인공지능(AI)과 프라이버시의 역설:
AI 서비스[스피커 및 음성비서]와 프라이버시를 중심으로

2019. 9. 18.
KISDI, 방송미디어연구실
심홍진 연구위원

□ 연구 배경

인공지능(AI) 서비스의 보편화에 따른 프라이버시 침해 가능성 증대

- AI 스피커나 AI 음성비서(assistant) 등의 인공지능 서비스는 우리에게 다양한 혜택과 최적화된 편리함을 제공하며 우리 생활의 필수 기기로 자리잡음
- 그러나 AI 서비스 발전은 이용자 데이터의 수집 및 활용이 불가피함에 따라 개인의 프라이버시 침해 및 사적영역의 붕괴 위협을 수반

□ 연구 목적

◆ AI 서비스 고유의 특성을 반영한 프라이버시 관련 개념을 규정하고, AI 서비스 발전 및 환경 변화를 고려한 정책적 시사점 제언

□ 주요 내용 및 시사점

◆ 인공지능에 기인한 경제·사회적 풍요 이면에 존재하는 프라이버시 역설

- AI 서비스(스피커 및 음성비서) 이용자가 보다 향상된 이용경험과 니즈를 요구할수록 이용자의 요구를 충족시키기 위한 제조사의 미필적 개인정보 이용 가능성 존재
- 이용자와의 원활한 상호작용을 위한 AI 서비스의 상시 대기상태는 이용자의 프라이버시 또한 상시로 침해 받을 수 있는 “프라이버시 로깅 (privacy logging)” 환경을 생성함
- 특히 AI 서비스부터 획득한 민감한 개인정보의 활용 정도, 수집된 정보에 대한 접근성 수준, 허용 범위 등의 모호한 기준으로 프라이버시의 경계가 흐릿해지면서 프라이버시 침해와 보안위협 가중
- AI 서비스와 연결되어 있는 금융, 쇼핑 등 생활 편의시스템이 확대됨에 따

라 프라이버시 관련 법제도를 비롯해 AI 서비스 관련 시스템의 보안 등 유관 법제도 및 정책 마련 시급

프라이버시 로깅(Privacy-logging)과 프라이버시 불감증(Privacy insensitivity)

o AI의 기술발전은 개인에게 다양한 편익을 제공하는 반면, 사용자가 의식하지 못한 순간(Unconsciously) 자신의 프라이버시가 끊김없이(Seamless) 지속적으로(Consistently) 디바이스에 기록(Logging), 저장될 수 있음

- 프라이버시 로깅으로 인해 AI 서비스 이용자는 서비스를 이용하면서 디바이스가 제공하는 단순한 편익을 위해 자신의 은밀하고 사적인 개인 정보를 부지불식간에 디바이스에 제공할 수 있음
- 게다가 AI 서비스가 인간화(humanization)를 지향할수록 개인정보 제공에 대한 이용자의 저항감이 감소할 수 있으며, 이용자는 자신의 개인정보 공개를 의식하지 못한 채 지속할 수 있고, 이는 프라이버시 노출에 무감해지는 프라이버시 불감증으로 심화될 수 있음

  ※ SK 텔레콤 '초시대 AI 생활' "아리야, 자동차 온도 23도로 시동 걸어줘! 왜? 낯설어서~곧 익숙해지겠지~!"
- 최근 AI 음성비서가 스마트홈 기기 등 다른 디바이스를 중계하는 인터페이스 역할을 하면서 개인정보를 다양한 디바이스로부터 동시 다발적으로 끊김없이 수집하는 프라이버시 로깅 플랫폼 등장 가능

◆ 상충관계(trade-off relationship)의 기울어진 운동장

o AI 서비스가 제공하는 편익의 대가로 디바이스 제조업체에게 이용자의 개인정보를 일정부분 제공할 수밖에 없는 상충관계 발생은 필연적, 그러나 제공받는 편익에 비해 과도한 개인정보 제공이라는 상충관계의 구조화된 비대칭이 발생할 수 있음

- AI 서비스 사용을 위해 이용자는 미디어 이용행태, 상품 구매 방식, 라이프스타일 등 이용자의 프라이버시를 과도하게 드러내야 하는 상충관계의 불균형을 야기할 수 있음
- AI 이용자의 니즈(needs)가 증가하고 더 나은 이용자 인터페이스와 이용자 경험이 요구될수록, 제조사는 더 많은 개인정보를 요구하고, 이는 상충관계 불균형이 고착화되는 요인

- AI 서비스에 대한 이용자의 니즈와 AI 서비스의 인간화(Humanization) 정도, 즉 휴머노이드 로봇화(humanoid Robot)가 본격화할수록 비대칭적 상충관계(Asymmetric trade-off relationship)의 강도 증가

ATR = NFAI * DOH
비대칭 상충관계의 강도(ATR): Asymmetric trade-off relationship 이용자의 AI 니즈(NFAI): Needs for AI 인간화 정도(DOH): Degree of humanization

- 무의식적 프라이버시 로깅을 유발하는 AI 기술 발전 속도를 프라이버시 예방 및 보호를 위한 정책 대응 속도가 따라잡을 수 없는 현실이 지속될 우려

IoT 환경의 일반화에 따른 프라이버시 로깅 확대 및 신규 위협요소

o IoT 환경은 인간과 AI 서비스 간의 대응 관계를 인간과 AI 음성비서가 통제하는 여러 사물인터넷 기기의 관계로 확대시킴으로써 프라이버시 로깅의 범위를 확대, 구축하고 개인정보 침해 위협요소의 외연을 확장

- AI 서비스와 여타 사물인터넷 기기가 정보를 주고받음으로써 인간과 AI 개체의 1:1 대응이 인간과 AI 군집간 대응, 즉 1:多 대응으로 확장될 수 있으며, 이는 디바이스 구분 없는 다차원적 프라이버시 로깅으로 전환될 수 있음
- 여기에 이용자의 미디어 이용행태까지 파악할 수 있는 행태정보를 AI가 군집단위로 수집할 수 있어 이용자의 생활 습관, 성격, 미디어 이용 행위 패턴을 분석하고 프로파일링(네이버, 2014[1])할 수 있는 신유형 프라이버시 로깅 등장할 우려
- 따라서 AI 서비스와 사물인터넷 기기간의 무차별적 연결보다는 연결로 인해 발생할 상충관계의 비대칭을 고려한 이용자, 디바이스 제조업자, 규제기관의 긴밀한 협업에 바탕을 둔 제도적 정비 필요

1) 출처: NAVER 프라이버시 센터, https://privacy.naver.com/main?menu=home