The right to privacy against surveillance society

- report from Korea -

Byoung-il Oh, Korean Progressive Network Jinbonet

Introduction of Jinbonet

- launched on November 14,1998
- Non-profit ISP for social movement
  - providing internet service such as web-hosting (about 300 sites) , mailing list, blog etc.
  - Social Funch, crowd-funding platform for social movement
- The advocacy of human rights in the information society
  - freedom of expression on the Internet, the right to privacy, Access to Knowledge, Network Neutrality, democratic Internet governance
- Taogi, Youtube channel
- a member of Association for Progressive Communications (APC)

Personal Data Protection in the age of Big Data

Brief history of privacy movement

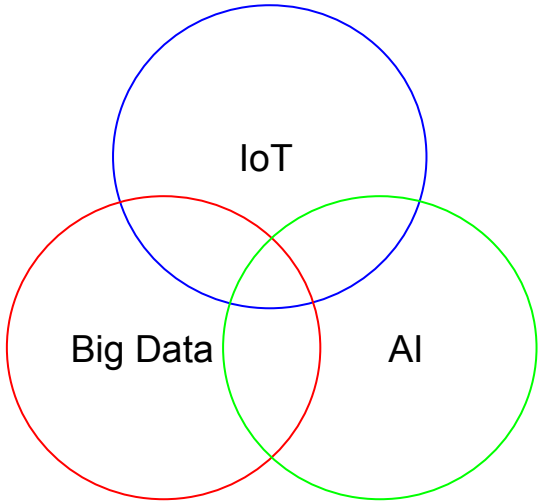
- controversy over E-ID card (1996-1997)
- controversy over National Education Information System (2003)
- Constitution court recognized the right to self-determination of personal information (2005. 5. 26. 99Hunma 513)
- enactment of Personal Information Protection Act(PIPA) (2011)
- the President’s plan to amend the Constitution (2018.3)
    - The provision on the right to self-determination of personal information was created.
    - Everyone has the right to protect and control the processing of information about themselves.

Personal Infomation Protection Regime

- before 2011
  - PIPA in public institution, the Network Act, Credit Information Act etc
- enactment of PIPA in 2011
  - Existing laws including the Network Act and Credit Information act were preserved.
  - establishment of Personal Information Protection Commission(PIPC), but has no enforcement power and not independent of the government.
  - suvervisory authority is distributed to the Ministry of the Interior and Safety(MoIS),Korea Communication Commission(KCC), and Financial Services Commission(FSC).
- revision of PIPA in 2020
  - provisions on personal information in the Network Act are integrated into the PIPA
  - PIPC is elevated to the administrative body, and integrates the supervisory authority of the MoIS and KCC. (but not that of FSC)

Emerging technologies and Personal Information

- creation of personal data without the knowledge of data subject
- massive personal data processing
- secondary use of personal data, such as big data analysis
- various processors are involved
- complexity of personal data processing
- cross-border movement of personal data
- increase of security threat



IMS health case

- collection of prescription data by the Pharmaceutical information center, which provides program to pharmacies.
- after encrypting resident registration number, prescription data were sold to IMS health Korea, without the consent of data subject.
- IMS health analysed the data, produced report and sell it to Korean pharmaceutical companies.
- Civil and Criminal trials in progress
    - Civil court acknowledged the (encrypted) data as personal information

Background of the issue on big data and personal information

- demand of deregulation of personal data in the name of development of big data and AI
- In the Park Keun-hye administration,
  - Ministries jointly published <Personal Data De-identification Guideline> (2016.6)
  - a total of 347,522,005 data between different private companies were combined Combined from August, 2016 to September, 2017.
  - Civic groups filed complaints against government agencies and 20 companies (2017.11)
- In the Moon Jae-in administration,
  - 2018.2. / 2018.4 : The Presidential Committee on the 4th industrial revolution hold a policy hackathon to seek social consensus on data policy.
  - 2018.8.31 : President Moon announced regulation innovation plan for data economy
  - 2018.11.15 : so-called 3 data bills were proposed in the National Assembly
  - 2020.1.9 : 3 data bills (revision of PIPA, Network Act, Credit information Act) were passed.

Issue[1] Concept of Personal Data

- Article 2. 1. "Personal Information" is information about a living individuals, which corresponds to any of the following items:
  - a. information that can identify an individual through name, resident registration number, and image. etc;
  - b. information that cannot identify a certain individual with that information alone, but can be easily combined with other information to identify that individual. In this case, whether other information can be easily combined shall be reasonably assessed by considering the time, cost, technology required for identifying an individual, including the possibility of obtaining other information ; or
  - c. information that cannot identify a certain individual without using and/or combining additional information to restore the information to the original state by pseudonymising the information in item a or item b pursuant to subparagraph 1-2 (hereinafter referred to as the “pseudonymous information”)
- Article.58-2(Exclusion of application) This act shall not apply to information that cannot identify the individual even using other information, when reasonably taking into account ~~all the means such as~~ time, cost, and technology, ~~that data controller can utilize.~~

Concept of Personal Data : GDPR

- Article 4 Definition
  (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- Recital 26: To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the mount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

Issue[2] scope of use out of purpose

- Corporate demand for the utilization and provision of personal data for commercial research purposes such as big data analysis
- reasons for proposed act : “Scientific research that includes industrial purposes such as the development of new technologies, products, and services…”
- Article 2-8. "Scientific research" refers to research that applies scientific methods such as technological development and demonstration, fundamental research, applied research and private investment research.
- Article 28-2(Processing of Pseudonymous Information, etc)
- ① A data controller may process pseudonymous information without the consent of the data subject for statistics, scientif research and archiving in the public interest, etc.
- ② The data controller shall not include information that can be used to identify a specific individual when providing the pseudonymous information to a third party pursuant to paragraph(1)
- Scientific Research : 科學的 研究 vs 學術 研究

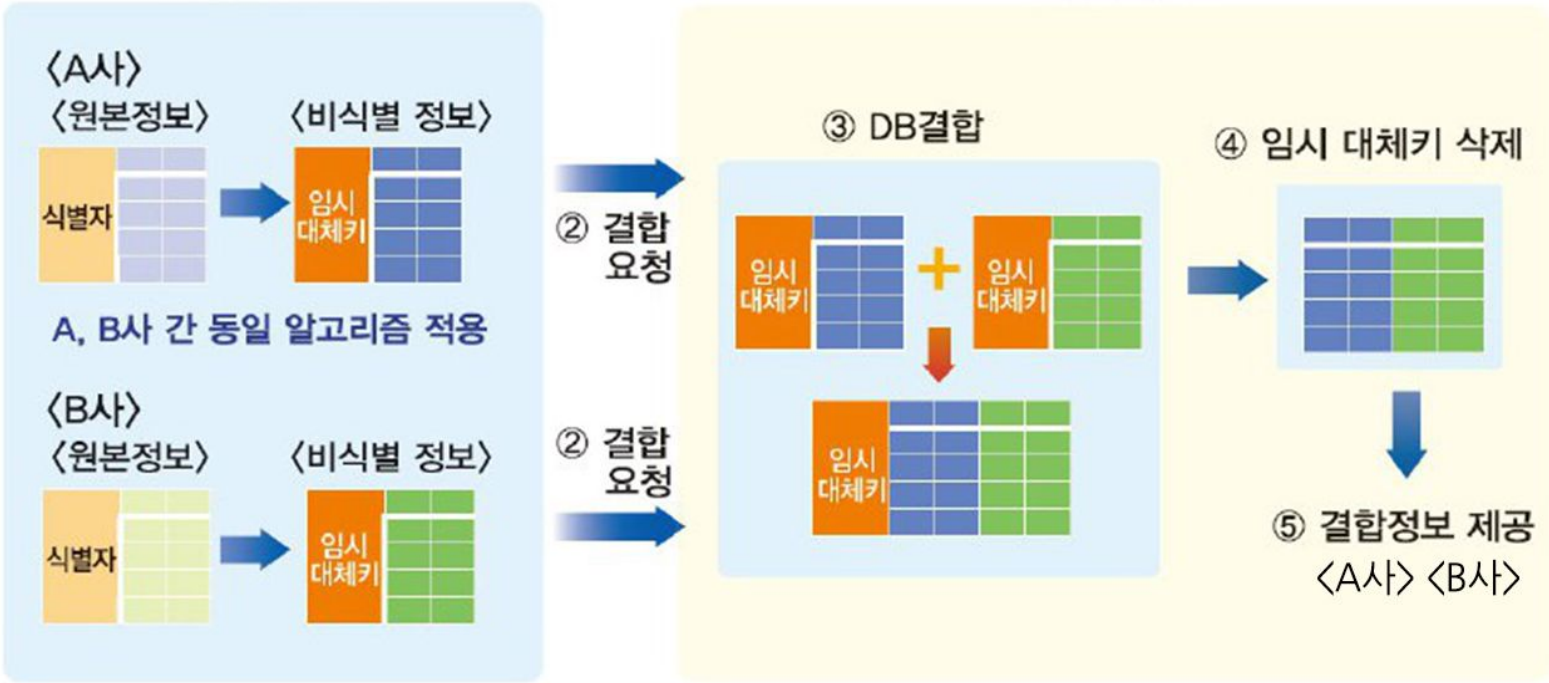
Scope of Scientific Research: GDPR

- Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes. (Article 5)
- GDPR recital 159
  ...the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area.
- TFEU 179(1) : aim to strengthen the scientific and technological base by achieving the European research area in which researchers, scientific knowledge and technology are freely distributed, which means that scientific research is not for commercial research conducted inside corporates, but the result of which can be freely circulated in the research area.

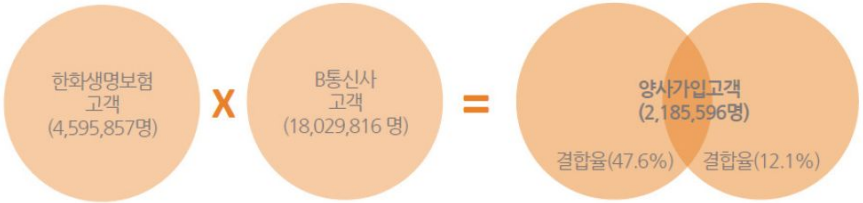
Issue[3] Combination of Data Sets

- Article 28-3(limitation of combination of pseudonymous information) ① Notwithstanding Article 28-2, the combination of data sets between different data controllers for statistics, scientific research and archiving purposes in the public interest, etc. shall be carried out by a specialized institution designated by the PIPC or the head of the central administrative body concerned.
- ② A data controller who wishes to take out the combined data sets outside the institution where the combination took place, it shall process it as pseudonymous information or the information that corresponds to article 25-2 and receive approval from the head of the specialized institution.

De-identification Guideline : combination of data sets



A case of combination of data sets : Hanwha Life Insurance - SK Telecom



한화생명	직업	신용대출건수	최초대출날짜	최초연체날짜	총신용대출금액	총상환금액	신용대출연체율
	최근1년 신용대출연체율	30일이내 신용대출연체율	최초신용등급	최근신용등급	보험료연체율	최근1년 보험료연체율	실효해지건수
	기납입보험료	월납입보험료	직업기반 추정소득금액	가구단위 추정소득금액	평균약관대출율	약관대출금액	자동이체 실패월수
B통신사	나이	성별	사용개월수	멤버쉽등급	월평균통화시간	월평균통화빈도	ARPU
	결합상품가입여부	단말기출고가	이용정지기간	당월 통신료연체금액	최근1년 최대 통신료연체금액	납부방법	회선상태
	남은단말기 할부원금	가입회선수	태블릿PC 보유여부	스마트워치 보유여부	멤버쉽 당월사용금액	멤버쉽 당년사용금액	통신료 미납횟수

준식별자 | 민감정보 | 신용정보

Overseas case on combination of data sets

- There is no separate provision for data combination in the GDPR.
  - Combination of data sets is a form of processing.
  - Each Controller who is involved in the combination shall have legitimate legal basis for the processing.
- In general, personal data by public institutions is provided to scientific researchers.
  - Separation principles : Data controller, linker, researcher is separated strictly.
  - Data Governance : Access to data in the Safe havens, Requirement for research project and researcher, etc.
  - The case of the National Statistical Office in New Zealand

Concern of Civil Society on the PIPA

- Allowance of utilization, provision, and combination of (pseudonymous) personal data for commercial purposes very broadly.

  Risk of infinite sharing of customer data among large enterprises in the every sector of industries including telecommunication, finance, health etc.

- There is no provision on right to object profiling
- Accountability provisions of controllers are not enough, such as
  - Data Protection Impact Assessment (DPIA)
  - Privacy by Design, Privacy by Default

Issue[4] Data Protection Regime

- The data protection provisions of the Network Act are integrated into the PIPA.
- The supervisory authorities of the MoIS and KCC are transferred to the PIPC.
- Credit Information Act and the supervisory authority of the FSC remain.
- PIPC is elevated to the administrative body which has authority over human resources and budget.
- Limitation of independence of the PIPC : Prime minister directs and supervises the PIPC except only some authorities of the PIPC.

State Surveillance and Protection of Communication Secrets

Protection of Communications Secrets Act

- The purpose of the act is to protect communications secrets and freedom
  - regulation of object and procedure of communication investigation by intelligence and investigative agencies
- Concepts
  - communication-restricting measures : wiretapping of contents of communication
  - communication confirmation data : meta-data of communication
    - the date and time of communications, the subscriber number of the other party, location information stored in the base station, log records including IP address etc.
  - communications data : subscriber’s information, which is regulated by the ‘telecommunications business act’

Unconstitutional Decisions on the protection of communications Secrets Act

- Unconstitutional Decision on base station investigation (2018.6.28. 2012 Hun-ma 538)
- Unconstitutional Decision on real-time location tracking (2018.6.28. 2012 Hun-ma 191·550, 2014 Hun-ma 357 combined)
- Unconstitutional Decision on packet monitoring by the National Intelligence Service of Korea (2018.8.30. 2016 Hun-ma 263)
- The act shall be amended until March 31, 2020, the date designated by the Constitutional Court.

Issue[1] Packet Monitoring

- Internet wiretapping : all unencrypted internet traffic is monitored, including internet surfing, e-mail, instant messaging, and shopping etc.
- People who are not suspects, but share an internet line with suspects at home or office are also monitored.
- 99% of all wiretapping cases are conducted by the NIS
  - 2017 : (all) 6,775 cases / NIS 98.77%
  - 2018 : (all) 6,760 cases / NIS 99.38%
- The result of wiretapping has hardly been used as an evidence, which means wiretapping is not used for investigation, but routine monitoring of specific target.

Unconstitutionality Suit on packet monitoring

- The fact that packet monitoring is conducted was first revealed during the trial of an unification movement organization (南北共同宣言實踐連帶)
- In 2011, NIS monitored the internet line of a teacher at his home and office.
- 2011.3.29 a petition to the constitutional court for packet monitoring
- In 2016, the constitutional court declared the end of the judgement because of the death of the teacher.
- 2016.3.29 packet monitoring against a priest. Constitutionality suit was filed again.
- 2018.8.30 The constitutional court ruled unconstitutional against packet monitoring.

packet monitoring : grounds of unconstitutionality

- The information collected through a packet monitoring is vast and comprehensive.
- A legal control system is needed on whether an investigative agency collects information that is unrelated to the purpose of criminal investigation or uses it out of the authorized purpose in the process of wiretapping.
- In the case of a prolonged investigation or suspension of indictment, no notice has been given, and thus a follow-up control over infringement of basic rights doesn't function properly.
- It is possible to abuse the collected data for monitoring purpose as the data is allowed to use to prevent crimes.

How to regulate packet monitoring

- Packet monitoring should be allowed?
- enforcement control
  - Only contents which are relevant to criminal activities should be recorded.
  - The wiretapping records should be sealed and submitted to the court
  - The access right of the target to the wiretapping records
- communication-restricting measures(wiretapping) for National Security
  - (present) conducted under presidential approval for wiretapping of foreigners → should to be amended to be conducted under a court's warrant
- notice to a target :
  - should be noticed to the target right after the termination of the wiretapping.
- control of wiretapping equipments
  - The change, transfer, discard of wiretapping equipments should be under control of the National Assembly.
  - A wiretapping program should be regarded as a kind of equipment, such as RCS hacking program.

Issue[2] Communication Confirmation Data

- condition and procedure to provide communication confirmation data
  - when deems it necessary to conduct any investigation or to execute any punishment
  - ask any telecommunications business entity after obtaining permission from the competent district court
- statistics on the provision of communication confirmation data
  (row : fixed-line telephone / mobile / internet etc / total)

구 분	'16년	'17년		'18년
	하반기	상반기	하반기	상반기
유선전화	31,722	31,831	27,695	**29,716**
이동전화	107,241	106,902	97,622	**99,987**
인터넷 등	18,891	19,867	17,340	**23,774**
합 계	157,854	158,600	142,657	**153,477**

Communication confirmation data : base station investigation

- An investigation method in which all telephone numbers and communication details recorded by a specific base station are provided without specifying a target
- Could be used to identify participants in a rally
- accounted for most of the total number of provision of communication confirmation data
    - For example, the number of warrants for base station investigation in 2015 was 1,394, 0.48 percent of all warrants (300,942) for communication confirmation data, while the number of phone numbers provided by base station investigation reached to 4,970,326, accounting for 90.2 percent of the total number of phone numbers (5,484,945) provided.

Communication confirmation data : base station investigation

- 2011.12 : In investigating the site of the preliminary primary to elect the leader of the main opposition Democratic Party, prosecutors inquired a slew of phone records and personnel information for all callers who went through base stations around the venue.
- 2012.3.20 : A journalist was notified of the fact that the warrant for communication confirmation data had been carried out.
- 2012.6.14 : The journalist raised constitutional suit.
- 2018.6.28 : The constitutional court ruled unconstitutional against base station investigation.

Communication confirmation data : real-time location tracking

- Access to prospective communication confirmation data
- The location of the device is automatically checked every 10 to 30 minutes even in sleeping mode, and the location information recorded in the base station is sent to the mobile phone of the investigator in charge.
- In 2011, the location of the ‘hope bus’ participants and their families to cheer for Kim Jin-sook, who is on a sit-in to protest against layoffs, had been tracked.
- In 2013, the location of mobile phone and access point from which internet sites were accessed, of the head of striking railway workers’ union, members and their families, had been tracked.
- 2018.6.28 : The constitutional court ruled unconstitutional against real-time location tracking.

Communication confirmation data : grounds of unconstitutionality

- Communication confirmation data, especially location information, is not communication contents, but very sensitive information because information about data subject could be inferred from it. It plays almost the same role as the communication content, and is therefore an essential element of freedom of communication.
- It is not properly controlled as only the need for investigation is required to collect communication confirmation data.
- There are other means which infringes fundamental rights less while doesn’t disrupt the investigation, for example by limiting the scope of a crime, or adding supplementary requirements like in the case that criminal investigation is difficult in other ways.
- Therefore, current rule goes against the proportionality principle.

How to regulate the access to communication confirmation data

- Access to communication confirmation data itself should be strictly controlled.
  - The scrope of crime for which access to communication confirmation data could be allowed should be limited to serious crime.
  - strengthening procedural requirement : (present) when deems it necessary to conduct any investigation or to execute any punishment → if there are specific criminal charges, and adding proportionality and supplementary requirements.
  - Stricter conditions are required for base station investigations and real-time location tracking, for example If there is no choice but to use the investigation techniques.
- 2019.12.27 : The National Assembly passed the revision of the act.
  - Supplementary requirements for real-time location tracking and base station investigation are strengthened, but doesn't apply to 'crimes by means of telecommunications'.
  - CSO criticized that control over investigative agencies is not enough.

Issue[3] Communication Data

- Telecommunications Business Act, Article 83, Clause 3
  - Investigators may ask telecommunication service providers to provide personal information such as the subscriber's name, personal identification number, resident registration number and address (without warrant)
  - There is no procedure to notify to the affected persons.
- Statistics of provision of communication data
  - About 10 million communication data are provided annually.
  - Portal sites have refused to provide communications data since the lawsuit against them was filed.
    (row : telecommunication (all) / internet (all) / naver + kakao)

통신 자료 제공	2013년		2014년		2015년		2016 년		2017년	
	문서수	계정수	문서수	계정수	문서수	계정수	문서수	계정수	문서수	계정수
통신 전체	944,927	9,574,659	1,001,013	12,967,456	1,124,874	10,577,079	1,109,614	8,272,504	989,751	6,304,985
인터넷 전체	115,194	392,511	114,260	489,916	100,643	423,533	84,302	312,056	65,151	635,795
네이버+카카오	1	17	0	0	0	0	0	0	0	0

How to regulate access to communication data

- In 2010, the Constitutional Court decided that the provision of communications data is an act at the discretion of a company, which means investigative agency is not responsible for the provision. (2010 Hun-ma 439)
- In 2016, the supreme court ruled that companies are not responsible for damages in providing communication data. (2016.3.10. pronounce 2012Da105482 judgement)
- On May 2016, 500 victims of whom communication data were provided filed once again petition to the Constitutional Court.
- How to regulate access to communication data
    - need to require warrant from the court to access to communication data

Thank you