Data Protection and data-related platform governance

K.S. Park

kyungsinpark@korea.ac.kr

Korea University/Open Net

Platform accountability

- Mainly about platforms being used

For disinformation/hate speech or government trolling/censorship

- Platforms affect privacy

- right to be forgotten
- targeted advertising
- data localization
- data retention

Data Protection Rights

- 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

- Data Protection Law: **All Data Controllers must NOT:**

(1) collect or have others collect Personal Data without Data Subject's consent;

(2) use for any purpose other than Consented to by Data Subjects

EXCEPT. . . Public interest, Contract, Life Saving, Data Processing Interest. . .

- **ALSO, AFTER COLLECTED,** Data Subjects have **absolute** right of inspection, right of deletion/correction/halt processing, and right to receive notifications 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! Therefore all processing are prohibited unless consented to otherwise.**

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 or no agreement on scope of use and transfer upon turning over the data

- equivalent to UNCONSENTED use and transfer and therefore SURVEILLANCE

Deep dive on data surveillance

- Classically, no privacy interest attached.
- Solution: Contract law
- not sufficient b/c powerless ppl not able to require contract or identify private/public, need a **property right**! →
- Presumption of "Peculiar" Concept that **One owns data about himself or herself regardless of public or private.**

"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 you 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

Implications

- **Korea:** Court judgments not open to public, all most all news articles pseudonimized
- **Germany:** Spichmich.de case
  - Opinions about teachers – teachers' personal data?
  - Information about teachers

→ Can data protection law act as censorship?

What is good about data protection law?

- You go to bookstore to buy a book. The bookstore keeps the list of books you bought.
- Can the bookstore sell the data to election campaigners so that they will contact you selectively for political bias?
- Can the bookstore use the data to suggest you more books?
- But for data protection law, bookstore thinks "voluntarily given to me, so no privacy. So I can sell". Contract not to disclose or repurpose? no contract is even required.

Good usage of data protection norms in Korea

- Striking down internet real name law – **data minimization** principle
- Striking down warrantless access to user data – **breach notification** principle
- Forcing telcos to respond to data access – right to inspection
- Stopping sale of user data to others for marketing purposes – consent requirement
- Targeted advertising – consent requirement

Problems with RTBF

- Costeja v Google case: fact of publicly announced judicial sale of one lawyer's house delisted from search results (right to halt processing)
- Problem: True, non-private info taken out of search results view
- Court: "no longer relevant" –but relevant from whose perspective? Are we supposed to use data about others only according to data subjects' wishes?
- Origin of problem: Supposed to protect one's privacy but protect one's ALL data, public or private
- But to whom does data belong to? DO YOU REALLY OWN DATA ABOUT YOU?
  - Who should control the data "John Beat Up Jane".
- Possible defense: "no public interest in search-viewing the data" → Can we really impose "public interest" obligations on individuals? Pluralist ideal of freedom of speech?

Deep dive on RTBF

- "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 – the former does not prohibit ppl from sharing the info.
  - RTBF hurts accountability, e.g., the case of Christian Right pastors desiring to delink their past discriminatory remarks during sermon
- Solution: Australia, Canada, India, Singapore,

pre-GDPR Germany exempts publicly available information from data protection law

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 your behavioral data on 3rd party websites?
- Can click-signing FB Terms of Use be consent for collecting and processing 3rd party website ?

Role of Meta/Google

- Can put banner ads "targeted" at you 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.
- In return, they inform Meta/Google the fact and details about the users' visit, augmenting the individual preferences data.
- Why Meta/Google? Because (1) already have much individual preferences data for targeting (2) can also "optimize" –using behavioral data of many to infer what users may want

Cookie consent

- Origin of “cookie” – Hansel and Gretel leaving cookie crumbs not to get lost in the Dark Forest by knowing their previous locations
- Instead of leaving crumbs in location visited, user keeps records of locations visited as small file(s) on the device so other apps/webs users visit will know where user has been

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
- Even monetization is important for HRDs/independent media
- What to do? – moderation by data protection law → informed consent

Data protection law responds:

- Korea' s PIPC Sept 2022: "Hard for consumers to expect 3rd party websites to be used for marketing"
- Europe: Affirmative cookie consent; 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")

Personal Information Protection Commission Resolution on Meta and Google in 2022

Korea's Personal Information Protection Commission ordered corrective measures and imposed penalty surcharges on Meta and Google (2022. 09. 14.)

Ordered Meta and Google to "notify the users clearly and easily and collect informed consent so that users can exercise free discretion in order to collect and use users' behavior data from other services."

And The commission also imposed surcharges of 69.2 billion Won to Google and 30.8 billion Won to Meta.

What did Google do?

Google did not clearly notify its users about collection and use of third party behavioral information when users join their service.

Hid it under the “more options,” setting the default value to “consent.” Since 2016, Google has shown a "Privacy and Terms" screen in the account creation process, and has indicated that when "users use apps or sites that use Google services(ex. Advertisement, Analytics, YouTube player)", Google also processes "information about the user's activities(ex. Watched Videos, Device ID, IP Address, Cookie data, and Location) ".

What did Meta Do?

Meta’s notification was difficult to access and only vaguely described in its data policy. In the process of creating a Facebook account, there is a mandatory checkbox that says 'I agree to the Facebook Data Policy.' By scrolling on the screen above this checkbox, Facebook provides the full text of the "Data Policy" In the process of creating an Instagram account, there is a screen for "Agreeing to the Terms of Service" where users must select "Data Policy (Required)". By clicking on "Learn More", Instagram provides the full text of the "Instagram Data Policy". In the Data Policy section on 'Information Provided by Partners', Meta states that advertisers (businesses) etc. can provide information to Meta through Meta's business tools (Facebook Login, Pixel, SDK)

Personal Information Protection Commission Resolution on Meta in 2023

In 2023. 02. 08, another penalty to Meta for requiring its users to provide behavioral data from third parties when joining its service.

The Commission stated that customized advertising itself or a platform's behavioral data collection practices are not prohibited, but third-party behavioral data for the basis of identifying users for customized advertising is not the minimum amount of personal information necessary for the service. Thus, in order to collect such data, Meta should have given its users a choice.

Meta's actions of making it impossible for users to sign up or use the services if they refuse to provide third-party behavioral data violates the Personal Information Protection Act.

What is the PIPC Resolution About

The resolution is NOT about prohibiting Targeted Advertising or Collection of Behavioral Data by the Platforms.

However, user identification-based third-party behavioral information for the purpose of Targeted Advertising is **not among the minimum required personal information** for SNS services. Therefore, users must be given the choice regarding its collection.

A corrective order regarding the act of **restricting service subscription/usage** based on the refusal to provide such information.

Data localization

- Different reasons for requiring platform servers to be placed within the country
  - Better surveillance and prevention on cybercrime by domestic authorities
  - Better ability to administer censorship and surveillance on dissidents
  - Taxation
- All the reasons translate into better control by regulators on platforms

--> Independence of platforms threatened

Example

- Russia
- China
- Is GDPR a data localization scheme?

-adequacy decision

#If governments are really concerned about cybercrime investigation, Budapest Convention may be a better deal.

Threats on Horizon: UN Cybercrime Convention

- Duty to criminalize fraud, white hat hacking, and "What Is Criminalized Offline Should Be Criminalized Online Also?"
- The Dangers of a Surveillance Treaty in Absence of a Privacy Treaty
- Surveillance Doubled-up and Unvetted: We Should Have a Right to Have Warrants to Search Us Reviewed by Judges Obligated to Respect Our Privacy

Data retention

- Mandate on platforms to collect and retain data about their users
- Enhances the ability for state surveillance by generating more personal data available for acquisition
- A lot of times, it is identity data that is required to be retained → anonymity threatened
- Violates **data minimization** principle

User/Website registration law

- User registration law struck down in South Korea
- User anonymity → substantive democracy
- How about website registration law?
- Why should speech be registered? Prior censorship? the ghost of periodical registration laws of the colonial times (India, South Korea)
- India (uncertain), Malaysia (social media), Indonesia, Pakistan (VPN only), South Korea, ~~Philippines (almost under Duterte)~~