초거대 AI 등장에 대응하는 해외 규제 동향

발제 유창하 미국변호사 (법무법인 린)

2023. 3. 25. IHCF 학술분과 세미나

麟 법무법인 린

발표자 소개

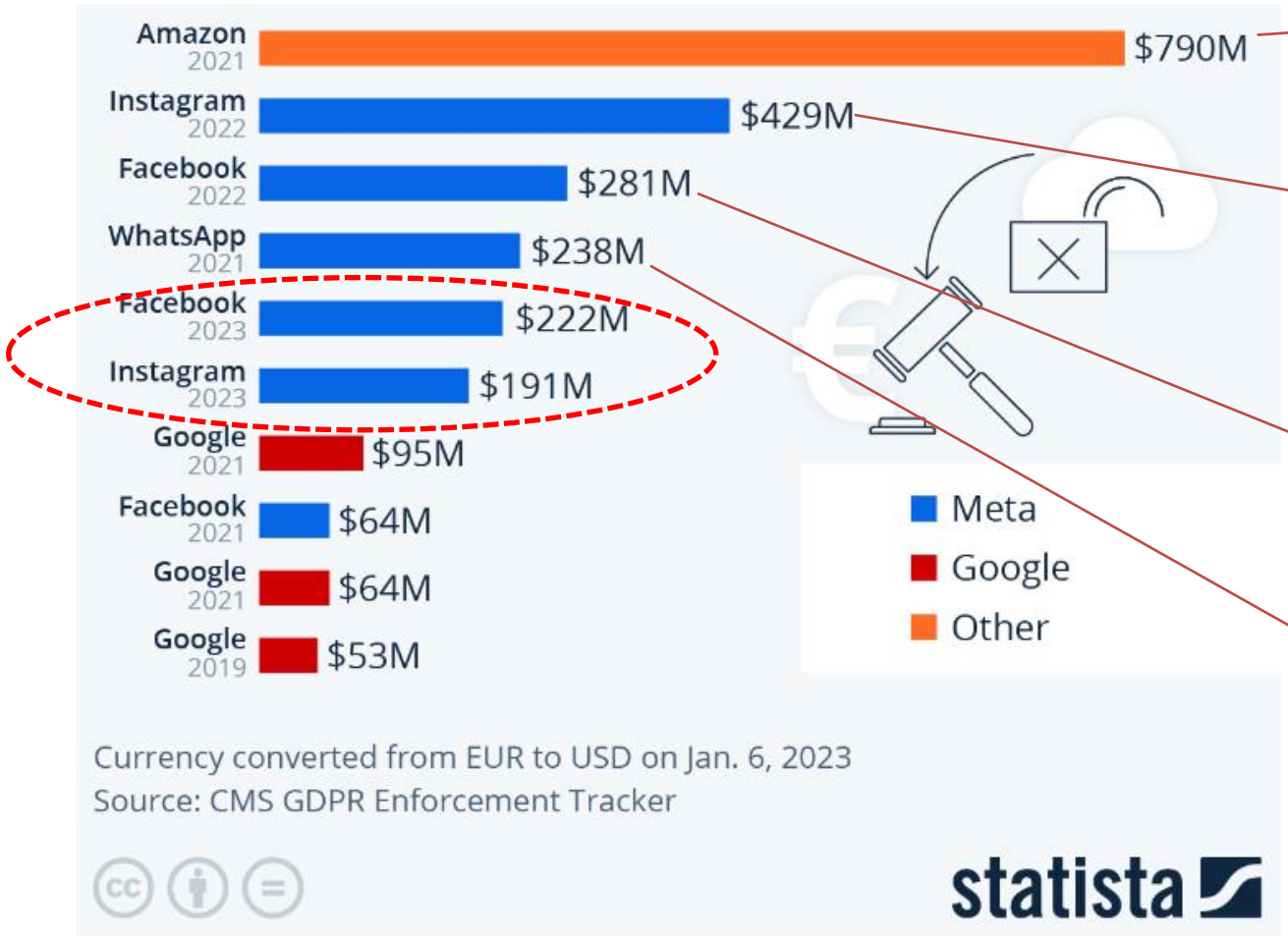
유창하 미국변호사

- 법무법인 린 미국변호사
- 서울지방경찰청사이버수사대 자문위원
- 한국CPO포럼 정회원
- 전) ㈜티몬 법무실장
- 전) ㈜다음커뮤니케이션 법무센터장
- 전) Hudson Advisors Korea 애널리스트
- Georgetown University Law Center. LL.M
- 고려대학교 법과대학 법학과 졸업

Contents

I. New Developments of Data Regulations in the EU & the US

1.Big Tech, Big Fines for breaching GDPR in the EU



Luxembourg's DPA, 2021.7
- 타겟광고 위해 이용자 정보를 남용

Irish DPA, 2022.9
- Articles 6(1), 5(1)(a), 5(1)(c), 12(1), 24, 25(1), 25(2) and 35(1) 위반
- 13-17세 아이들이 인스타그램에서 비지니스 어카운트 운영을 허용하고 경우에 따라 아이들의 전화번호와 이메일 주소를 노출하도록 함
- 이용자 등록 시점에서 아동들의 계정이 디폴트로 공개되도록 설정

Irish DPA, 2022.11
- Article 25 technical and organisational measures 위반
- 페이스북상의 개인정보가 데이터 스크레이핑됨

Irish DPA, 2021.8
- 투명성원칙 위반
- 이용자 정보를 동의없이 다른 페이스북 서비스와 공유

2.Irish DPA decision on Meta

- **Issues**

- GDPR 이 발효(May 25, 2018)되기 직전에 메타는 맞춤형 광고 게재를 한다는 내용으로 페이스북과 인스타그램의 약관을 개정하고 이용자들의 동의를 요구함.

- 맞춤형 광고를 위한 개인정보 처리의 근거를 처음에는 이용자의 동의라고 했다가 계약의 이행(for the performance of a contract)을 위한 것으로 변경

EU 2.Irish DPA decision on Meta

- **Rules: GDPR**

개인정보처리의 법적 근거: (a)동의 (b)계약의 이행 (c)법적 의무 이행 (d) 정보주체 혹은 제3자의 중대한 이익 (e)공공기관 소관사무 수행 (f)콘트롤러 또는 제3자의 정당한 이익

Article 6 Lawfulness of processing

1.Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

EU 2.Irish DPA decision on Meta

- **Decision** — *eur 210mil for Facebook, eur 180mi for Instagram*

- **애당초 Irish DPA**(lead supervisory authority**) 결정**: Meta는 투명성, 공정정 원칙은 위배. 다만, 계약이행을 위한 것이라는 메타 주장은 인정

- **CSAs(Concerned Supervisory Authority)**: 투명성, 공정성 원칙 위배, 계약이행을 위한 것을 근거로 삼는 거 부정. 그 이유는 *맞춤형광고가 페이스북이나 인스타그램 서비스의 필수적 요소라고 보기 어렵기 때문이라는 것.*

- **Irish DPA**: CSAs 결론에 반대

- **EDPB(the European Data Protection Board)**: 맞춤형 광고를 위해 계약 이행을 근거로 삼을 수 없음.

US ADPPA: (1)AFFIRMATIVE EXPRESS CONSENT

- **American Data Privacy and Protection Act(ADPPA)**
  2022년 7월 20일자로 미국 하원 The House Committee on Energy and Commerce를 통과함
- **명시적이고도 명확한 동의의 원칙 천명**
  개인의 자유의사에 따라서 부여된 특정적이고도 애매하지 않은 승인
- **동의 추정 금지의 원칙 천명**

DEFINITION (1) AFFIRMATIVE EXPRESS CONSENT.

- (A) IN GENERAL.—The term "affirmative express consent" means an affirmative act by an individual that clearly communicates the individual's freely given, specific, and unambiguous authorization for an act or practice after having been informed, in response to a specific request from a covered entity that meets the requirements of subparagraph(B).

- (C) EXPRESS CONSENT REQUIRED.—A covered entity may not infer that an individual has provided affirmative express consent to an act or practice from the inaction of the individual or the individual's continued use of a service or product provided by the covered entity.

US ADPPA: (2)COVERED DATA

- **개인정보의 정의를 도입**

다른 정보와 결합하여 합리적으로 특정 개인에게 연결될 수 있는 정보. 합리적으로 특정 개인과 연결될 수 있다면 특정 디바이스에 대한 정보도 이에 해당 가능

- **개인정보의 예외를 명시적으로 열거**

종업원의 정보/ 공개된 정보원으로부터 추론 제외

DEFINITION (8)COVERED DATA

- (A) IN GENERAL —The term "covered data" means information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual, and may include derived data and unique persistent identifiers.
- (B) EXCLUSIONS

(i) de-identified data;

(ii) employee data;

(iii) publicly available information; or

(iv) inferences made exclusively from multiple independent sources of publicly available information that do not reveal sensitive covered data with respect to an individual.

US ADPPA: (3)COVERED ENTITY

- **GDPR의 controller와 유사한 개념 요소 도입**
  개인정보 수집, 처리, 전송의 목적을 결정하는 실체이거나 개인이어야 함
- **영리기관, 비영리 기관 모두 적용 대상**

DEFINITION (9)COVERED ENTITY

(A) IN GENERAL.—The term “covered entity”—

(i) means any entity or any person, other than an individual acting in a non-commercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data and—

(I) is subject to the Federal Trade Commission Act (15 U.S.C. 41 et seq.);

(II) is a common carrier subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all Acts amendatory thereof and supplementary thereto; or

(III) is an organization not organized to carry on business for its own profit or that of its members; and

(ii) includes any entity or person that controls, is controlled by, or is under common control with the covered entity.

US ADPPA: (4)LARGE DATA HOLDER

- 대량 개인정보보유자의 개념을 도입

DEFINITION (2) LARGE DATA HOLDER

(A) IN GENERAL.—The term “large data holder” means a covered entity or service provider that, in the most recent calendar year—

(i) had annual gross revenues of $250,000,000 or more; and

(ii) collected, processed, or transferred—

(I) the covered data of more than 5,000,000 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals, excluding covered data collected and processed solely for the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested product or service; and

(II) the sensitive covered data of more than 200,000 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals.

US ADPPA: (5)ENFORCEMENT

- **원칙적 법 집행권한:** 각 주의 법무부장관(attorney general) & 미국 연방거래위원회(the Federal Trade Commission)
- **개인들의 소송 권한:** 집단소송을 비롯하여 개인정보처리자에 대해 직접 민사소송 제기 가능. 다만 소송을 제기하기 위해서는 해당 개인정보처리자에게 45일의 치유기간을 먼저 부여해야 함
- **과징금은 The Federal Trade Commission Act에 의하도록 함**
- **형사처벌 조항은 별도 없음**

II. AI Regulations in the EU & the US

EU 1.The Artificial Intelligence Act

- **2021. 4 European Commission이 제안**

  산업의 활성화와 이용자 보호의 조화를 꾀함

- **Risk-based Approach: Minimal Risk/ Limited Risk/ High Risk/ Unacceptable Risk**

  -Limited Risk AI에 해당할 경우, 자율적으로 영향평가를 수행하면 상품화 가능

- **규제 위반시 전세계 매출액의 6%를 과징금 부과**

EU 1.The Artificial Intelligence Act

- **High Risk :** the European Artificial Intelligence Board (EAIB)가 정하는 별도의 인증절차를 사전에 통과해야 비로소 상품화할 수 있음.

-Critical infrastructures (e.g. transport), that could put the life and health of citizens at risk

-Educational or vocational training, that may determine the access to education and professional course of someone's life (e.g. scoring of exams)

-Safety components of products (e.g. AI application in robot-assisted surgery)

- Employment, workers management and access to self-employment (e.g. CV sorting software for recruitment procedures)

-Essential private and public services (e.g. credit scoring denying citizens opportunity to obtain a loan)

- Law enforcement that may interfere with people's fundamental rights (e.g. evaluation of the reliability of evidence)

- Migration, asylum and border control management (e.g. verification of authenticity of travel documents)

- Administration of justice and democratic processes (e.g. applying the law to a concrete set of facts)

- Surveillance systems (e.g. biometric monitoring for law enforcement, facial recognition systems)

EU 1.The Artificial Intelligence Act

- **Unacceptable Risk**

-subliminal distortion of a person's behavior

-exploiting vulnerabilities of specific groups of people

-Evaluating or classifying the trustworthiness of natural persons based on their social behaviour or known or predicted personal or personality characteristics

EU 2.How to deal with Generative AI?

- AI Act가 제안된 시점인 2021년에는 generative AI의 출현을 예상하지 못하였음
- 최근, AI Act 제정 작업의 핵심 역할을 한 유럽의회 의원인 Dragos Tudorache와 Brando Benifei는 generative AI를 high-risk로 분류해서 관리해야 한다는 입장을 밝힘
- 이에 대하여 generative AI를 일괄적으로 high-risk로 분류해서 규제 비용을 증가시키는 것은 합리적이지 못하다는 비판의 목소리도 있음
- AI Act 최종안에 대해서, EU Commission, Council of EU, EU Parliament가 협의를 진행할 예정인데, generative AI를 최종법안에 어떻게 반영할 것인가가 핵심적인 쟁점이 될 전망

US 1.AI Risk Management Framework: (1)catalogue of characteristic

By the National Institute for Standards and Technology (NIST)

AI가 갖춰야 하는 특성들을 제시

- **Valid & Reliable**: AI is accurate, able to perform as required over time, and robust under changing conditions.
- **Safe**: AI does not cause physical or psychological harm, or endanger human life, health, or property.
- **Fair & Nonbiased**: Bias in results is managed at the systemic, computational, and human levels.
- **Explainable & Interpretable**: The AI's operations can be represented in simplified format to others, and outputs from AI can be meaningfully interpreted in their intended context.
- **Transparent & Accountable**: Appropriate information about AI is available to individuals, and actors responsible for AI risks and outcomes can be held accountable.

US 1.AI Risk Management Framework: (2)action framework

By the National Institute for Standards and Technology (NIST)

기업들이 AI risk를 관리하는 방법을 제시

- **"Map"** refers to the planning stage for AI – e.g., mapping the intended purpose of AI and its likely context of use – to identify likely risks and build AI to address risk while achieving intended functionality.
- **"Measure"** occurs during the development stage, when AI is built. It comprises identifying methods for building AI and metrics for measuring its performance – including metrics for evaluating AI's trustworthy characteristics.
- **"Manage"** refers to risk management after AI has been deployed. It includes monitoring whether AI is performing as expected, documenting risks identified through AI use, and developing responses to identified risks.

US 2.How to deal with Generative AI

- 미국은 연방 개인정보보호법인 ADPPA도 의회를 통과한 상황은 아니고, EU와 같이 AI를 직접 규율하는 법도 없는 만큼, generative AI를 어떻게 규율할 것인지에 대해서는 기초적인 논의 단계임

- Doe vs. Github, November 2022

  -두 명의 개발자가 Microsoft, GitHub, OpenAI를 대상으로 소송을 제기.

  -원고들의 주장은 이들 회사가 Copilot 프로그램을 훈련시키는 과정에서, open-source licensing 조항을 위반하여 자신들의 컴퓨터 코드를 불법적을 사용하였다는 것.

- Getty Images vs. Stability AI, January 2023(영국), February 2023(미국)

  - Getty Images가 Stability AI를 대상으로 소송을 제기

  - Stability AI가 이미지 생성 AI인 Stable Diffusion을 훈련시키는 과정에서 Getty Images의 저작물을 복제하거나 2차적 저작물을 만들어 냈다는 것. 또한 이 과정에서 저작권 침해 은폐 등을 목적으로 저작권관리 정보를 허위로 제공하거나 이를 제거 변경하였다는 것.

III. Major Implications

Major Implications

- **빅테크 기업에 대한 이용자 정보 남용 규제 강화**

  - 맞춤형 광고에 대한 동의 여부는 지속적 쟁점으로 다뤄지고 서비스의 필수적이고도 본질적인 부분을 구성하느냐에 대해 논쟁이 이어질 것으로 보이는 바, 이러한 논쟁은 generative AI시대에서도 지속적으로 강화될 것으로 보임.

  - 데이터 이용과 관련하여서 정보주체의 명시적이고도 명확한 동의 원칙이 강화될 것으로 보임.

- **EU의 risk-based approach와 Generative AI**

-본 법안이 제안된 2021년은 Gemerative AI가 고려되지 않았음.

- Chat GPT가 향후 수행하는 업무가 high risk 내지 unacceptable risk에 해당할 가능성이 높음

-규제 이행을 위한 비용이 크게 발생할 수 있고, 이로 인하여 대기업과 중소기업간 격차가 더 커질 수 있음

- **미국의 ADPPA와 Generative AI**

-ADPPA가 발효될 경우, 미국의 generative AI 사업은 강한 데이터 규제에 직면할 수 있고, 집단 소송의 가능성도 큼. 특히, 명확한 동의 원칙이 AI환경 특히 Generative AI에도 적용을 해야 할 것인가에 대하여 논란의 소지가 클 것으로 보여짐.

-저작권 침해 중심으로 진행 중인 소송의 결과도 향후 미국의 generative AI 산업 방향에 큰 영향을 미칠 것으로 보임

Thank You

麟 법무법인 린