SNU AI POLICY INITIATIVE

# 차분 프라이버시 (Differential Privacy)의 가능성과 한계

http://ai.re.kr

「데이터 3법 시대의 과제: 가명처리, 연구목적 활용, 데이터 거래」 웨비나

# 차분 프라이버시(Differential Privacy)의 가능성과 한계


**고학수**

서울대학교 법학전문대학원 교수

**구본효**

서울대학교 법학대학원

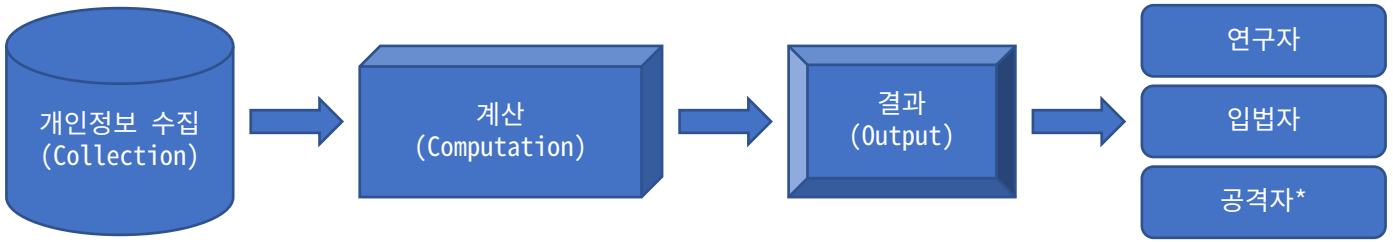
박사과정



SNU AI POLICY INITIATIVE

# 개인정보 보호

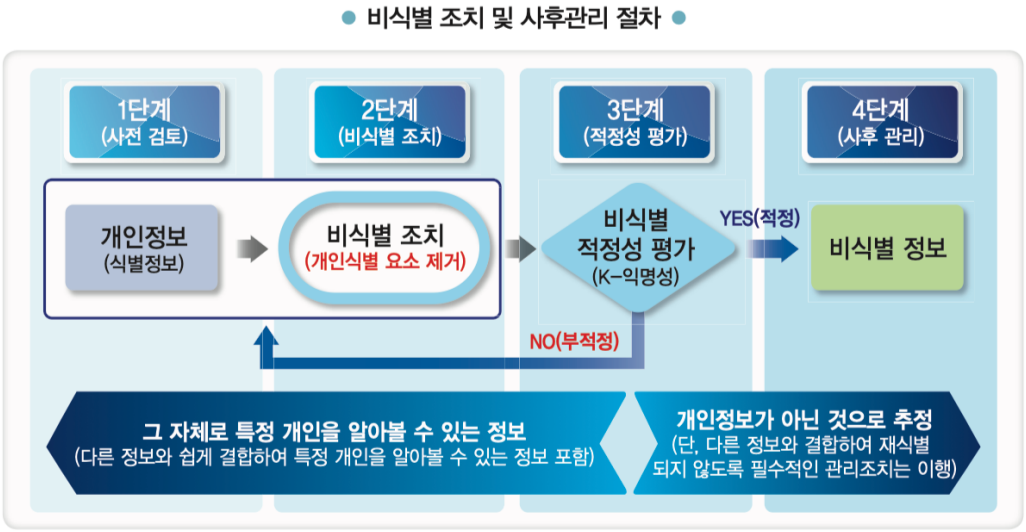
- **상충관계(trade-off)**
  - 개인정보 효용(utility; data accuracy), 정보주체 이익(privacy) 사이 상충관계 존재
  - 해법으로 비식별처리(deidentification)와 익명처리(anonymization) 논의
    - 개인정보, 가명정보, 익명정보 등을 구분하고 위험 수준 판단하여 보호 제공하는 방식




Nissim et al, “Bridging the Gap Between Computer Science and Legal Approaches to Privacy,” Harvard Journal of Law & Technology 31, no. 2 (2018)

# 개인정보 보호

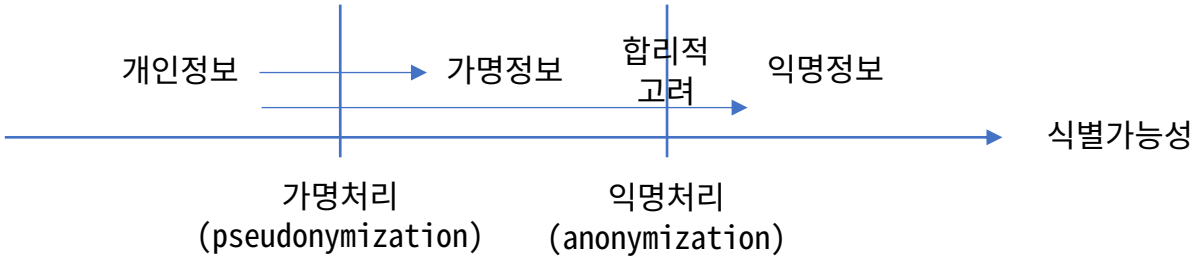
- **상충관계(계속)**
  - 기존 가이드라인은 k-익명성(k-anonymity)을 기준으로 위험 수준 판단
    - 계량 분석 결과, k-익명성의 값이 평가 기준보다 높은 경우 적정으로 판단




개인정보 비식별 조치 가이드라인-비식별 조치 기준 및 지원·관리체계 안내-(2016)

# 개인정보 보호

- **위험**
  - 비식별정보도 재식별(reidentification)이 가능
    - 보조정보(auxiliary information)와의 연결 공격(linkage attack)
      - 사례: Netflix 리뷰, IMDB 리뷰 정보 결합으로 정보주체 식별
    - 개인정보 보호법은 재식별의 위험성을 고려하여 금지의무 등을 규정(제28조의5)
    - 이와 관련하여, 식별가능성(identifiability)이 주요 논의 대상



# 개인정보 보호

- **위험**
  - 식별가능성이 없는 통계 형식으로 정보 제공하는 경우에도 위험 존재
    - 개인정보 재구성(reconstruction)과 정보주체 소속 여부(membership) 확인 가능

| | | AGE | | |
|---|---|---|---|---|
| STATISTIC | GROUP | COUNT | MEDIAN | MEAN |
| 1A | total population | 7 | 30 | 38 |
| 2A | female | 4 | 30 | 33.5 |
| 2B | male | 3 | 30 | 44 |
| 2C | black or African American | 4 | 51 | 48.5 |
| 2D | white | 3 | 24 | 24 |
| 3A | single adults | (D) | (D) | (D) |
| 3B | married adults | 4 | 51 | 54 |
| 4A | black or African American female | 3 | 36 | 36.7 |
| 4B | black or African American male | (D) | (D) | (D) |
| 4C | white male | (D) | (D) | (D) |
| 4D | white female | (D) | (D) | (D) |
| 5A | persons under 5 years | (D) | (D) | (D) |
| 5B | persons under 18 years | (D) | (D) | (D) |
| 5C | persons 64 years or over | (D) | (D) | (D) |

*Note: Married persons must be 15 or over*

| AGE | SEX | RACE | MARITAL STATUS |
|---|---|---|---|
| 8 | F | B | S |
| 18 | M | W | S |
| 24 | F | W | S |
| 30 | M | W | M |
| 36 | F | B | M |
| 66 | F | B | M |
| 84 | M | B | M |

=

| SOLUTION #1 |
|---|
| 8FBS |
| 18MWS |
| 24FWS |
| 30MWM |
| 36FBM |
| 66FBM |
| 84MBM |

Garfinkel et al, “Understanding Database Reconstruction Attacks on Public Data,” *ACM Queue* 16, no. 5 (2018)

# 개인정보 보호

- **평가**
  - 너무 정확하고(“too accurate”) 너무 많은(“too many”) 결과 값을 제공하는 경우 위험 존재
  - 인구조사국(Census Bureau)의 실험
    - 2010년 인구조사 결과 바탕으로 308,745,538명의 개인정보 복원 시도
      - 주소, 성별, 연령, 인종, 민족 등을 46% 이상 정확하게 복원
      - 공개되어 있는 상업 개인정보와의 결합으로 17% 이상 정확하게 복원


Dwork et al, “Robust Traceability from Trace Amounts,” 2015 IEEE 56th Annual Symposium on Foundations of Computer Science. IEEE (2015).

# 차분 프라이버시

- **차분 프라이버시(Differential Privacy)**
  - 사례: Terry Gross의 개인정보 수집 동의 여부와는 상관 없이 개인정보 보호 실패
    - 공격자가 보유하고 있는 보조정보에서 기인(impossibility theorem)
    - 옵트 아웃 상황(opt-out scenario)만큼 개인정보 보호 제공하는 것이 최선
  - 차분 프라이버시는 옵트 아웃 상황보다 조금 덜한(ε) 수준으로 개인정보 보호 제공
    - 개인정보 수집 동의 인센티브 증가(Census Bureau)

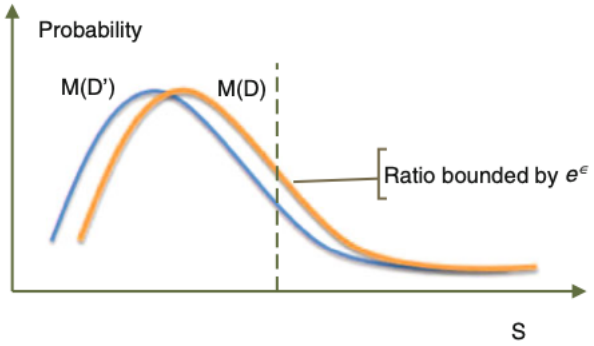
**Terry Gross의 사례**

"Terry Gross는 리투아니아의 여성 평균 신장보다 2인치가 작다."라는 보조정보 있는 경우,
공격자는 리투아니아의 여성 평균 신장 정보만으로도 Terry Gross의 개인정보 취득

Dwork, Cynthia. "Differential Privacy." In Automata, Languages and Programming, edited by Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, 4052:1–12. Berlin, Heidelberg: Springer Berlin Heidelberg, (2006)

# 차분 프라이버시

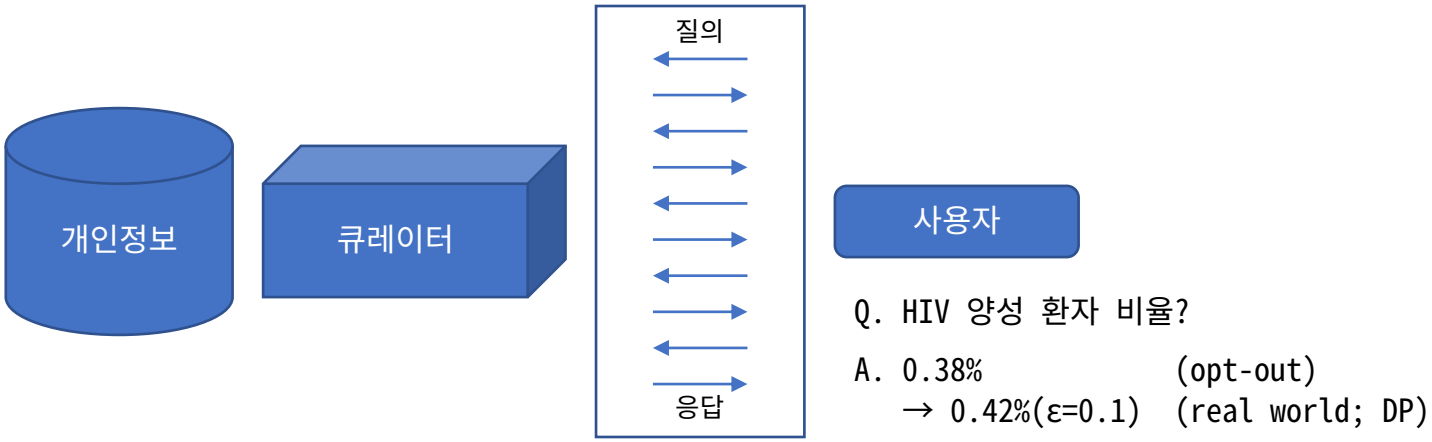
- **차분 프라이버시(계속)**
  - 의미 있는 개인정보 보호 제공(formal, quantifiable measure of privacy)
    - 정의에 의하여 보장되어 있는 개인정보 보호
  - 계속, 반복적인 보호 제공(composition theorem)




Zhu et al, "Preliminary of Differential Privacy," Differential Privacy and Applications, Advances in Information Security, vol 69. Springer, Cham (2017)

# 차분 프라이버시

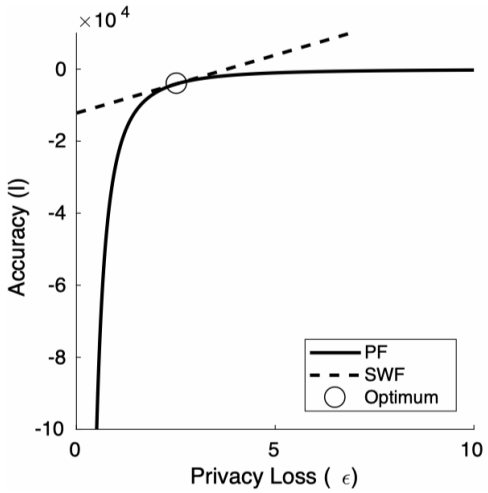
- **방법**
  - 개인정보처리자가 큐레이터(curator)로서 질의응답 체제 제공하는 상황 가정
    - 개인정보처리자는 응답 값을 변조(perturbation)하여 사용자에 제공




Wood et al, "Differential Privacy: A Primer for a Non-Technical Audience," *Vanderbilt Journal of Entertainment & Technology Law* 21, no. 1 (2018).

# 보호 비용

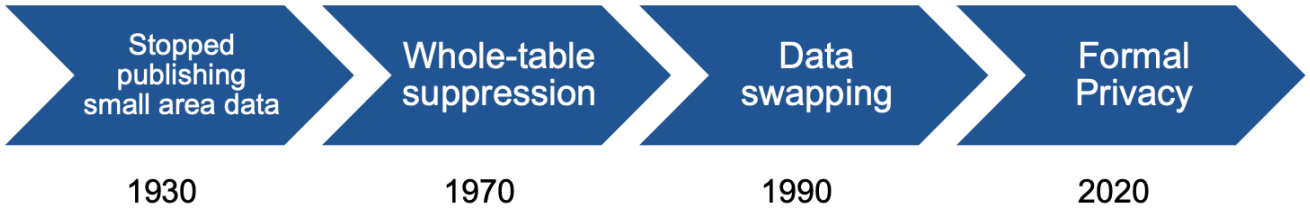
- **보호 비용(ε)**
  - 보호 비용 설정 문제 존재(값이 작을수록 정보주체 이익 보호 가능하나 개인정보 효용 감소)
  - 이는 법경제학에서 논의하는 사회 선택(social choice) 문제




Abowd and Schmutte, "An Economic Analysis of Privacy Protection and Statistical Accuracy as Social Choices," American Economic Review 109.1 (2019)

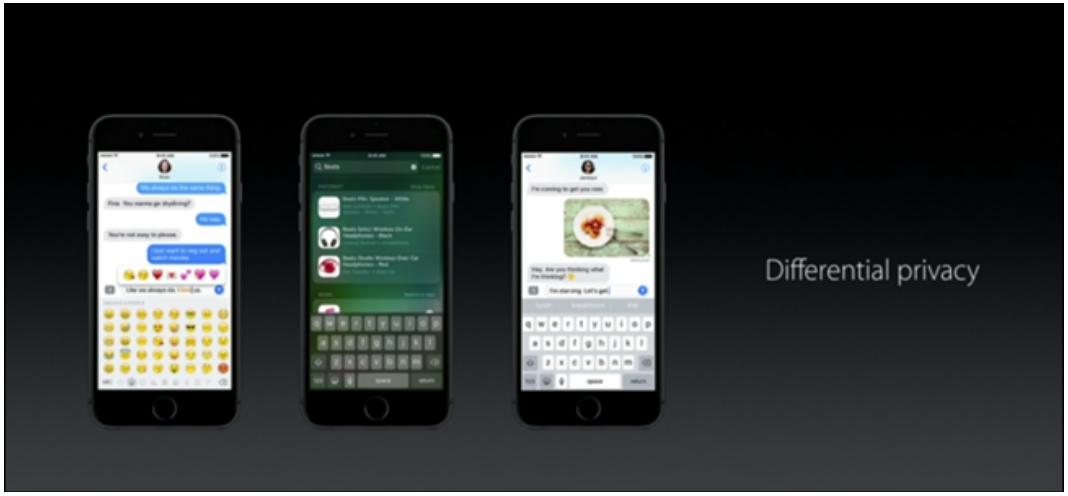
# 사례

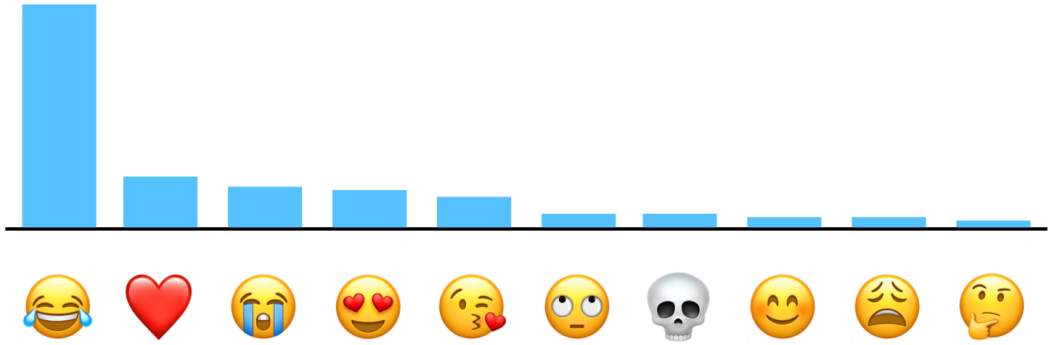
- **기업**
  - 구글, 애플 등은 지역 모형(local model)으로 차분 개인정보 보호 제공
  - 페이스북 등은 중앙 모형(centralized model)으로 차분 개인정보 보호 제공
- **공공기관**
  - 미국 인구조사국은 2020년도 인구조사부터 차분 개인정보 보호(formal privacy) 제공
    - 13 U.S.C. §9(a)(2)




Hawes, “Title 13, Differential Privacy, and the 2020 Decennial Census,” New Mexico SDC Affiliates Meeting and Workshop (2019)

# 사례



# 한계

- **한계**
  - **비용 과다**
    - 인구조사국은 이론(hierarchical mechanisms) 및 구현 방식 연구
    - 초기 단계에는 실력 있는 연구자가 부족하여 운영상의 문제 직면
  - **개인정보 효용 감소**
    - 개인정보 효용 감소 과다하여 대안 필요(Bittau et al, 2017)
    - 사용자의 불만(Ruggles et al, 2019)
      - 개인정보파일 제공 요구
      - 변조되어 부정확한 결과 값으로는 사회 구성원이 기대하는 연구 수행 불가
      - 기존 개인정보 보호 방식(data swapping)으로 규범 준수 가능

# 개인정보 보호법과 관계

- **개인정보 보호법의 주요 내용**
  - 개인정보 보호법은 식별가능정보(identifiable information) 규정
    - 소위 formal, quantifiable measure of privacy 논의 곤란
    - 과학, 법학 사이 가교 필요(Nissim et al, 2018)
  - 가명정보 처리(further processing) 목적 요건으로 통계작성 규정
    - 수량으로 표현되는 정보주체와의 연결성이 없는 총계 정보(aggregate data)
- **개인정보 보호 정보 분석(Privacy Preserving Data Mining)**
  - 개인정보 보호법은 주로 개인정보파일 자체 이용, 제공 등을 고려
  - 개인정보 분석 결과 값을 제공하는 모형과는 상이

# 질의 · 응답

# 감사합니다