data File – an aggregate of personal data made easily searchable
 - Data Controller – a person who operates the data file for business purposes
- Consent Right: **All Data Controllers must NOT process unless Consented to by Data Subjects EXCEPT. . . Public interest, etc.**
- **ALSO**, Data Subjects have **absolute [can't be forfeited by consent]** right of access, right of correction, right to oppose/stop processing (RTBF?), right to delete (RTBF?), and right to receive notifications of breach.

Rights of data subjects (= duties of data controllers)

- Specific Consent for collection, use, disclosure, or any other kind of processing
- Notification to data subject in event of collection from 3rd party
- Right to inspect (access)
- Right to correct
- Right to "opt out" or delete data about themselves
- Notification to data subject in event of breach

Classical privacy vs. modern broader privacy (data protection law)

- Privacy
 - Applicable only to confidential information
 - Protects only from collection and disclosure (usually to the public) **against data subject's will**
- Data protection
 - Usually applies to all information including non-confidential ones
 - Protects from collection and disclosure **not affirmatively approved by data subject**

Default: **All personal information is “private” unless indicated otherwise!**

Own Data about Oneself

- "K.S. Park is a Professor."
 - Let's assume you run an educational website and want to spread info about K.S. Park. You need my consent to receive that data?
 - You need my consent for you to relay that data to a 3rd person?
 - You need my consent for you to use that data in making comments about me?
-
- Owning data as if you own a car → Let's say you let your friend borrow a car from you for weekend use inside the city
 - consent for new use
 - consent for transferring to a 3P
 - right to get it back
 - right to check

So, limited application

- Applied only against DATA CONTROLLERS (using data file for business purposes) cf. phone numbers list in your personal mobile phones?
- Applied only against **Searchable files** cf. your lecture notes

What is good about data protection law?

- You go to library to check out a book. The library keeps the list of books you checked out.
- Can the library sell the data to election campaigners so that they will contact you selectively for political bias?
- Can the library use the data to figure out your political beliefs?
- What if the library keeps incorrect data?

Good usage of data protection norms

- Striking down internet real name law
- Striking down warrantless access to user data
- Forcing telcos to respond to data access
- Forcing telcos to notify breaches
- Stopping sale of user data to others for marketing purposes
- Targeted advertising

Targeted advertising

- Behavior data – what sites/postings do you read for how long?
- Targeted advertising uses behavioral data
- When you sign on FB or Youtube, what do you agree to and what do you expect?
- How about behavioral data on 3rd party websites?
- Can sign-up clicks be consent for collecting and processing 3rd party websites?
- Korea' s PIPC Sept 2022: "Hard for consumers to expect 3rd party websites to be used for marketing"
- Europe: Affirmative cookie consent

Role of Meta/Google

- Meta/Google already have much individual preferences data → can put "targeted" banner ads if they know when individuals visit websites with banner ad spaces
- Website operators wanting more \$\$ for their online spaces can sign up to let Meta/Google place "targeted" ads on their website spaces.
- At the same time, they can inform Meta/Google the fact that users visited their websites, augmenting the individual preferences data.

Harms of targeted advertising

- Filter bubble / Echo chamber → extremism
- Works with content monetization → rewards posting of extreme content by recommending them → extremism
- But benefits of targeted advertising: SME website operators can sell their online presence at \$\$\$ → independence of journalism
- What to do? – moderation by data protection law → informed consent

Cookie consent

- Origin of "cookie" – Hansel and Gretel leaving cookie crumb not to get lost in the Dark Forest
- Instead of leaving crumbs in location visited, user keeps records of locations visited as a file on the device so other apps/webs user visit will know where user has been
- GDPR requires consent for data collection and "cookie" automates collection so requires consent
- Originally, consent implied by visiting but GDPR requires explicit consent → cookie consent rule → website operators doing targeted advertising must obtain "informed consent", meaning, for non-essential (like marketing) cookies, can only "opt-in" (explain "opt-out")

Malaysian solution

Art 43. (1) A data subject may, at any time by notice in writing to a data user, require the data user at the end of such period as is reasonable in the circumstances to cease or not to begin processing his personal data for purposes of direct marketing.

Can Data Protection work as censorship?

- Right to be forgotten on previous publication: Court judgment database not open to public because of "data protection concerns" with parties and witnesses
- Control on First publication:
 - presidential office threatening to file criminal complaint on a journalistic article
 - police filing criminal complaint for a video revealing oppressive interrogation tactics
- Data protection law **can** work as censorship because it gives ownership-like control over all personal data, not just private or defamatory data

"Is data ownership feasible?"

- Data: "A and B met at C's restaurant."
- Who owns the data? A, B or C? or all of the above.
- How about "X and Y met at C's restaurant when X and Y are not identifiable"?
- If all of the above, how much information remains for the public to know what goes on in other ppl's lives?

Fight Discrimination?

- “Make Us Blind to Our Own Mistakes” – Is this a proportionate way of fighting discrimination?
- Which is a better society? Voluntary Informed Tolerance vs. Forced, Ignorant Acceptance
- Rehabilitation law vs. RTBF
- RTBF hurts accountability
- How about public interest exception? – You need exception to speak? Should it not be the other way around?

Origins of “Ownership-like” 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 – using or spreading data **voluntarily made available by data subjects** against your wish -. Incomplete or no enforceable agreement on scope of use and transfer upon data disclosure - equivalent to UNCONSENTED use and transfer and therefore **SURVEILLANCE** , e.g., **1983 Census Decision (West Germany)**

Data protection law:

How to stop data surveillance

- Preventing data surveillance
 - contract law enforcing data subject's consent
 - but powerless ppl not able to negotiate scope of use or 3rd party transfer
 - need for ownership where ppl are assumed into (or defaulted into) "owning" data
 - puts obligations on data controllers to affirmatively obtain consent for collection, state reason for collection (use purpose, scope of disclosure), and "ask before using or transferring beyond the consented use/disclosure" → data protection law

Publicly available data

- Lawfully publicly available data does not need correction of bargaining imbalance
→ no need for ownership-like control
- data protection laws of Germany (pre-2017), Canada, Australia, Singapore, Taiwan : exception for publicly available data
- Malaysian law: None

Malaysia RTBF?

Art 38. (1) A data subject may by notice in writing withdraw his consent to the processing of personal data in respect of which he is the data subject.

- (2) The data user shall, upon receiving the notice under subsection (1), cease the processing of the personal data.

Art 37 "expression of opinion" note → even correct information needs be editorialized.

Exceptions for journalism

- GDPR – exception for journalistic activity
- Malaysia: Good?

Malaysian data exemption, art 45(2) for journalistic activity

- (f) the data user reasonably believes, taking into account the special importance of public interest in freedom of expression, the publication would be in the public interest.

Can it be decided objectively instead of subjectively?

Public interest exception

- Malaysian data protection law: no
- GDPR: public interest exception

Risk prevention, not behavior prevention

- Exceptions for low-risk use or transfer and for greater good usage/transfer
- When data controller's right overwhelms data subject's interest, NO CONSENT needed for collection or use
- When needed to protect life, body, or property, no consent needed for 3r transfer
- When other laws allow or mandate such use or transfer, no consent needed
- How about for "public interest"?

Malaysian data processing consent exemption, article 6 (1)

- (a) for the **performance of a contract** to which the data subject is a party;
- (b) for the taking of steps at the request of the data subject with a view to **entering into a contract**;
- (c) for compliance with any **legal obligation** to which the data user is the subject, other than an obligation imposed by a contract;
- (d) in order to protect the **vital interests** of the data subject;
- (e) for the **administration of justice**; or
- (f) for the exercise of any functions conferred on any person by or **under any law**.

→ **Compare to total exclusion of Government from data protection law. Key is access**

Big Data and AI

- 3V = Variety + Volume + Velocity
- Variety requires combining EXISTING and FUTURE DATABASES but that is unconsented-to use!
- Problem: Creativity comes from UNPREDICTED USE – UNCONSENTED-TO USE
- Solution: Anonymize databases so that data are no longer personal data and therefore can be used w/o consent → Beginning of a new problem?

95 EU Data Protection Directive and 2017 GDPR

- Whether one is identifiable from data should take into account "all the means likely reasonably to be used to identify"
- Identified by whom? - Article 29 Working Party: "By the controller or by any other person", e.g. when the combined original exists. → Does this mean omniscient approach?
- A29 WP: Effective anonymization "prevents (1) singling out an individual in a dataset, (2) linking two records within a dataset (or between two separate datasets) and (3) inferring any information in such dataset. → So, okay.

Is Anonymization Data Processing?

- “Working Party considers that anonymisation as an instance of further processing of personal data can be considered to be compatible with the original purposes of the processing but only on condition the anonymisation process is such as to reliably produce anonymised information”

So Okay to Keep Original somewhere?

- Personal data definition: absolute or relative to data controller?
 - Breyer(ECJ c582/14) on **webhost's** unconsented-to storing of dynamic IP address: "Even though German law prohibits ISP from transmitting the additional data necessary to identify the individual, it appears that, in certain cases, such as a cyberattack, the webhost may contact the competent authority which can in turn obtain the information from the ISP."
- Probably, not an omniscient approach but an objective approach

Anonymization technique

- Randomization: adulterate data
 - noise addition – consistency is key
 - permutation – special case of noise addition
 - differential privacy – depends on what the data requester wants
- Aggregation:
 - k-anonymity, l-diversity and t-closeness
- Pseudonymization? – possible to re-identify with the key – personal data (GDPR)

Malaysian data exemption, article 45(2)

- (c) processed for preparing statistics or carrying out research shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle and other related provisions of this Act, provided that such personal data is not processed for any other purpose and that the resulting statistics or the results of the research are not made available in a form which identifies the data subject;

Difference with GDPR

- Pseudonymized data is still protected by data protection law.

No consent regime but access, correction, etc.

AI depends on big pseudonymized data.

Big Three problems with AI:

- "Garbage in Garbage out" – algorithmic affirmative action needed
- Data monopoly - data portability
- Income inequality - ??

Anyway, to supply data portability and open "affirmative action", we need to apply data protection law on pseudonymized data.