「 '4차 산업혁명'과 정보인권 」 연속토론회

사물인터넷 환경에서의 개인정보보호와 보안

일 시 | 2017년 8월 31일(목) 오후 2시~4시

장 소 | 국회의원회관 제1세미나실

주 최 |

국회 과학기술정보방송통신위원회
변재일 의원 (더불어민주당, 충북 청주시청원구)
김성수 의원 (더불어민주당, 비례대표)
추혜선 의원 (정의당, 비례대표)
국회 행정안전위원회
진선미 의원 (더불어민주당, 서울 강동구갑)
권은희 의원 (국민의당, 광주 광산구을)
이재정 의원 (더불어민주당, 비례대표)
언론개혁시민연대, 정보인권연구소, 진보네트워크센터, 참여연대, 한국소비자단체협의회, 함께하는시민행동

후 원 | 국가인권위원회

순 서

2:00 ~ 2:05	개회	
2:05 ~ 2:15	인사말	
	사회	조순열	경실련 시민권익센터 운영위원
2:15 ~ 2:45	발제	오병일	정보인권연구소 이사
2:45 ~ 3:45	토론	강장묵	고려대학교 연구교수
		권석철	큐브피아 대표
		박준우	함께하는시민행동 사무처장
		좌혜선	한국소비자단체협의회 사무국장
		김호성	한국인터넷진흥원 개인정보기술단장
3:45 ~ 4:00	전체토론	

추혜선 | 정의당 국회의원

안녕하세요, 정의당 국회의원 추혜선입니다.

먼저 다섯 차례에 걸친 ‘4차 산업혁명과 정보인권’ 연속토론회를 함께 주최해 주신 진보네트워크센터, 언론개혁시민연대, 정보인권연구소, 참여연대, 한국소비자단체협의회, 함께하는시민행동 관계자 여러분과 변재일·김성수·이재정·진선미·권은희 의원님, 그리고 토론회 준비를 위해 고생하신 모든 관계자 여러분께 감사의 말씀을 드립니다. 또한 토론회를 후원해 주신 국가인권위원회에도 감사드립니다.

발전하는 기술이 주는 놀라운 혜택은 기업에게는 미개척의 시장을, 국민들의 삶에는 편의와 풍요를 더해 주고 있습니다. 그 중 '사물인터넷' 기술은 인류의 가사노동 부담을 덜고, 교통사고 등 물리적 위험에서 보호하고, 특정 개인의 행동패턴을 인식해 맞춤형 서비스를 제공하는 등 국민들의 실생활과 가장 밀접한 공간으로 접근하고 있습니다.

하지만 물리적 노동과 위험을 줄인 대신 새로운 위험이 우리에게 다가오고 있습니다. IoT 기기의 보안 취약점을 이용한 사생활 침해 사례가 세계 곳곳에서 발생하기 시작했습니다. 특히 IoT기기를 통해 수집 가능한 건강정보, 금융정보, 위치정보 등, 유출될 경우 특정 개인에게 심대한 사회경제적 불이익을 안길 수 있는 개인정보의 보호에 대한 경고의 목소리가 높아지고 있습니다.

다양한 분야의 기술이 다양한 형태로 응용·융합되는 상황에서 정보인권 보호의 기본 원칙이 흔들리게 된다면, 규제의 속도가 산업발전의 흐름을 따라잡지 못하여 그 피해는 소비자인 국민들이 고스란히 떠안게 될 것입니다.

오늘의 토론회를 통해 국민의 안전과 편익을 동시에 지켜내는 지혜로운 해법들이 제시되기를 바랍니다.

다시 한 번 함께하신 모든 분들께 감사드립니다.

고맙습니다.

사물인터넷 환경에서의 개인정보 보호와 보안

오병일 | 정보인권연구소 이사

사물인터넷(Intenet of Things)의 정의

- 사물인터넷(IoT)의 개념은 통상의 일상적인 기기-다른 물건이나 개인과 연결된 것들, 혹은 "사물" 그 자체-에 내장된 수십억 개의 센서가 데이터를 기록, 처리, 저장, 전송하도록 고안되고, 고유한 식별자와 연계되어, 네트워크 기능을 가진 다른 기기나 시스템과 상호작용하는 인프라를 의미한다. (WP29, 2014)
- 사물인터넷은 일상의 사물들이 인터넷에 연결되어 데이터를 주고 받는 능력을 지칭한다. (FTC, 2015)
- 사람, 사물, 데이터 등 모든 것이 인터넷으로 서로 연결되어, 정보가 생성, 수집, 공유, 활용되는 기술, 서비스를 통칭하는 개념. (미래창조과학부, 2014)

사물인터넷 현황

- 전 세계 인터넷 연결 사물 수: ('13) 26억개→('20) 260억개 (Gartner, 2013)
- 세계 사물인터넷 시장은 2013년 2천억 달러 규모에서 2020년 1조 달러로 성장 (연평균 약 26%)할 것으로 전망(Machina Research, 2013),
- 국내 사물인터넷 시장은 2013년 2.3조원으로 세계시장 대비 1% 남짓에 불과

(미래창조과학부, 2014)

IoT가 약속하는

행복한 세상

미래창조과학부(2014)

국내 사물인터넷 기본계획 (정부부처 합동, 2014)

- 비전 : 초연결 디지털 혁명의 선도국가 실현
- 추진전략 :
  - 1. 생태계(SPNDSe) 참여자 간 협업 강화
  - 2. 오픈 이노베이션 추진
  - 3. 글로벌 시장을 겨냥한 서비스 개발.확산
  - 4. 대.중소기업.스타트업별 맞춤형 전략
- 주요 추진과제
  - 1. 창의적 IoT 서비스 시장 창출 및 확산
    - 유망 IoT 플랫폼 개발 및 서비스 확산 / ICBM 新융합서비스 발굴.확산 / 이용자 중심의 창의적 서비스 발굴
  - 2. 글로벌 IoT 전문기업 육성
    - 개방형 글로벌 파트너십 추진 / 스마트 디바이스 산업 육성 / 스마트 센서 산업 육성 / 전통산업과 SW신산업 동반성장 지원 / 생애 전주기 종합지원
  - 3. 안전하고 역동적인 IoT 발전 인프라 조성
    - 정보보호 인프라 강화 / 유무선 인프라 확충 / 핵심기술 개발, 인력양성 / 규제없는 산업환경 조성

사물인터넷과 개인정보

- 사물인터넷은 이용자의 주변 환경 관련 데이터를 측정하거나, 이용자 개인(신체, 행동 등)의 데이터를 수집, 분석하고 이 데이터의 수집 및 조합을 통해 애플리케이션이나 서비스를 제공.
- 개인을 식별하거나 식별할 수 있는 데이터를 수집한다는 점에서, 이 데이터는 개인정보로 간주됨.
- 개인정보보호법 제2조
  - "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

사물인터넷 관련 법제

- 개인정보 보호 관련 법제
  - 개인정보보호법, 정보통신망법, 위치정보보호법 등
- 보안 관련 법제
  - 정보통신망법, 정보통신기반보호법 등
- 영역별 개별 법률
  - 헬스케어 : 의료법
  - 자율주행자동차 : 자동차관리법 등

자율주행자동차의 사례

- 자율주행자동차(혹은 Connected Car)에서 수집되는 정보
  - 자율주행을 위해 필요한 차량 관련 정보
    - 현대자동차 블루링크(BlueLink)의 사례 (출처 : 김범수 외(2014))
  - 운전자에 대한 모니터링 정보
  - 차량 내 엔터테인먼트 등 서비스를 위한 정보

관리 영역		정보
디바이스		• H: 위치정보 • M: 주행일자, 주행거리, 운행시간 • L: 평균속도, 최고속도, 공회전시간, 주행가감속 분포, 차속구간 분포, 배터리전압/냉각수온도/자동변속기 오일 온도/엔진오일 온도 이상시간, 고장 코드, 누적 주행거리, 소모품 교환(점검) 정보
네트워크	Wi-Fi	• SSID(Service Set Identifier), 단말기 정보(모델, 일련번호, IMEI번호, USIM 번호, 구매년월일, MAC 정보)
	블루투스	• SpecificationID, VendorID, ProductID, Version PrimaryRecord, VendorRecord, VendorIDSource
	3G/4G	• MEID(Mobile Equipment Identifier), ESN(Electric Serial Number), MSIN(Mobile Subscriber Identifier Number)
플랫폼/서비스		• H: 성명(법인명), 주민(법인)등록번호, 사업자등록번호 주소, 전화번호, 이메일, 긴급연락처, 계좌/카드번호, 청구주소 • M: 차대번호, 차량번호, 보험사, 보험만기일, 차량계약번호 • L: 차량 모델

자율주행자동차의 사례

- 미국 도로교통안전국(NHTSA) Federal Automated Vehicles Policy (2016.9)
  - 일반도로에서 운행될 자율주행자동차의 성능 가이드라인을 규정. 15개 항목으로 구성.
- 유럽
  - 비엔나 협약에서 "운전자가 항상 차량을 제어하고 있어야 한다"라는 규정에 의해 자율주행 기술개발 및 시험평가에 제한을 받았으나, 자율주행 사용화를 위하여 해당 협약 개정.
- 한국
  - 자율주행자동차 정의와 시험, 연구 목적으로 운행하기 위한 자동차관리법 개정
  - 자동차의 구조 및 기능, 탑승인원 및 방법, 보험가입, 사전시험주행 등 다양한 요건을 충족을 위해 <자율주행자동차의 안전운행요건 및 시험운행 등에 관한 규정>마련
  - 주변 차량과의 정보 교환을 위한 위치정보법 개정안 계류 중 : 소유자의 사전동의 없이도 사물위치정보를 처리할 수 있도록 규정

자율주행자동차의 사례

➢ Vehicle Performance Guidance

법령	내용
데이터 기록과 공유(Data Recoding and Sharing)	자율주행 시 생산 및 활용되는 데이터는 주행 상태, 교통사고 상황, 시스템 오류 등을 확인할 수 있는 주요 정보의 민감 관련 데이터를 충실히 기록하고 공유하여 폭넓게 활용할 수 있어야 함
사생활 보호(Privacy)	자율주행 중 어떤 데이터가 수집·저장되는지 운전자가 알 수 있어야 하고, 자동차 이용자는 개인 생체 정보나 행태와 같은 개인정보의 수집을 거부할 수 있어야 함
시스템 안전(System Safety)	시스템 오작동이나 교통사고 등의 경우, 안전하게 대응할 수 있어야 하고, 자동차의 안전시스템은 객관적인 외부 검증을 거쳐야 하고, 기술적 문제가 있더라도 안전하게 작동할 수 있음이 증명되어야 함
사이버 보안(Vehicle Cyber-security)	사이버 공격을 방어할 수 있는 보안시스템을 갖추어야 하며, 제조사는 보안 관련 프로그램과 평가 내용을 기록해야 하고, 이 정보는 동일 산업 분야 내에서 공유되어야 함
인간-기계 인터페이스 (Human-Machine Interface)	자율주행과 인간 조종 모드의 원활한 전환이 가능해야 하고, 운전자는 자율주행이 어려운 상황을 쉽게 인지할 수 있어야 함. 자율주행 중에 자동차가 보행자나 타 차량, 혹은 도로시설과도 통신(소통)할 수 있어야 함
충돌 성능(Crash-worthiness)	자율주행자는 일반 자동차와 동일한 안전기준을 만족시키는 구조와 장치를 갖추어야 하고, 도로교통안전청(NHTSA)의 자동차 안전기준을 충족해야 하고, 사고 시 승객을 충분히 보호할 수 있음을 증명해야 함
소비자 교육과 훈련 (Consumer Education and Training)	제조사는 판매자(딜러) 등에게 자율주행의 작동 원리를 설명할 수 있도록 관련 직원을 교육하여야 하고, 제조사와 판매자는 소비자에게 자율주행차의 기능과 한계, 긴급상황 대처 요령 등을 충분히 설명해야 함
등록 및 인증 (Registration and Certification)	자율주행 관련 모든 소프트웨어의 업데이트 내용이나 새로운 무인주행 기능을 도로교통안전청(NHTSA)에 보고해야 함

출처 : 박준환(2016)

사고 후 대처 (Post-Crash Behavior)	자율주행차가 충돌 후 다시 운행될 때, 제조사는 차량의 안전함을 미리 증명해야 함. 즉, 손상된 센서나 안전 제어시스템이 완전히 복구되었음이 입증되지 않는 한 자율주행은 허용되지 않음
연방, 주 및 지역 법률 (Federal, State and Local Laws)	자율주행차는 각 주(州)별 법과 관습을 지켜야 함. 지역별 제한속도나 유턴(U-turn) 금지, 일방통행 등을 인식할 수 있어야 하며, 충돌 등 긴급상황 대처를 위해 잠시 중앙선 침범 등 일시적 법 위반도 할 수 있도록 함
윤리적 고려 (Ethical Considerations)	사람이 운전 중에 여러 윤리적 판단을 하는 것처럼 자율주행 프로그램도 윤리적 측면의 결과 도래 윤리적 판단이 요구되는 상황별 대응전략이나 프로그램은 정부에 보고되어야 함
운영 설계(ODD: Operational Design Domain)	제조사는 여러 상황에서 자율주행차 작동 방식을 정의·문서화한 ODD를 작성해야 함. ODD는 도로 종류나 제한속도, 날씨 등 각 상황에서 자율주행차가 작동되는 기능이나 시스템의 정의 혹은 이를 기술한 설명서.
인식과 대응(Object and Event Detection and Response)	자율주행차가 사물과 상황을 어떻게 인식하여, 적절히 대응하는지가 입증되어야 함. 인식과 대응 능력은 일반 운행(Normal Driving)과 충돌방지 능력(Crash Avoidance Capability)으로 구분되어 입증해야 함
비상 대처 (Fall Back)	기술적 오작동 등 비상 상황 시, 안전하게 인간이 운전하는 모드로 전환하는 등의 비상 대처 전략이 있어야 함. 이 대처는 운전자가 운전이 가능한지, 졸음이나 음주 상태는 아닌지 등 여러 상황이 고려돼야 함
검증 (Validation)	제조사는 자율주행에 사용되는 수많은 기능이나 장치가 안전하게 작동되는지 평가·검증할 방법을 제시해야 함. 이 검증은 시뮬레이션은 물론 시험 도로나 일반 도로에서의 테스트를 포함하여야 함

자율주행자동차의 사례

- Auto alliance 의 Privacy Principles for Vehicle Technologies and Services
  - 투명성 (Transparency)
  - 선택권(Choice)
  - 맥락 존중 (Respect for Context)
  - 수집최소화(Data Minimization, De-Identification & Retention)
  - 데이터 보안(Data Security)
  - 무결성과 접근(Integrity & Access)
  - 책임성 (Accountability)
- Federal Automated Vehicles Policy
  - 제조사의 소비자 프라이버시 및 보안 협약 및 고지에 따라야 함을 규정

IoT와 개인정보보호 위협

WP 29 (2014)

- 통제의 결여와 정보의 비대칭
  - 눈에 잘 띄지 않는 방식으로 구석구석에 편재하는(pervasive) 서비스 제공 → 정보주체의 통제권 상실 가능성.
  - 물건과 물건, 물건과 개인 기기, 물건과 후단의 시스템 사이의 데이터 흐름을 통제하기 어려움. → 애초 설정된 목적을 벗어난 이용의 가능성.
- 이용자 동의의 품질
  - 이용자가 충분히 이해한 상황에서 동의했다고 할 수 있는가.
  - 일반 사물과 연결된 (connected) 사물의 식별 어려움 (ex : 일반 시계와 스마트 시계)
  - 일부 기기의 경우, 설계상 이용자 동의 메커니즘의 부재.

IoT와 개인정보보호 위협

- 데이터로부터의 추론과 원래 목적에서 벗어난 처리
  - 데이터량 증가에 따른 2차적 이용 요구 증가
  - 원시 데이터로부터 사용자에 대한 민감 정보 추론 (ex : '걸음수'로 건강상태 추론)
- 행동 패턴의 과도한 노출과 프로파일링
  - 분산된 데이터의 누적, 집적에 따라 이용자 프로파일링 가능성 확대
  - 이용자 행동 방식에 영향 (ex : 비정상적으로 보이는 행동 자제) → 잠재적 감시

IoT와 개인정보보호 위협

- 서비스 사용시 익명성 유지의 한계
  - 정보주체 주변의 모든 사물은 개인 식별에 연결되는 고유 식별자 생성 (ex : MAC 주소)
  - 개인 위치 및 이동성 분석에 활용 가능
  - CCTV 혹은 인터넷 로그와 같은 다른 시스템의 데이터와 결합 가능성.
- 보안 위험 : 보안 대 효율성
  - 기기의 제한된 컴퓨터 자원과 보안 요구사항의 균형 문제.
  - 보안 수준이 낮은, 네트워크에 연결된 기기는 공격 수단으로 악용될 수 있음.
  - 서로 다른 이해관계자(기기 제조업체, 애플리케이션 개발자, 네트워크 등) 사이의 보안 조정 문제.

IoT와 개인정보보호 위협

FTC (2015)

1. 민감 정보의 수집 (건강, 금융, 위치정보 등)
2. 개인정보, 습관, 위치, 물리적 조건에 대한 누적 수집 / 방대한 정보 수집 → 빅데이터 분석을 통해 민감 정보에 대한 추정
3. 데이터의 차별적 이용 : 보험, 신용, 고용 등
4. (업체 및 공격자에 의한) 민감한 개인정보에 대한 도청 위험성
5. 프라이버시 및 보안 위험성은 소비자의 신뢰 저해.

IoT의 보안위험성

- 무단 접근 및 개인정보 남용
- 다른 시스템에 대한 공격 수단으로 이용
- 개인 안전에 대한 위험

IoT 보안이 특히 더 취약한 이유.

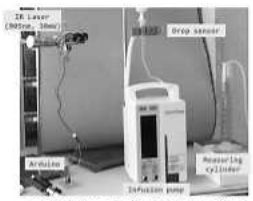
- IoT 업체가 보안 이슈에 대한 경험이 없는 경우가 많음.
- 많은 IoT 기기가 저렴하고 제품수명이 단기적.

(FTC, 2015)

IoT 보안 침해 사례

- 약물 주입기(Infusion Pump)의 센서 해킹 사례
- 삼성페이의 카드 정보를 탈취 후 다른 장비에 심어 불법 결제 성공
- 크라이슬러의 체로키 해킹(2015.7)
- 아마존에서 판매하고 있는 CCTV에 악성코드 탑재

(김학용, 2016)



자료 : KAIST, 전자신문에서 재인용

자료 : 유튜브, 전자신문에서 재인용

자료 : The Hacker News

FTC의 IoT 보안 권고

- 보안중심 설계(security by design)
  - 프라이버시/보안 위험 평가 수행
  - 수집, 보유하는 데이터의 최소화
  - 제품 출시 전 보안조치 테스트
- 모든 피고용인에 대해 보안에 대한 훈련
- 관련 서비스 제공자들이 합리적 보안 조치를 유지하고 감독할 것
- 시스템 내의 중대한 위험이 있을 경우, 여러 단계에서 보안 조치 구현 (defence-in-depth)
- 무단 접근을 제한할 수 있도록 합리적인 접근통제 조치를 취할 것
- 생애 주기 전반에 걸쳐 제품에 대한 지속적인 모니터링
- 보안 침해시 소비자에게 고지하도록 의무화하는 법의 입법을 의회에 제안

WP29의 보안관련 권고

- 보안 중심설계(Security by Design)
- 보안 취약점 발견시 이용자에게 고지
- 보안 지원 중단시 이용자에게 통보 및 대안적 해결책 제시
- 데이터 유출시 이용자에게 고지
- 사물인터넷의 특수성에 부합하는 가벼운 암호 및 통신 규약 개발

미래부 사물인터넷 정보보호 로드맵 시행계획 (2015)

- 비전 : 누구나 안전하게 사물인터넷의 편리함을 누리는 세계 최고의 스마트 안심국가 실현
- 추진전략
  - 기반 : 보안이 내재화된 IoT 기반 조성
  - 기술 : 글로벌 IoT 보안 핵심기술 개발
  - 산업 : IoT 보안 산업경쟁력 강화
- 추진과제
  - 1. Securaty Native : 보안이 내재화된 IoT 기반 조성
  - 1-1. 7대 분야 IoT 제품, 서비스 보안 내재화
  - 1-2. 'IoT 사이버위협 종합 대응체계' 구축
  - 1-3. 안전한 IoT 제품, 서비스를 위한 신뢰성 확보
  - 2. Security Frontier : 글로벌 IoT 보안 선도기술 개발
  - 2-1. IoT 보안 9대 핵심 원천기술 개발
  - 2-2. IoT R&D 오픈 이노베이션 체계 구축
  - 3. Security Premier : IoT 보안 산업경쟁력 강화
  - 3-1. IoT 보안 우수기업 발굴, 육성
  - 3-2. IoT 보안 제품, 서비스 수요 창출
  - 3-3. ICT와 Security가 결합된 맞춤형 'IoT Security Brain' 양성

IoT 개인정보보호 법제에 대한 문제제기

- 고지 및 동의 제도의 적절성
  - 편재하는 개인정보 수집 환경에서 동의의 실행 가능성
  - 이용자 인터페이스가 부재하거나 제한적인 경우
- 최소수집 원칙의 적절성
  - 추가 데이터 수집으로 가능한 애초에 예상하지 못했던 혁신의 제한
- 개인정보 규제 강화는 국제 경쟁력 약화

IoT 개인정보보호에 관한 WP29의 입장

- 이용자는 제품 수명주기 전반에 걸쳐 자신의 개인정보를 완벽하게 통제할 수 있어야 하며, 처리의 근거로서 동의가 필요할 경우, 그 동의는 충분한 정보에 기반하여 자유롭고 명확하게 주어져야 한다.
- 공정성 원칙은 개인정보가 해당 개인이 실제로 인식하지 못하는 방식으로 수집되고 처리되어서는 안된다는 것을 특별히 요구한다.
- 작업반은 … 데이터 최소화 원칙은 EU 법이 개인에게 부여한 개인정보보호 권리의 보호에 핵심적인 역할을 하며, 따라서 여전히 존중되어야 한다고 주장한다.

IoT 개인정보보호에 관한 WP29의 입장 [2]

- 가명화(pseudonymization) 또는 심지어 익명화(anonymization) 기술을 실행한 후에만 처리해야하는 개인에 관한 데이터도 개인정보로 고려되어야만 할 수 있다.
- 사물인터넷에서의 데이터 처리는 가입자 혹은 사물인터넷의 실제 이용자가 아닌 개인과도 관련됨. 가입자 외 이용자를 포함한 모든 정보주체의 개인정보 보호 필요.
- 자기정보에 대한 접근권 + 이전권(right to portability)
- 동의철회 및 처리거부권

최소수집 원칙에 대한 FTC의 입장.

- … (FTC) 직원들은 기업들이 소비자 데이터의 수집 및 보유를 합리적으로 제한할 것을 고려해야만 한다고 언급한 사람들의 입장에 동의한다.
  - 데이터가 많아질수록 내외적인 공격 유인이 높아짐
  - 소비자의 합리적 기대를 벗어나는 방식으로 데이터가 사용될 가능성이 높아짐
- FTC는 최소수집 원칙에 유연한 입장
  - 기업들은 (1) 데이터를 전혀 수집하지 않거나 (2) 제품 및 서비스에 필수적인 데이터만 수집하거나, (3) 덜 민감한 데이터만 수집하거나, (4) 수집한 데이터의 비식별화, (5) 혹은 추가적인 데이터 수집에 대해 소비자의 동의를 얻을 수 있음.

IoT 데이터의 비식별화에 대한 FTC의 입장

- 가능하면 비식별화된 형태로 데이터 수집할 것 권고
- 기술 발전에 따라 재식별의 위험은 상존. 따라서 기업의 책임성 메커니즘 중요.
  - 기술 발전을 고려하여, 비식별화하기 위한 합리적 조치를 취할 것
  - 데이터를 재식별화하지 않겠다는 것을 공중에 약속
  - 데이터를 공유하는 제3자 역시 재식별하지 않도록 효과적인 계약 체결.
- 데이터가 합리적인 수준에서 비식별화되지 않았을 경우, 그래서 향후 재식별되었을 경우, 규제자는 기업에 책임을 물을 수 있음.

동의(Notice and Choice)에 대한 FTC의 입장

- FTC 직원들은 소비자의 선택이 사물인터넷에서 여전히 중요한 역할을 할 것이라 생각한다. (The Commission staff believes that consumer choice continues to play an important role in the IoT.)
- 고지와 선택은 민감 데이터가 수집될 경우 특히 중요하다.
- FTC 직원들은 소비자에게 고지에 기반한 선택을 제공하는 것이 사물인터넷에서 여전히 현실적(practical)이라고 생각한다.
  - 단, 이것이 개인정보 수집시마다 매번 동의를 받아야 한다는 의미는 아니다.

동의를 위한 소비자 인터페이스가 없는 경우

- 판매 시점에서의 동의 (Choices at point of Sale)
- 비디오 설명서(video tutorials)
- 기기에 QR 코드 부착(affixing QR codes on devices)
- 기기 초기설정시 동의
- 웹포털 등을 통한 프라이버시 대시보드
- 아이콘 (예를 들어 네트워크에 연결할지, 말지를 간단한 버튼으로 제공)
- 소비자와의 별도의 통신 ("out of band" communication) : 이메일 등
- 일반적 프라이버시 메뉴 : 소비자 선택을 "패킷"으로 제공 (예를 들어, low, medium, high)
- 이용자 경험에 기반한 접근 : 이용자의 과거 선호에 따라 프라이버시 기본 설정
- 어떤 방식이든 명확하고 눈에 띄어야 함.

Use-based Approach 에 대한 FTC의 입장

- Use-based Approach : (입법자, 규제자, 자율규제기구, 업체 등이) 허용되는 이용과 허용되지 않는 이용 설정.
- 아직 IoT에 이용기반 접근 모델을 전적으로 채택하는 것은 시기상조
  - (1) 우선 아직 이용기반접근의 법적 근거가 없으며, 행동규약으로도 광범하게 채택되지 못한 상황이기 때문에, 누가 허용/비허용 기준을 결정할지 모호함.
  - (2) 이용 제한 자체만으로는 프라이버시/보안 위험을 해결할 수 없음.
  - (3) 이용기반접근은 민감 정보 수집에 대한 소비자의 우려를 고려하고 있지 못함.

IoT 개인정보 보호를 위한 WP29의 권고

1. 프라이버시 영향평가 수행
2. 가능한 한 원본 데이터 삭제
3. 프라이버시 중심설계 및 기본설정 원칙을 적용
4. 이용자 자기정보통제권 보장
5. 정보 제공, 거부권 안내, 동의 요청의 방식은, 가능한 한 이용자 친화적인 방식으로.
6. 정보주체에게 정보를 제공할 수 있는 방식으로 기기 및 애플리케이션 설계.

이용자의 개인정보 보호에 대한 신뢰가 IoT 성장의 열쇠임.

"Indeed, empowering individuals by keeping them informed, free and safe is the key to support trust and innovation, hence to success on these markets." (WP29)

참고문헌

- FTC(2015), Internet of Things : Privacy & Security in a Connected World, FTC Staff Report, 2015.1
- WP29(2014), Opinion 8/2014 on the on Recent Developments on the Internet of Things, ARTICLE 29 DATA PROTECTION WORKING PARTY, 2014.9.16
- 관계부처 합동(2014), 초연결 디지털 혁명의 선도국가 실현을 위한 사물인터넷 기본계획, 2014.5.8
- 구태언(2015),IoT 시대 개인정보보호를 위한 개인정보 정의/동의제도/시정 제도 개선 제안, 2015.4.13, https://www.slideshare.net/Gootiee/20150413-46915991
- 김범수 외(2014), 스마트기기 보급 확대에 따른 개인정보보호방안 연구 - 사물인터넷 환경을 중심으로, 개인정보보호위원회, 2014.12
- 김학용(2016), 사물인터넷 보안 사례 및 대응 방안, 2016.11.9, https://www.slideshare.net/honest72/20161109-68529308
- 나성현(2015), IoT 환경에서의 개인정보보호 이슈, 정보통신정책연구원 KISDI Premium Report, 2015.8
- 미래창조과학부(2014), [보도자료] 초연결 디지털 혁명의 선도국가 실현을 비전으로 사물인터넷 국가전략 수립, 2014.5.8
- 박준환 (2016), 자율주행자동차 시대를 대비한 법.제도적 체계 정비 방안, 국회입법조사처, 2016.11.15
- 신영진(2015), IoT 시대에서의 개인정보보호정책과제에 관한 연구, 한국행정학회 제2015년 하계학술발표논문집, 2015.12
- 이득연(2015), 신유형 서비스 소비자 문제연구(Ⅰ)-사물인터넷을 중심으로-, 한국소비자원 정책연구 15-14, 2015.12
- 황창근(2014), 사물인터넷과 개인정보보호, 법제연구 제46호, 2014.6.

사물인터넷(IoT) 분야 최근 개발 상황에 대한 2014/8 의견서[1)]

유럽연합 개인정보보호 제29조 작업반

2014년 9월 16일 채택됨.

개인정보의 처리에 관련하여 개인의 보호에 관한 작업반은 1995년 10월 24일의 유럽의회 및 유럽연합위원회 지침 95/46/EC에 따라 구성되었으며, 그 29조 및 30조를 유념하고, 절차 규칙을 유념하여, 현재의 의견서를 채택하였다.

요약

사물인터넷(IoT)이 유럽 시민의 삶에 통합되는 문턱에 서있다. 사물인터넷의 많은 프로젝트의 성공 가능성은 여전히 검증되어야 하지만, 우리의 가정, 자동차, 작업 환경 및 신체 활동을 모니터링하고 의사 소통하는 "똑똑한 것들"은 제공되고 있

1) 진보네트워크센터 번역. 원문 : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

다. 이미 오늘날, 연결된 기기는 개인삶의 계량화 및 가정 자동화의 대규모 시장에서 EU 시민의 요구를 성공적으로 충족시키고 있다. 따라서 사물인터넷은 이러한 시장에서 운영되고 있는, 크고 작은, 많은 수의 혁신적이고 창조적인 EU 기업을 위한 상당한 성장 전망을 가지고 있다.

WP29는 EU의 시민과 산업계의 이익을 위해 이러한 기대를 충족시키고자 열망한다. 그러나 이러한 기대되는 이익은 사물인터넷과 관련된 프라이버시 및 보안 문제 또한 존중해야만 한다. 종종 전통적인 IT 구조 외부에서 배포되고 기기 내 충분한 보안을 결여한, 이러한 기기의 취약점을 둘러싼 많은 논란이 제기되고 있다. 데이터 손실, 악성 코드에 의한 감염은 물론 개인 데이터에 대한 무단 접근, 웨어러블 기기의 침해적인 사용 또는 불법 감시는 사물인터넷의 이해관계자들이 자신들의 제품이나 서비스의 최종 사용자를 끌어들이기 위해 해결해야만 하는 많은 위험 요소들이다.

법적, 기술적 준수를 넘어, 사실 중요한 것은 그것이 사회 전체에 미칠 결과이다. 제품 개발에 있어 프라이버시 및 개인정보보호를 우선하는 조직은 자신들의 제품과 서비스가 프라이버시 중심설계의 원칙을 존중하고 EU 시민이 기대하는 프라이버시 친화적 설정을 갖추고 있음을 보장하는데 좋은 위치에 있을 것이다.

현재 이러한 분석은 EU 및 기타 국가의 많은 규제기관 및 이해관계자들에 의해 매우 일반적인 용어로만 언급되고 있다. WP29는이 의견서를 채택함으로써, 이 문제를 더욱 진전 시키고자 한다. 이를 통해 WP29는 EU의 개인정보 보호에 관한 높은 수준의 보호를 개발하는 것을 비롯하여, 사물인터넷에서 법적 개인정보 보호 체제의 통일적인 적용에 기여하고자 한다. 이 체제를 준수하는 것은 법적, 기술적 문제를 해결하는 것 뿐만 아니라, 그것이 기본적 인권으로서 개인정보 보호의 정도에 달려있기 때문에, 사회적 문제를 해결하는 데에도 핵심적인 관건이다.

따라서 이 의견서는 EU의 법적 체제가 이 맥락에 어떻게 적용되어야 하는지에 대한 지침을 제공하기 전에, 사물인터넷 생태계 내에 놓여있는 주요한 개인정보 보

호 위험을 확인하고 있다. 작업반은 관련 이해관계자들의 프로젝트의 핵심에 개별 이용자에 대한 가능한 높은 수준의 보증이 결합될 것을 지지한다. 특히 이용자는 제품 수명주기 전반에 걸쳐 자신의 개인정보를 완벽하게 통제할 수 있어야 하며, 처리의 근거로서 동의가 필요할 경우, 그 동의는 충분한 정보에 기반하여 자유롭고 명확하게 주어져야 한다. 그들이 이러한 목표를 달성하도록 돕기위해, 작업반은 서로 다른 이해관계자들(기기 제조업자, 응용 프로그램 개발자, 소셜 플랫폼, 추가 데이터 수신자, 데이터 플랫폼 및 표준화 기관)이 자신들의 제품 및 서비스에 프라이버시 및 개인정보 보호를 구현할 수 있도록 돕기 위한 포괄적인, 실질적 권고사항을 고안하였다.

실제로, 개인들에게 충분한 정보를 제공하고, 자유롭고 안전하게 함으로써 그들에게 권한을 부여하는 것은 신뢰와 혁신을 지원하고, 그래서 이 시장에서 성공하는데 핵심적이다. 작업반은 그러한 기대에 부응하는 이해관계자가 고객들이 자신의 데이터가 처리되고 공유되는 정도에 대해 인식하지 못하도록 하고 자신들의 생태계에 가두어 놓는데 의존하는 사업모델을 갖고 있는 자들보다 확고한 경쟁 우위를 가질 것이라고 굳게 믿는다.

사물인터넷에 의해 제기된 주요한 개인정보 보호 문제를 고려할 때, WP29는 그 발전을 계속 모니터링 할 것이다. 이를 위해 다른 국가 또는 국제 규제기관 및 입법자들과 이 문제에 대해 협력하는데 열려있을 것이다. 또한 시민사회 대표 뿐만 아니라, 특히 EU 내의 개인정보처리자(data controller) 혹은 개인정보취급자(data processor)로 운영되는 관련 업계와의 토론에도 열려있다.

도입

사물인터넷(IoT)의 개념은 통상의 일상적인 기기–다른 물건이나 개인과 연결된 것들, 혹은 “사물” 그 자체–에 내장된 수십억 개의 센서가 데이터를 기록, 처리, 저장, 전송하도록 고안되고, 고유한 식별자와 연계되어, 네트워크 기능을 가진 다른

기기나 시스템과 상호작용하는 인프라를 의미한다. 사물인터넷은 눈에 띄지 않게 통신하고 끊김없는 방식으로 데이터를 교환하도록 설계된 센서를 통해 광범위한 데이터 처리 원칙에 의존하기 때문에, "산재하는 (pervasive)" 그리고 "유비쿼터스 (ubiquitous)" 컴퓨팅 개념과 밀접하게 관련되어 있다.

사물인터넷 이해관계자는, 이용자의 환경 관련 데이터 "만"을 측정하기 위하여 혹은 이용자의 습관을 구체적으로 관찰하고 분석하기 위하여, 개인에 관한 이 데이터의 수집 및 추가 조합을 통해 새로운 애플리케이션과 서비스를 제공하는 것을 목표로 한다. 다시 말해, 사물인터넷은 일반적으로 식별되거나 식별가능한 자연인과 관련된 데이터의 처리를 의미하며, 따라서 EU 개인정보 보호 지침 2조의 의미에서 개인정보로 간주된다.

이러한 맥락에서 그와 같은 데이터 처리에는 상당히 많은 수의 이해관계자들(즉, 기기 제조업자 – 이들은 때로 데이터 플랫폼으로서 역할하기도 한다, 데이터 수집자 또는 중개자, 애플리케이션 개발자, 소셜 플랫폼, 기기 대여업체 또는 임대업체 등)이 조율되어 관여하게 된다. 이 이해관계자들 각각의 역할은 이 의견서에서 추가적으로 다뤄질 것이다. 이러한 서로 다른 이해관계자들은 다양한 이유로 관여하게 되는데, 즉 기술적인, 그리고 프라이버시 설정을 관리할 수 있도록 하기 위한 추가적인 기능 혹은 사용하기 쉬운 제어 인터페이스를 제공하기 위하여, 혹은 이용자가 별개의 웹 인터페이스를 통해 수집된 자신의 데이터에 일반적으로 접근할 수 있기 때문이다. 또한, 일단 데이터가 원격 저장되면, 그것은 다른 당사자와 공유될 수 있는데, 때로는 해당 개인이 그 사실을 모르는 경우도 있다. 이러한 경우, 기기의 대부분의 기능을 무력화시키지 않고는 이용자들이 이용자 데이터의 추가적인 전송을 방지할 수 없는 상태에 놓인다. 이러한 일련의 작업의 결과로, 사물인터넷은 기기 제조업자와 그들의 상업적 파트너가 매우 상세한 이용자 프로파일을 만들거나 접근할 수 있도록 할 수 있다.

위에서 언급한 바에 비추어, 사물인터넷의 발전은 새롭고 중요한 개인정보 보호

및 프라이버시 문제를 확실히 제기한다. 사실, 제어가 불가능한 경우, 사물인터넷의 일부 발전은 EU 법상 불법으로 간주 될 수 있는, 개인에 대한 감시의 형태로까지 발전할 수 있다. 사물인터넷은 또한 중요한 보안 문제를 제기하는데, 보안 침해가 그와 같은 맥락에서 데이터가 처리되는 개인에게 중요한 프라이버시 위험을 수반할 수 있기 때문이다.

따라서 WP29는 EU 시민의 기본적 권리가 위태로워질 수 있는, 그러한 활동으로부터 파생된 위험을 식별하고 모니터링하는 것에 기여하기 위해 이 의견서를 발표하기로 결정했다.

1. 의견서의 범위 : 3 가지의 사물인터넷 개발에 특별히 중점을 둠

현 단계에서 사물인터넷이 발전하는 정도를 확실하게 예측하는 것은 불가능하다. 이는 사물인터넷을 통해 수집된 모든 데이터가 유용한 것으로, 그래서 상업적으로 실현가능한 것으로 어떻게 변화된 것인지 여전히 열려있기 때문이기도 한다. 또한 사물인터넷이 클라우드 컴퓨팅 및 예측 분석과 같은 다른 기술 발전과의 융합 및 시너지 효과가 있는지 여부는 아직 명확하지 않으며, 현 단계에서는 신흥 시장 개발에만 관심이 있다.

따라서 WP29는 본 의견서에서 (1) 사용자와 직접 접속(인터페이스)하고 (2) 실제로 사용되는 기기 및 서비스에 해당하는, 그래서 실제로 개인정보보호법 하의 분석에 적합한, 세 가지 특정한 사물인터넷의 발전(웨어러블 컴퓨팅, 개인삶의 계량화 및 홈 자동화)에 대해 특히 초점을 맞추기로 결정하였다. 그래서 이 의견서는 M2M(“기계 대 기계)의 개발 뿐만 아니라, B2B 애플리케이션과 "스마트 도시", “스마트 운송” 과 같은 더욱 지구적인 이슈를 특별히 다루지는 않는다. 그러나 이 의견서의 원칙과 권고 사항은 여기서 다루는 좁은 범위외에도 적용될 수 있으며, 사물인터넷의 다른 발전을 포함할 수 있다.

1.1 웨어러블 컴퓨팅

웨어러블 컴퓨팅은 시계나 안경과 같이, 원래의 기능을 확장하기 위해 센서가 포함된 일상의 물건과 옷들을 지칭한다. 웨어러블(착용하는) 물건들은 개인에게 친숙한 일상의 물건들의 유용성이 확대되는 것이기 때문에 빨리 채택되기 쉽다. 그것들이 연결되지 않은 동종의 물건과 거의 구별이 되지 않을 경우 더욱 그렇다. 그것들은 기록하고, 기기 제조업자에게 데이터를 전송할 수 있는 카메라, 마이크, 센서를 내장할 수 있다. 더구나 웨어러블 기기용 API (예를들어, Android Wear3)가 공개되어 있어 제3자가 애플리케이션을 만들 수 있고, 그래서 그것들에 의해 수집된 데이터에 접근할 수 있다.

1.2 개인삶의 계량화(Quantified Self)

개인삶의 계량화(Quantified Self)는 자신의 습관이나 라이프스타일에 대한 정보를 기록하려는 개인에 의해 정기적으로 수행되도록 고안된다. 예를 들어, 개인은 수면 패턴에 대해 폭넓게 파악하기 위해 매일 밤 수면 추적기를 착용하기 원할 수 있다. 또 다른 기기는 소모한 칼로리나 걸은 거리 등 개인의 신체적인 활동과 관련한 양적 지표를 지속적으로 측정하고 보고해주는 활동 카운터와 같은 '움직임의 추적'에 초점을 맞춘다.

어떤 물건들은 체중, 맥박 및 기타 건강 지표를 더 측정하기도 한다. 시간 경과에 따른 추세와 행동의 변화를 관찰함으로써, 사전에 정의된 임계값이나 질병 증상의 존재 가능성에 기초하여 신체적 활동의 질과 효과에 대한 평가를 하는 등 질적인 건강관련 정보를 어느 정도까지는 추론하기 위하여 수집된 데이터가 분석될 수 있다.

개인삶의 계량화 센서는 종종 관련 정보를 추출하기 위해 특정한 조건 하에 착용할 것을 요구한다. 예를 들어, 적절한 알고리즘을 내장한, 정보주체의 벨트에 부착

된 가속도계는 복부의 운동을 측정할 수 있으며(원시 데이터), 호흡의 리듬에 대한 정보를 추출하고(총합데이터와 추출된 정보), 정보주체의 스테레스 정도를 보여줄 수 있다.(보여지는 데이터) 어떤 기기에서는 이용자에게 단지 후자의 정보만이 보여지지만, 기기 제조업자 혹은 서비스 제공자는 이후 단계에서 분석될 수 있는 훨씬 더 많은 데이터에 접근할 수도 있다.

개인삶의 계량화는 건강과 관련된 정보, 그래서 잠재적으로 민감한 정보가 수집된다는 점에서 뿐만 아니라, 그러한 데이터가 광범하게 수집된다는 점에서 문제이다. 사실, 이러한 움직임은 이용자가 건강할 수 있도록 자극하는데 주력하기 때문에, 전자의료(e-health) 생태계와 많은 관련을 가지고 있다. 그러나 최근 조사에 따르면, 측정값의 정확성 및 이들 데이터로부터 만들어진 추정의 정확성도 과제로 남아있다.

1.3 홈 자동화 ("domotics")

오늘날, 사물인터넷 기기는 인터넷을 통해 원격으로 통제될 수 있는 “연결된 전구”, 온도 조절기, 연기 경보기, 기상 관측소, 세탁기 또는 오븐 등과 같이 사무실이나 가정에도 놓일 수 있다. 예를 들어, 모션 센서를 포함하는 것들은 이용자가 언제 집에 있는지, 움직임의 패턴이 어떤지를 감지하고 기록할 수 있으며, 미리 지정된 특정한 작동(예 : 조명 전환 또는 실내 온도 변경)을 할 수 있다. 대부분의 가정용 자동화 기기들은 상시적으로 연결되어 있으며 데이터를 제조업체에 전송할 수 있다.

분명, 도모틱스는 특정한 개인정보 보호 및 프라이버시 문제를 제기한다. 왜냐하면, 그러한 맥락에서 사용 패턴을 분석하면 거주자의 생활 방식에 대한 세부 정보, 습관 또는 선택 사항 또는 단순히 지금 집에 있는지 등을 밝혀낼 수 있기 때문이다.

위에서 언급한 세가지 범주의 기기들은 현재 상태의 사물인터넷과 관련된 주요 프라이버시 이슈의 대부분을 보여주는 전형적인 사례들이다. 그러나 위의 범주가 배타적인 것은 아니라는 점을 지적한다. 예를 들어, 스마트 시계와 같은 “웨어러블” 기기는 심장박동수를 측정하는데 사용할 수 있다. 즉, 개인삶의 계량화 측정을 위한 기기가 될 수 있다.

2. 사물인터넷과 관련된 프라이버시 및 개인정보 보호 문제

WP29는 사물인터넷이 가져올 많은 중대한 프라이버시 및 개인정보 보호 문제들, 어떤 것은 새롭고 어떤 것은 좀더 전통적인, 하지만 사물인터넷의 진전에 따른 기하급수적인 데이터 처리의 증가와 관련하여 증폭되는 문제를 고려하여 이 의견서를 내기로 결정했다. 아래에 제시한 EU 개인정보 보호 법제와 실무적인 해당 권고사항들을 적용하는 것의 중요성은 이러한 문제들에 비추어 바라보아야 한다.

2.1 통제의 결여와 정보의 비대칭

눈에 잘 띄지 않는 방식으로 구석구석에 편재하는(pervasive) 서비스를 제공할 필요성의 결과로, 이용자들은 실제적으로 제3자의 모니터링 아래에 놓일 수 있다. 이는 개인정보가 투명한 방식으로 수집, 처리되느냐 여부에 따라, 이용자가 자신의 개인정보 배포에 대한 모든 통제력을 잃어버리는 상황을 초래할 수 있다.

보다 일반적으로, 물건들 사이의, 물건과 개인 기기 사이의, 개인과 다른 물건 사이의, 그리고 물건과 후단의 시스템 사이의 상호작용에 따라, 정보주체의 이익과 권리를 적절하게 보호하기 위해 사용되는 전통적인 도구들을 갖고는 거의 관리할 수 없는 데이터의 흐름을 만들어내는 결과를 낳을 수 있다. 예를 들어, 다른 종류의 콘텐츠와 달리, 사물인터넷이 발생시키는 데이터는 그것이 공개되기 전에 정보주체가 적절하게 검토하기 힘들 수 있으며, 이는 이용자가 통제권의 결여와 자신이

과도하게 노출될 위험을 명백하게 초래한다. 또한, 물건들 사이의 통신이 개인이 인식하지 못하는 상태에서, 기본설정에 의해 혹은 자동적으로 이루어질 수 있다. 물건들이 어떻게 상호작용할 것인지 효과적으로 통제하거나, 특정한 사물의 활성 영역과 비활성 영역을 정의하는 실질적인 경계선을 정의할 수 있는 가능성이 부재한 상황에서, 생성된 데이터 흐름을 통제하는 것은 엄청나게 어려워질 것이다. 그 데이터의 후속적인 사용을 통제하는 것은 더욱 어려워질 것이며, 이에 따라 애초 의도한 목적을 벗어나서 사용되는 것(function creep)을 막기 힘들어진다. 통제 결여의 문제는 클라우드 컴퓨팅이나 빅데이터와 같은 다른 기술적 발전에서도 우려가 제기되는데, 이러한 서로 다른 새로운 기술들이 복합적으로 사용될 수 있음을 고려하면 더욱 문제가 될 것이다.

2.2 이용자 동의의 품질

많은 경우, 이용자는 특정한 물건에 의해 수행되는 데이터 처리를 인식하지 못할 수 있다. 정보주체는 충분히 정보를 제공받은 상태에서 동의를 해야하므로, 이와 같은 정보의 부족은 EU법 상 유효한 동의를 입증하는데 중요한 장벽이 된다. 그러한 상황에서는 EU법 상 상응하는 데이터 처리의 법적 기반으로서 동의에 의존할 수 없게된다.

또한 스마트 시계와 같은 웨어러블 기기는 잘 눈에 띄지 않는다. 대부분의 사람들은 일반 시계와 커넥티드 시계를 구별하지 못할 수 있는데, 커넥티드 시계는 카메라, 마이크, 모션 센서를 장착하고 이용자가 인식하지 못하는 상태에서, 그리고 그러한 처리에 동의하지 않은 상태에서 데이터를 기록하고 전송할 수 있다. 이는 웨어러블 컴퓨팅을 통한 데이터 처리의 식별에 대한 문제를 제기하는데, 이는 정보주체가 실제로 볼 수 있는 적절한 표지를 두는 방식으로 해결될 수도 있다.

더불어, 최소한 어떤 경우에는, 사물인터넷 기기의 특정 서비스나 기능을 포기할

가능성은 현실적인 대안이라기 보다는 이론적 개념에 가깝다. 그러한 상황은 배후의 데이터 처리에 대한 이용자의 동의가 자유로운 것으로 간주될 수 있는지, 그래서 EU 법에 따라 유효한 것으로 간주될 수 있는지에 대한 문제를 제기한다.

또한, 이용자의 동의를 얻는 고전적인 메커니즘은 사물인터넷에 적용하기 어려울 수 있는데, 이는 정보의 부족에 기반한 "낮은 수준"의 동의, 혹은 개인의 명확한 의사표시에 의거한 세부적인 동의의 제공이 사실상 불가능해지는 상황을 초래한다. 실제로 오늘날 센서 기기는 통상적으로 스스로 어떠한 정보를 제공하거나, 혹은 개인의 동의를 얻는 유효한 메커니즘을 제공하지 않는 방식으로 설계되고 있다. 그러나, 이용자의 유효한 동의를 얻는 새로운 방식이 사물인터넷 이해관계자에 의해 고려되어야만 하는데, 예를 들어 기기 자체를 통한 동의 메커니즘을 구현하는 것이 될 수 있다. 프라이버시 프록시나 고정 정책 (Sticky Policies)과 같은 특정한 사례들을 추후 이 문서에서 언급할 것이다.

2.3 데이터로부터의 추론과 처리에 대한 원래 목적의 변경

사물인터넷에 의해 생성되는 데이터 양의 증가는 데이터 분석 및 상호매칭과 관련된 현대적 기술과 결합하여 이 데이터를 2차적으로 이용하도록 할 수 있다. 그것이 원래의 처리 목적과 관련이 있든 없든 말이다. 따라서 다른 당사자가 수집한 데이터에의 접근을 요청하는 제3자는 이 데이터를 완전히 다른 목적으로 이용하기를 원할 수 있다.

기기(예 : 스마트폰의 가속도계와 자이로스코프)를 통해 원래 수집된 명백히 중요하지 않은 데이터가 이후 완전히 다른 의미(예. 개인의 운전 습관)를 가진 다른 정보를 추론하는데 사용될 수 있다. 그와 같은 "원시" 정보를 통해 추론을 이끌어 낼 수 있는 이러한 가능성은 컴퓨터 과학 분야에서 잘 알려진 현상인 센서 융합과 관련하여 분석되는 고전적 위험과 결합되어야 한다.

개인삶의 계량화(Quantified Self)는 또한 집계 및 고급분석을 통해 모션 센서로부터 얼마나 많은 정보를 추론할 수 있는지 알려준다. 이 기기는 종종 원시 데이터(예: 정보주체의 동작)를 포착하기 위한 기본 센서를 사용하고, 민감한 정보(예:스텝 수)를 추출하기 위해 정교한 알고리즘에 의존하며, 최종 사용자에게 보여줄 잠재적으로 민감한 정보(예:신체적 조건)를 추론한다.

이와 같은 추세는 특정한 문제를 안고 있다. 사실, 이용자가 하나의 특정 목적을 위해 원래의 정보를 공유하는 것에는 상관하지 않아도, 완전히 다른 목적으로 사용되는 2차적 정보의 공유는 원하지 않을 수 있다. 따라서 (원시 데이터, 추출 데이터, 표시된 데이터) 각각의 수준에서 사물인터넷 이해관계자들이 데이터가 정보 처리의 원래 목적에 부합하는 목적으로만 데이터가 이용되고, 그러한 목적을 이용자가 알수 있도록 보장하는 것이 중요하다.

2.4 행동 패턴의 과도한 노출과 프로파일링

서로 다른 물건들이 개별적으로 분리된 정보를 따로 수집하는 경우에도, 충분한 양의 데이터가 수집되고 추가 분석되면, 개인의 습관, 행동, 선호의 특정 측면을 드러낼 수 있다. 위에서 보다시피, 센서의 확산에 의해 사소하거나 심지어 익명적 데이터로부터 일반적 지식의 생산이 쉬워질 것이며, 이는 중요한 프로파일링 역량을 촉진할 것이다.

이것을 넘어서, 사물인터넷 환경에서 수집된 정보에 기반한 분석을 통해 개인의 보다 더 상세하고 완전한 삶과 행동 패턴을 탐지할 수 있게 된다.

사실, 이러한 경향은 개인이 실제 행동하는 방식에 영향을 줄 수 있다. CCTV의 집중적인 이용이 공공 장소에서 시민들의 행동에 상응하는 영향을 미쳤음이 드러난 것과 같이 말이다. 사물인터넷으로 말미암아 그와 같은 잠재적 감시는 이제 가정을 비롯한 개인의 가장 사적인 공간에 미칠 수 있다. 이는 비정상적으로 보이는

것으로 탐지되지 않기 위해 통상적이지 않은 행위를 피하도록 개인에게 압력이 될 수 있다. 그러한 경향은 사적인 삶과 개인의 친밀함에 대한 침해가 될 수 있으므로, 매우 주의깊게 모니터링되어야 한다.

2.5 서비스 사용시 익명성 유지의 한계

사물인터넷 기능이 완전히 발전하면 현재 서비스를 익명적으로 이용하는 것을 어렵게 하고, 일반적으로 익명의 유지 가능성을 제한할 수 있다.

예를 들어, 정보주체와 매우 가깝게 위치하는 웨어러블 사물의 경우, 정보주체의 위치를 추적할 수 있는 지문을 생성하는데 유용한 다른 기기의 MAC 주소와 같은, 일련의 다른 식별자들에도 접근할 수 있다. 다수의 센서 기기의 다수의 MAC 주소의 수집은, 사물인터넷 이해관계자가 특정 개인을 식별할 수 있는 고유의 지문과 더 안정적인 식별자의 생성에 도움이 된다. 이러한 지문이나 식별자는, 군중과 개인의 위치 분석이나 이동 패턴의 분석과 같은 다양한 목적에 사용될 수 있다.

이와 같은 추세는 그 데이터들이 추후 다른 시스템(예: CCTV 또는 인터넷 로그)에서 생성되는 다른 데이터와 결합될 수 있다는 사실과 결합되어야 한다.

이와 같은 환경에서, 어떤 센서 데이터는 특히 재식별 공격에 취약하다.

위에서 언급한 바에 비추어볼 때, 사물인터넷 환경에서 익명성을 유지하고 개인의 프라이버시를 보호하는 것이 점차 어려워질 것임은 명백하다. 이러한 측면에서 사물인터넷의 발전은 중요한 개인정보 보호 및 프라이버시 우려를 수반하게 된다.

2.6 보안 위험 : 보안 대 효율성

사물인터넷은 몇 가지 보안 문제를 제기한다. 즉, 보안 및 자원 제약으로 인해 기기 제조업체들이 배터리의 배터리의 효율과 기기의 보안 사이에서 균형점을 찾고 있기 때문이다. 특히, 기기 제조업체들이 처리 순서의 모든 단계에서 기밀성, 완

전성(integrity), 가용성 기준의 구현과 물건 및 센서에 의한 컴퓨터 자원-과 에너지-의 사용을 최적화할 필요를 어떻게 균형을 맞출지 아직 명확하지 않다.

따라서, 사물인터넷으로 인해 일상의 물건들이 잠재적인 프라이버시 및 정보 보안의 공격대상이 될 위험이 있으며, 이 공격대상들은 현재의 인터넷보다 훨씬 더 넓게 분산된다. 보안 수준이 낮은, 네트워크에 연결된 기기는 잠재적으로 효과적인 새로운 공격 방법으로 사용될 수 있는데, 이는 용이해진 감시 행위와 데이터 유출을 포함한다. 데이터 유출은 개인 정보의 도난이나 손상을 야기할 수 있는데, 이는 소비자 권리와 사물인터넷 보안에 대한 개인의 인식에 광범한 영향을 미칠 수 있다.

또한 사물인터넷 기기와 플랫폼은 데이터를 교환하고 서비스 제공자의 인프라에 저장할 것으로 예상된다. 따라서 사물인터넷 보안은 단지 기기의 보안만이 아니라 통신 링크, 저장 인프라, 이 생태계의 다른 입력들까지 고려해야 한다.

마찬가지로, 서로 다른 처리 단계에서 기술 설계와 구현이 서로 다른 이해관계자에 의해 제공될 경우, 그들 사이에 적절한 조정을 보장할 수 없으며, 취약점으로 사용될 수 있는 약점을 초래할 수 있다.

예를 들어, 현재 시장에 출시된 대부분의 센서는 통신용 암호화 링크를 설정할 수 없는데, 컴퓨팅 요구사항이 저전력 배터리로 제한되는 기기에 영향을 미치기 때문이다. 단대단(end-to-end) 보안 관련하여, 일군의 서로 다른 이해관계자에 의해 제공되는 물리적, 논리적 구성요소가 통합되면서 가장 약한 요소의 보안 수준만큼만 보장하게되는 결과를 초래하게 된다.

3. 사물인터넷에서의 개인정보 처리에 관한 EU 법의 적용

3.1 적용가능한 법률

EU 내에서 사물인터넷이 제기하는 프라이버시 및 개인정보 보호 이슈를 평가할 관련 법적 체제는 지침(Directive) 95/46/EC와 지침 2009/136/EC에 의해 개정된 지침 2002/58/EC의 특정 조항으로 구성된다.

이 체제는 지침 95/46/EC 4조에서 설정한 조건이 충족되는 경우에 적용된다. 작업반은 적용가능한 법률에 대한 8/20108 의견서에서 4조의 조항의 해석에 대한 폭넓은 가이드를 제공한 바 있다.

특히, 지침의 제 4-1(a)항에 따르면, 회원국의 국내법은 해당 회원국의 영토 내에서 개인정보 처리자(controller)가 “설립된 상황에서" 수행되는 모든 개인정보 처리에 적용된다. 인터넷 기반 경제의 맥락에서 이 "설립(establishment)"이라는 개념은 최근 유럽사법재판소(European Court of Justice)에 의해 매우 광범하게 해석되어 왔다.

또한, 개인정보 처리자가 공동체의 영토 내에서 설립되지 않았지만, 회원국의 영토 내에 위치한 “장비(equipment)"를 사용하는 경우에도 회원국의 국내법이 적용된다. (4-1(c)항). 따라서, 지침 95/46/EC에 따른 개인정보 처리자로서 자격을 갖춘 (사물인터넷 기기의 개발, 배포, 또는 운영에 관련된) 사물인터넷 이해관계자가 4-1(1)항의 의미에서 EU 내에서 설립되지 않았더라도, EU 내에 위치한 이용자의 “장비”를 통해 수집된 개인정보를 처리하는 한 여전히 EU 법의 적용을 받을 가능성이 높다.

사실, 사물인터넷에서 서비스 제공의 맥락에서 개인정보를 수집하고 추가 처리하는데 사용되는 모든 물건들은 지침에서 의미하는 장비의 자격을 갖는다. 이러한 자격은 분명 기기 자체 (걸음 측정기, 수면 추적기, "연결된" 가정용 장치인 자동 온도 조절 장치, 연기 경보기, 연결된 안경 또는 시계 등)에 적용된다. 또한, 내장된 센서나 네트워크 인터페이스를 통해 이용자의 환경을 모니터링하고, 기기가 수집한 데이터를 다양한 관련 개인정보 수집자에게 전송하기 위해 소프트웨어나 앱이 사전에 설치된 이용자의 단말기 (예 : 스마트폰 또는 태블릿)에도 적용된다.

사물인터넷에 관여하는 서로 다른 이해관계자의 역할을 식별하는 것은 개인정보 수집자로서의 법적 지위를 부여하고, 그들 각자의 책임 뿐만 아니라 그들이 구현하는 처리에 적용가능한 국내법을 식별하기 위해 필수적이다. 사물인터넷에 관여하는 당사자들의 역할에 대한 식별은 아래 3.3 절에서 분석할 것이다.

3.2 개인정보의 개념

EU 법은 지침 95/46/EC 2조에 정의되어 있는 개인정보의 처리에 적용된다. 작업반은 개인정보의 개념에 대한 4/2007 의견서에서 이 개념의 해석에 대한 폭넓은 가이드를 제공한 바 있다.

사물인터넷의 맥락에서는, 개인이 "사물(things)"로부터 발생하는 데이터에 기반하여 종종 식별될 수 있다. 실제로 그러한 데이터–즉, 조명, 난방, 통풍, 에어콘 등의 중앙 제어에 의해 생성된 데이터–로부터 특정한 개인 혹은 가족의 생활 패턴을 식별할 수 있다.

또한, 가명화(pseudonymization) 또는 심지어 익명화(anonymization) 기술을 실행한 후에만 처리해야하는 개인에 관한 데이터도 개인정보로 고려되어야만 할 수 있다. 사실, 사물인터넷의 맥락에서 자동 처리되는 많은 양의 데이터들은 재식별될 위험을 안고 있다. 이 점에서, 작업반은 익명화 기술에 관한 최근 의견서에서 관련 발전을 언급했는데, 이는 이러한 위험을 식별하고 이 기술의 구현과 관련된 권고를 하는데 도움을 준다.

3.3 EU에 기반을 둔 개인정보 처리자(data controllers)로서의 사물인터넷 이해관계자

개인정보처리자(data controller)의 개념과 개인정보취급자(data processor) 개념과의 상호작용은 지침 95/46/EC의 적용에 핵심적인데, 그들이 EU 개인정보 보호

규칙과 관련하여 개인정보 처리의 실행에 관여하는 다양한 조직 각각의 책임에 영향을 미치기 때문이다. 이해관계자들은 “처리자" 및 “취급자" 개념에 대한 WP29의 1/2010 의견서를 참조할 수 있는데, 이는 다수의 행위자를 가지고 있는 복잡한 시스템에 이 개념을 적용하는데 관한 가이드를 제공하는데, 이러한 시스템에서 처리자들과 취급자들이 단독으로 혹은 결합하여, 서로 다른 정도의 자율성과 책임을 갖고 관여하는 많은 시나리오가 있을 수 있다.

실제로, 사물인터넷의 구현은 통상 기기 제조업체, 소셜 플랫폼, 써드파티 응용프로그램, 기기 대여업자 또는 대여자, 데이터 브로커 또는 데이터 플랫폼 등 다수의 이해관계자들이 결합하여 관여하고 있음을 보여준다.

이해관계자들의 복잡한 관계망에 따라, 그들 각각이 어떻게 관여하고 있는지의 특수성에 기반하여, 개인정보의 처리와 관련한 법적 책임을 그들 사이에 정확하게 분배할 필요성이 요청된다.

3.3.1 기기 제조업체

사물인터넷에서 기기 제조업체는 단지 물리적 상품을 고객에게 팔거나 다른 기관에게 무상표 제품을 판매하는 것 이상의 역할을 한다. 그들은 “물건들(Thing’s)”의 운영체제를 개발하고 수정하거나, 데이터의 수집과 그 빈도, 데이터가 어떤 목적으로 언제, 누구에게 전송되는지 (예를 들어, 회사가 자기 직원들에게 착용하도록 한 추적기를 통해 보고받은 데이터에 기반하여 보험료를 책정할 수 있음) 등 기기의 전반적인 기능을 결정하는 소프트웨어를 설치했을 수 있다. 그들 대부분은 실제로 기기에 의해 생성된 개인 데이터를 수집하고 처리하는데, 그들 자신이 그 목적이나 수단을 전적으로 결정한다. 따라서 그들은 EU 법 하의 개인정보처리자로 인정된다.

3.3.2 소셜 플랫폼

정보주체는 그런 데이터를 공개하거나 다른 이용자들과 공유할 수 있을 때 연결된 기기를 더욱 사용할 가능성이 크다. 특히, '개인삶의 계량화(Quantified Self)' 기기의 이용자는 그룹 내의 일종의 긍정적 경쟁을 촉진하기 위해 소셜 네트워크에서 다른 사람과 데이터를 공유하는 경향이 있다.

"사물"에 의해 수집되고 집계된 데이터의 그와 같은 공유는, 이용자가 애플리케이션을 그런 방식으로 설정해두면, 종종 자동으로 실행된다. 그리고 공유 역량은 통상 제조업체의 애플리케이션 표준 기본설정에 따르게 된다.

소셜 플랫폼에 이러한 정보들이 집계된다는 것은 특정한 개인정보 보호 책임이 이제 그들에게 적용된다는 것을 의미한다. 이 데이터가 이용자에 의해 그들에게 푸시(push)되기 때문에, 소셜 네트워크에서 그들 자신이 결정한 고유한 목적대로 이 데이터가 처리된다면, 그들은 EU 법에 의거하여 독자적으로 개인정보처리자의 지위를 갖게 된다. 예를 들어, 어떤 소셜 네트워크가 만보계에서 수집한 정보를 사용하여 특정 이용자가 규칙적으로 러닝을 하는 사람이라고 추론하고, 러닝 운동화에 대한 광고를 보여줄 수 있다. 이러한 지위 부여의 결과는 소셜 네트워크에 관한 앞선 WP9 의견서에 자세하게 서술되어 있다.

3.3.3 제3자 애플리케이션 개발자

많은 센서들이 애플리케이션 개발을 위해 API를 제공하고 있다. 애플리케이션을 사용하기 위해 정보주체는 제3자 애플리케이션들을 설치해야만 하는데, 이를 통해 그들은 기기 제조업체에 의해 저장된 이용자 데이터에 접근할 수 있다. 이 애플리케이션을 설치함으로써 종종 API를 통해 앱 개발자에게 데이터에 대한 접근을 제공하게 된다.

어떤 애플리케이션들은 특정 사물의 이용자에게 보상을 제공하기도 하는데, 예를

들어 건강보험업체에 의해 개발된 애플리케이션은 개인삶의 계량화 “기기”의 이용자들에게 보상을 제공할 수 있으며, 혹은 주택보험업체는 자신의 고객이 네트워크에 연결된 화재경보기를 제대로 설정하도록 하기 위한 특정한 애플리케이션을 개발할 수 있다. 이러한 정보들이 제대로 익명화되지 않는다면, 그러한 접근은 지침 95/46/EC의 2조에 따른 처리에 해당하게 되며, 따라서 데이터에 대한 접근을 설계한 앱 개발자들은 EU 법 하의 개인정보처리자로 간주되어야만 한다.

그러한 앱은 전통적으로 옵트인 방식으로 설치된다. 실제로, 그러한 접근이 이용자의 사전 동의를 받아야 하는 요구조건을 만족해야 할 경우, 그 동의는 명확하고 구체적이며 충분한 정보에 입각해야 한다. 그러나 실제 관행을 보면, 종종 제3자 애플리케이션 개발자에 의한 승인 요청이 충분한 정보를 보여주고 있지 않은 경우가 많아, 이용자의 동의가 구체적이고 충분한 정보에 근거했다고, 그래서 EU 법 하에서 유효하다고 보기가 힘들다. (아래 참조)

3.3.4 기타 제3자들

기기 제조업체와 제3자 응용프로그램 개발자 외의 제3자들도 개인에 관한 정보를 수집하고 처리하기 위해 사물인터넷 기기를 이용할 수 있다. 예를 들어, 건강보험업체는 소비자들이 얼마나 자주 운동을 하는지 모니터하고 이에 따라 보험료를 조정하기 위해 소비자들에게 만보기를 주고 싶어할 수 있다.

기기 제조업체와 달리, 그러한 제3자들은 사물에 의해 수집되는 데이터의 유형을 통제할 수는 없다. 그러나, 그들이 자신들이 결정한 특정한 목적을 위해 사물인터넷 기기에서 생성되는 데이터를 수집하고 저장한다면, 그 처리에 대해서는 개인정보처리자의 지위를 갖는다.

사례 : 한 보험회사가 새로운 사업을 개시하면서 좀 더 낮은 보험료 적용을 원하는

가입자에게 제공한다. 그 제안을 받아들인 가입자는 회사가 설정하고 등록한 만보계를 받게 된다. 가입자는 만보계가 기록한 데이터에 접근할 수 있지만, 그 기기 자체는 "FeelGood"이라는 업체가 소유하고 있으며, 그 업체 역시 가입자 데이터에 접근할 수 있다. 이 경우, 가입자는 정보주체로 간주되어야 하며, 만보계 애플리케이션의 계정에 접근 권한을 갖아야 한다. 반면, 보험 회사는 개인정보처리자의 지위를 갖게된다.

3.3.5 사물인터넷 데이터 플랫폼

표준화 및 상호운용성의 결여로, 사물인터넷은 때때로, 각 제조업체들이 자신만의 고유한 인터페이스와 데이터 포맷을 정의하는, "사물 인트라넷"으로 보여지기도 한다. 이때 데이터는 갇혀진 환경(walled environment)에 저장되며, 이는 이용자들이 자신의 데이터를 한 기기에서 다른 기기로 전송하거나 (혹은 심지어 결합하는 것)을 효과적으로 방지한다.

그러나 스마트폰과 태블릿이 많은 사물인터넷 기기를 통해 수집된 데이터가 인터넷으로 연결되는 자연스러운 관문 역할을 하게 되었다. 그 결과, 제조업체들은 관리를 중앙집중화하고 단순화하기 위해, 서로 다른 기기를 통해 수집된 데이터를 보관하기 위한 플랫폼을 계속해서 개발하고 있다.

그런 서비스의 개발로 그들이 자신의 목적을 위해 이용자의 개인정보를 수집하는 경우라면, 그러한 플랫폼 역시 EU 개인정보보호법 하의 개인정보처리자가 될 수 있다.

3.4 정보주체로서의 개인 : 가입자, 이용자, 비-이용자

사물인터넷의 가입자 및 보다 일반적으로 이용자는 EU 법 하의 정보주체의 지위를 갖는다. 수집되고 저장된 데이터가 단지 개인적, 혹은 가정내 목적으로만 사용된다면, 이는 지침 95/46/EC의 소위 "가정 면제"에 해당하게 된다. 그러나 실제로

사물인터넷의 사업모델은 이용자의 데이터가 개인정보처리자의 지위를 갖는 기기 제조업체, 애플리케이션 개발자, 다른 제3자에게 체계적으로 전송되는 방식이다. 따라서 사물인터넷의 맥락에서 "가정 면제"는 제한적으로만 적용될 것이다.

사물인터넷에서의 데이터 처리는 가입자 혹은 사물인터넷의 실제 이용자가 아닌 개인과도 관련될 수 있다. 예를 들어, 스마트 안경과 같은 웨어러블 기기는 기기 소유자보다는 다른 정보주체에 대한 데이터를 수집하게 될 것이다. 그렇다고 이러한 상황에 EU 법 적용이 배제되는 것은 아니라는 것을 강조할 필요가 있다. EU 개인정보 규정의 적용은 기기나 단말의 소유권이 아니라, 누구의 개인정보이든, 개인정보 처리 그 자체에 의해 결정되게 된다.

4. 사물인터넷 이해관계자들에게 부과되는 의무들

EU 법 하에서 (독자적이든 결합해서이든) 개인정보처리자의 지위를 갖는 사물인터넷 이해관계자는 지침 95/46/EC 및 지침 2002/58/EC의 관련 조항의 적용에 따라 그들에게 부여된 서로 다른 의무들을 준수해야만 한다. 이 의견서는 이 맥락에서 특별한 주의를 요하는 조항들의 적용만을 다루지만, 다른 조항들의 적용을 배제하는 것은 아니다.

4.1 e-Privacy 지침의 제5조(3)의 적용

사물인터넷 기기가 지침 2002/58/EC 5(3)조의 의미에서 "단말 기기"의 지위에 있는 한, 사물인터넷 이해관계자가 기기에 정보를 저장하거나 이미 저장된 정보에 대한 접근 권한을 획득할 때 해당 조항이 적용된다. 이 조항은 "가입자 혹은 이용자의 명시적인 요청에 의한 서비스 제공을 위해 꼭 필요한" 경우가 아닌 한, 그러한 행위가 합법적이기 위해서는 그러한 저장 및 접근에 대해 관련 가입자 혹은 이

용자가 동의할 것을 요구한다. 이러한 요구조건은 그러한 단말 기기에 저장된 프라이버시-민감 정보에 이용자 및 가입자가 아닌 이해관계자가 접근할 수 있을 때 특히 중요하다.

5(3)조의 동의 요구조건은 주로 기기 제조업체에 관련되지만, 이 인프라에 저장된 집계된 원시 데이터에 접근하려는 모든 이해관계자에 적용된다. 또한, 이용자 기기에 추가적으로 데이터를 저장하려는 모든 개인정보처리자에도 적용된다.

그러한 상황에서, 사물인터넷 이해관계자는 관련된 사람이, 처리자로부터 처리 목적에 대한 명확하고 포괄적인 정보를 얻은 후에, 그와 같은 저장 및 접근에 효과적으로 동의했음을 보장해야 한다.

따라서, 어떤 기기(웨어러블 기기를 포함하여)의 지문을 생성하는데 사용할 수 있는 기기 정보에 접근하기 전에 이용자의 동의가 확보되어야만 한다. 작업반은 작업문서 02/2013(WP-208)에서 쿠키 혹은 유사한 추적 기술에 대한 동의 개념에 대한 가이드를 이미 발표한 바 있으며, 지문에 대한 향후 의견서에서 이 이슈에 대한 추가적인 가이드를 제공할 것이다.

사례 : 만보계는 이용자의 걸음 수를 기록하고 이 정보를 내부 메모리에 저장한다. 이용자는 자신의 컴퓨터에 애플리케이션을 설치하여, 기기에서 직접 걸음 수를 다운로드할 수 있다. 기기 제조업체가 만보계에서 서버로 데이터를 업로드하려면, 지침 2002/58/EC 5(3)조에 따라 이용자의 동의를 얻어야 한다.

기기 제조업체는 데이터를 서버에 업로드한 후, 단지 분당 걸음수의 총계값만을 보유한다. 그 데이터에 대한 접근을 요청하는 애플리케이션은, 데이터가 기기 제조업체의 서버에 저장되어 있는 한, e-Privacy 지침의 5(3)조가 아니라, 추가적인 처리의 적법성과 관련된 지침 95/46/EC 조항의 적용을 받게 된다.

또한, 사물인터넷 기기의 소유자와 자신의 데이터가 모니터되는 사람(정보주체)은 다른 사람일 수 있다. 이러한 상황은 지침 2002/58/EC의 5(3)조와 지침

95/46/EC이 분산되어 적용될 수 있다.

사례 : 차량 대여 서비스는 렌트카에 차량 추적 기기를 설치한다. 차량 대여 서비스가 기기/추적 서비스의 소유자/가입자이지만, 차를 임대한 개인은 기기 이용자가 된다. 그럼, 5(3)조는 기기 제조업체에 (최소한) 기기 이용자(이 경우 차를 대여한 개인)의 동의를 얻을 것을 요구하게 된다. 또한, 차를 대여한 개인과 관련한 개인정보 처리가 합법적이기 위해서는 지침 95/46/EC 7조에 따른 별도의 요구사항을 따라야 한다.

4.2 처리의 법적 근거 (지침 95/46의 7조)

사물인터넷에서 개인정보처리자의 지위를 갖는 이해관계자는 (위의 4.3 절 참조) 합법적인 개인정보 처리에 대한 이 지침 7조에 열거된 요구조건 중 하나를 충족할 필요가 있다. 이 요구조건들은 5(3)조의 적용 외에 이 이해관계자들 일부에 적용되는데, 문제의 처리가 정보의 저장 이상일 경우, 혹은 이용자/가입자의 단말 기기에 저장된 정보에 접근할 경우이다.

이러한 상황에서 세 개의 법적 근거가 관련된다.

기기 제조업체에 의해서든, 혹은 소셜 또는 데이터 플랫폼, 기기 대여자 혹은 제3자 개발자에 의해서든, 사물인터넷 맥락에서 우선적인 첫번째 법적 근거는 동의이다. (7(a)조) 몇 가지 경우에 대해, 작업반은 지침 2002/58/EC의 7(a)조 및 5(3)조 요구조건의 동시 적용에 대한 가이드를 발표한 바 있다. EU 법 하에서 그러한 동의가 유효하기 위한 조건은 앞선 작업반 의견서에 명시된 바 있다.

또한, 7(b)조는 정보주체가 계약 당사자인 계약의 이행을 위해 필요할 경우 그 처리가 합법적임을 규정한다. 이 법적 근거의 범위는 “필요성” 기준에 제한되는데, 이는 처리 그 자체와 정보주체가 기대하는 계약의 이행 목적 사이의 직접적이고 객관적인 연결을 요구한다.

셋째, 7(f)조는 처리자 혹은 제3자나 그 데이터가 제공된 당사자의 정당한 이익의 목적에 필요할 경우 개인정보 처리를 허용하고 있는데, 이 경우 그 이익보다 지침 1(1)조에 의해 보호되는 정보주체의 이익 혹은 기본적 권리와 자유-특히, 개인정보 처리와 관련한 프라이버시권-가 더 중요할 경우에는 제외된다.

앞선 ASNEF 및 FECEMD (C-468/10 및 C-469/10) 병합 소송에서 이미 제시된 것에 더하여, 구글 스페인 소송에 대한 판결에서 유럽사법재판소는 이 조항의 해석에 대한 중요한 가이드를 제공하였다. 사물인터넷의 맥락에서 개인정보의 처리는, 사물인터넷 기기가 없었다면 데이터가 상호연결되지 않았거나 아주 힘들게 연결되었을 환경에서, 개인의 기본적 프라이버시권 및 개인정보 보호에 중대한 영향을 미칠 가능성이 크다. 그러한 상황은 수집된 데이터가 개인의 건강상태, 가정 혹은 친밀한 관계, 위치, 그리고 개인의 사적인 삶의 많은 측면들과 관련될 경우에 발생할 수 있다. 그러한 침해의 잠재적 심각성에 비추어볼 때, 사물인터넷 이해관계자가 가지고 있는 경제적 이해관계만으로 그러한 처리가 정당화되기 어렵다는 것은 분명하다. 처리자 혹은 제3자, 혹은 데이터가 제공된 당사자들이 추구하는 다른 이익들은 유효해야 한다.

사례 : 공공 교통수단의 사용을 촉진하고 오염을 줄이기 위한 계획의 체제 내에서, 시의회는 주차료 부과 및 접근 제한을 통해 도심의 주차를 규제하고자 한다. 요금은 엔진의 유형 (디젤, 가솔린, 전기) 및 차량의 연식 등 여러 변수에 따라 달라진다. 차량이 주차 공간에 접근했을 때, 센서가 번호판을 인식하여, 데이터베이스를 확인한 후, 사전에 설정된 기준에 따라 자동적으로 적용될 할증 혹은 할인을 파악한다. 이 사례에서, 요금을 결정하기 위해 번호판 정보를 처리하는 것은 개인정보수집자의 정당한 이익을 충족한다. 제한 구역을 통과하는 차량의 움직임에 대한 - 익명화되지 않은- 정보를 얻는 것과 같은 추가 처리에 대해서는 다른 법적 근거의 이용이 요구될 것이다.

4.3 데이터 품질과 관련된 원칙

종합하여, 지침 95/46/EC의 제6조의 원칙은 EU 개인정보보호법의 핵심을 구성한다.

개인정보는 공정하고 합법적으로 수집되고 처리되어야 한다. 공정성 원칙은 개인정보가 해당 개인이 실제로 인식하지 못하는 방식으로 수집되고 처리되어서는 안된다는 것을 특별히 요구한다. 이 요구조건은 사물인터넷과 관련하여 더더욱 중요한데, 센서가 실제로 눈에 잘 띄지 않도록, 즉 가능하면 보이지 않도록 설계되기 때문이다. 그러나 사물인터넷 환경에서 활동하는 개인정보수집자(무엇보다 기기 제조업체)는 지리적으로 혹은 디지털적으로 주변에 있는 모든 개인들에게, 그들 혹은 주변 환경과 관련한 정보가 수집될 때에는 그 사실을 알려야 한다. 이 조항을 준수하는 것은 엄격한 법적 요구조건 이상이다. : 공정한 수집은 사물인터넷과 관련된, 특히 웨어러블 컴퓨터에 대한 이용자의 가장 중대한 기대사항에 속한다.

> 사례 : 건강관련 기기는 정맥에서 혈액이 어떻게 흐르는지 모니터하고, 심장 박동 정보를 재기 위해 작은 빛을 이용한다. 이 기기는 혈액의 산소 수준을 측정하는 또 다른 센서도 포함하고 있지만, 기기나 이용자 인터페이스 상에서 이 데이터 수집에 대한 아무런 정보도 제공하고 있지 않다. 혈중 산소를 재는 센서가 완전한 기능을 갖추고 있어도, 이용자에게 먼저 고지하지 않고는 이 기능이 작동되어서는 안된다. 이 센서를 작동하려면 명시적 동의가 필요하다.

목적 제한의 원칙은 데이터가 구체적이고 명시적이며 합법적인 목적으로만 수집될 수 있다는 것을 의미한다. 애초의 목적에 부합하지 않는, 어떠한 추가적인 처리도 EU 법 하에서 불법적이다. 이 원칙의 목표는 이용자가 자신의 개인정보가 어떻게, 어떠한 목적으로 사용될지 알고, 개인정보처리자에게 자신의 개인정보를 맡길 수 있는지 결정할 수 있도록 하는 것이다. 이 목적은 데이터 처리가 발생하기 이전

에 규정되어야 하는데, 이는 처리의 핵심적인 조건들이 갑작스럽게 변경되는 것은 배제한다. 이는 사물인터넷 이해관계자들이 어떠한 개인정보 수집을 시작하기 전에 자신의 비즈니스 사례를 잘 파악하고 있어야 함을 나타낸다.

또한, 정보주체에 관해 수집되는 개인정보는 개인정보처리자가 사전에 결정한 특정 목적에 필요한 범위로 엄격하게 제한되어야 한다. ("데이터 최소화" 원칙) 그 목적에 불필요한 데이터는 "만일을 위해" 혹은 "나중에 필요할 수 있어서" 수집되거나 보관되어서는 안된다. 어떤 이해관계자들은 데이터 최소화 원칙이 사물인터넷의 잠재적인 기회를 제한할 수 있으며, 그래서 혁신에 장벽이 될 수 있다고 생각하는데, 이는 데이터 처리의 잠재적인 이익이 분명하지 않은 상관관계와 경향을 발견하기 위한 탐색적 분석으로부터 발생한다는 생각에 기반한다. 작업반은 이러한 분석에 동의하지 않으며, 데이터 최소화 원칙은 EU 법이 개인에게 부여한 개인정보 보호 권리의 보호에 핵심적인 역할을 하며, 따라서 여전히 존중되어야 한다고 주장한다. 이 원칙은 개인정보가 사물인터넷에서 작동하는 특정한 서비스 제공을 위해 필요하지 않을 때, 정보주체는 최소한 익명으로 서비스를 사용할 가능성을 제공받아야 함을 의미한다.

또한 6조는 사물인터넷의 맥락에서 수집되고 처리되는 개인정보가 그 데이터가 수집된 목적에 필요한 이상으로 보관되거나 추가적으로 처리되지 않도록 요구한다. 이러한 필요성 테스트는 사물인터넷에서 특정 서비스를 제공하는 각각의 이해관계자 모두에 의해 수행되어야 하는데, 그들 각자의 처리 목적이 실제로 다를 수 있기 때문이다. 예를 들어, 사물인터넷 상의 특정 서비스에 가입할 때 이용자가 전달한 개인정보는 이용자가 가입을 종료했을 때에는 즉시 삭제되어야 한다. 마찬가지로, 이용자가 그의 계정에서 삭제한 정보는 보관되어서는 안된다. 이용자가 서비스나 애플리케이션을 정해진 일정시간 동안 사용하지 않을 경우, 이용자 프로파일은 비활성화되어야 한다. 그 후 일정시간이 지나면, 그 데이터는 삭제되어야 한다. 이용자는 그러한 단계들이 취해지기 전에, 관련 이해관계자들이 사용할 수 있는 어떠한

방법을 통해서든, 고지를 받아야 한다.

4.4 민감한 데이터의 처리 (제8조)

사물인터넷에서 애플리케이션은 인종 또는 민족적 기원, 정치적 견해, 종교적 또는 철학적 신념, 노동조합 가입여부, 건강 또는 성생활 등을 드러낼 수 있는 개인정보를 처리할 수 있는데, 이것들은 실제로 "민감정보" 의 지위를 가지며, 지침 95/46/EC 8조에 의거하여 특별한 보호를 필요로 한다. 실제로, 사물인터넷에서 민감정보에 8조를 적용하기 위해서, 정보주체 스스로 그 정보를 공개하지 않는 이상, 개인정보처리자가 이용자의 명시적 동의를 받을 것을 요구한다.

그러한 상황은 “개인삶의 계량화” 기기와 같은 특정한 맥락에서 발생할 가능성이 있다. 이런 경우들에서, 관련 기기들은 대부분 개인의 웰빙과 관련한 데이터를 등록하고 있다. 이 데이터가 반드시 건강정보 자체를 구성하는 것은 아니지만, 데이터가 일정 시간동안 등록되면서 개인의 건강에 대한 정보를 빠르게 제공할 수 있고, 이에 따라 주어진 기간 동안의 변동성으로부터 추론을 이끌어낼 가능성이 있다. 개인정보처리자는 이런 질적 변화 가능성을 예상하고 이에 따른 적절한 조치를 취해야 한다.

사례 : 회사 X는 소비자들이 통상적으로 이용할 수 있는 상용 센서에 의해 발생하는 심전도 신호로부터 원시데이터를 분석하여, 약물 중독의 패턴을 감지할 수 있는 애플리케이션을 개발하였다. 이 애플리케이션 엔진은 ECG(심전도) 원시 데이터에서 특정한 특성을 추출할 수 있는데, 이는 사전 조사 결과에 의거하여 약물 소비와 연계될 수 있다. 시장에 출시된 대부분의 센서와 호환이 되는 이 제품은 단일 애플리케이션으로 사용할 수도 있고, 데이터 업로드를 요구하는 웹 인터페이스를 통할 수도 있다. 그러한 목적으로 데이터를 처리하기 위해서는 이용자의 명시적인 동의를 얻어야만 한다. 이러한 동의 요구조건의 준수는 7(a)조에 의거하여 정보주체로부터 동의를 받는 것과 같은 조건으로, 그리고 그 시점에 충족될 수 있다.

4.5 투명성 요구사항 (10조 및 11조)

6(2)조의 공정한 수집 요구조건을 넘어, 개인정보처리자는 10조 및 11조의 적용에 대해 정보주체에게 구체적인 정보를 전달해야 한다 : 처리자의 신원, 처리 목적, 데이터 수령자, 접근 권한과 반대 권한의 존재 (데이터가 추가로 더 공개되지 않도록 사물을 분리하는 방법에 대한 정보 포함).

애플리케이션에 따라, 이 정보들은 예를 들어, 사물 그 자체에서 제공될 수도 있고, 무선 연결을 통해 정보를 발신할 수도 있으며, 중앙의 서버에 의해 수행되는 프라이버시-보호 근접성 테스트를 통한 위치를 활용해 센서 근처에 위치한 이용자에게 알릴 수도 있다.

이 정보는 공정 처리 원칙에 따라 명확하고 이해하기 쉬운 방식으로 제공되어야 한다. 예를 들어, 기기 제조업체는 센서를 장착한 물건에 QR 코드 또는 플래시 코드를 부착하여 센서의 종류와 그것이 수집하는 정보 및 데이터 수집의 목적을 설명할 수 있다.

4.6 보안 (제17조)

개인정보 보호지침 17조에서는 처리자는 “개인 정보를 보호하기 위한 적절한 기술적, 조직적 조치를 반드시 취해야 한다” 및 “처리자는, 자신을 대신하여 처리가 수행되는 경우에는, 반드시 수행될 처리를 규율하는 기술적 보안 조치와 조직적 조치를 충분히 보장할 수 있는 취급자를 선택해야만 한다."고 규정하고 있다.

따라서, 개인정보처리자의 지위를 갖는 어떠한 이해관계자라도 데이터 처리의 보안에 대한 완전한 책임을 유지한다. 보안 원칙의 위반을 초래하는 보안 결함이 부적절한 설계 혹은 사용된 기기의 정비의 결과일 경우, 이는 개인정보처리자의 책임이 된다. 그런 의미에서, 이러한 개인정보처리자들은, 조합가능한 보안 원칙

(principles of composable security)을 적용하여 부품 단계를 포함한 시스템 전체적인 보안 평가를 수행할 필요가 있다. 같은 맥락에서, 사물인터넷 생태계의 전반적인 보안을 향상시키기 위해 국제적으로 인정되는 보안 표준의 준수 및 기기 인증의 이용이 구현되어야 한다.

개인정보를 실제로 처리하지는 않으면서 다른 이해관계자를 대신하여 하드웨어 부품을 설계, 제조한 하청업체의 경우, 엄격하게 얘기한다면, 개인정보 침해사고가 발생할 경우에, 기기의 보안에 결함이 있었다는 이유로 95/46/EC 지침 17조에 따른 책임을 지지는 않는다. 그러나, 다른 이해관계자들은 사물인터넷 생태계의 보안 유지에 있어서 핵심적인 역할을 한다. 정보주체에 대해 개인정보 보호에 대해 직접 책임을 지는 이해관계자들은 이 하청업체들이 제품을 설계하고 제조할 때 프라이버시 관련 높은 보안 수준을 실제 지원하도록 보장해야만 한다.

앞서 언급했듯이, 보안 조치는 사물인터넷 기기의 특정한 운영상 제한을 고려하여 구현되게 된다. 예를 들어, 오늘날, 대부분의 센서는 암호화된 연결을 제공하지 못하는데, 왜냐하면 기기의 물리적 자율성 혹은 비용 문제가 우선적으로 고려되기 때문이다.

또한, 사물인터넷에서 작동하는 기기는 보안을 지키기 어려운데, 기술적인 이유와 사업적인 이유가 모두 있다. 그 요소들은 통상 무선 통신 인프라를 사용하며, 에너지와 컴퓨팅 파워에 있어 자원이 제한적이라는 특징이 있기 때문에, 기기들이 물리적 공격, 도청 혹은 프락시 공격에 취약하다. PKI 기반과 같은, 현재 사용되는 대부분의 일반 기술들을 사물인터넷 기기에 이식하기 쉽지 않은데, 대부분의 기기들이 요구되는 처리작업을 감당하는데 필요한 컴퓨팅 파워를 가지고 있지 않기 때문이다. 사물인터넷은 서로 다른 정도의 책임을 부담하는 다수의 이해관계자들과 복잡한 공급망을 형성하고 있다. 보안 침해는 이들 누구로부터도 발생할 수 있는데, 특히 기기 사이의 데이터 교환에 기반한 M2M 환경을 고려하면 더욱 그렇다. 따라서, 저수준의 자원 환경에서도 사용할 수 있는 안전하고 가벼운 프로토콜 사용

의 필요성을 고려해야만 한다.

감소된 컴퓨팅 능력이 안전하고 효율적인 통신을 위험에 처하게 할 수 있는 상황에서, WP29는 데이터 최소화의 원칙을 준수하고, 개인정보 처리와 특히 기기에의 저장을 요구되는 최소한으로 제한하는 것이 특히 더 중요하다는 것을 강조한다.

또한, 인터넷을 통해 직접 접근할 수 있도록 설계된 기기들이 항상 이용자에 의해 설정되는 것은 아니다. 따라서 이 기기들이 기본 설정에 따라 계속 운영된다면, 공격자에게 쉬운 접근 경로를 제공해줄 수 있다. 네트워크 제한에 기반한 보안 관행은, 기본설정으로 중요하지 않은 기능을 비활성화하고, 신뢰할 수 없는 소프트웨어 업데이트 소스의 사용을 금지하여 (그래서 코드 변경에 기반한 멀웨어 공격을 제한하여) 데이터 유출의 영향과 정도를 제한하는데 도움이 될 수 있다. "프라이버시 중심설계(Privacy by Design)" 원칙을 적용하여, 그러한 프라이버시 보호가 처음부터 내장되어야만 한다.

또한, 자동 업데이트가 없으면 전문 검색 엔진을 통해 쉽게 발견될 수 있는, 패치되지 않은 취약점이 종종 발생한다. 심지어 이용자들이 자신의 기기에 영향을 미치는 취약점을 인식하고 있는 경우에도, 제조사의 업데이터에 접근할 수 없을 수 있는데, 이는 하드웨어의 제한 때문이거나 기기가 소프트웨어 업데이트를 지원할 수 없도록 하는 구식의 기술 때문이다. 기기 제조업체가 기기의 지원을 중단해야 한다면, 이를 지원할 수 있는 대안적 해결책이 제공되어야 한다. (예 : 소프트웨어를 오픈소스 커뮤니티에 개방하는 방법 등) 이용자는 자신의 기기의 결함이 수리되지 않은 채 노출될 가능성이 있음을 통보받을 수 있어야 한다.

시장에 출시된 어떤 자가추적 시스템(예 : 만보계, 수면 추적기) 또한 보안 결함이 있어, 공격자가 애플리케이션이나 기기 제조업체게 보고되는 측정값을 조작할 수 있도록 한다. 특히 이 센서에 의해 보고된 값이 간접적으로 이용자의 건강관련 결정에 영향을 줄 수 있다면, 이 기기들은 데이터 조작을 방지할 수 있는 적절한 보호를 필수적으로 제공해야 한다.

마지막으로 중요한 것은, 데이터 유출 통지를 위한 적절한 정책은 이 문제에 대한 지식을 전파하고 가이드를 제공함으로써, 소프트웨어와 설계 결함의 부정적 효과를 제한하는데 도움이 될 수 있다는 것이다.

5. 정보주체의 권리

사물인터넷 이해관계자들은 지침 95/46/EC의 12조 및 14조에 규정한 조항에 따라 정보주체의 권리를 존중해야 하며, 이에 따라 조직적 조치를 취해야 한다. 이 권리는 사물인터넷 서비스 가입자나 기기 소유자에 제한되지 않으며, 자신의 개인정보가 처리되는 모든 개인에 관련된다.

5.1 접근권

12(a) 조는 정보주체에게 개인정보처리자로부터, 처리되는 데이터 및 그 소스에 대한 모든 정보를 이해가능한 형식으로 취득할 수 있는 권리를 부여한다.

사실, 사물인터넷 상의 이용자는 특정한 시스템에 고착되는 경향이 있다. 기기는 통상 먼저 기기 제조업체에 데이터를 보내고, 기기 제조업체는 이 데이터를 웹포털이나 앱을 통해 이용자가 접근할 수 있도록 한다. 이러한 설계는 제조업체가 기기의 성능을 활용할 수 있는 온라인 서비스를 제공할 수 있도록 하는 반면, 이용자 측면에서는 기기와 상호작용하는 서비스를 자유롭게 선택할 수 없게될 수 있다.

또한, 오늘날 최종 이용자는 사물인터넷 기기에 의해 등록된 원 데이터에 접근할 수 있는 위치에 있는 경우가 드물다. 분명, 이용자들은 이해할 수 없는 원 데이터보다는 해석된 데이터에 더 즉각적인 관심을 갖고 있다. 그러나 그러한 데이터에 접근할 수 있다면, 기기 제조업체가 원 데이터로부터 자신에 관해 무엇을 추론할 수 있는지 최종이용자가 이해하는데 도움이 될 것이다. 또한, 원 데이터에 접근할 수 있다면, 예를 들어 원래의 개인정보 처리자가 자신이 원하지 않는 방식으로 프

라이버시 정책을 변경할 때, 이용자는 자신의 데이터를 또 다른 개인정보처리자에게 이전하거나 서비스를 바꿀 수 있을 것이다. 오늘날 실제로 이용자들은 서비스 이용을 중단하는 것 말고는 다른 선택의 여지가 없는데, 대부분의 개인정보처리자들이 그러한 기능을 제공하지 않거나, 저장된 원 데이터의 질낮은 버전에만 접근할 수 있도록 하기 때문이다.

WP29는 그러한 태도는 지침 95/46/EC의 12(a) 조에 따라 개인에게 부여된 접근권의 효과적인 행사를 가로막는 것이라고 생각한다. 반대로, 사물인터넷 이해관계자들은 이용자들이 이 권리를 효과적으로 실행할 수 있도록 하는 조치를 취해야 하고, 이용자가 기기 제조업체가 제안하지 않은 다른 서비스를 선택할 수 있는 여지를 제공해야만 한다. 그러한 취지로 데이터 상호운용성 표준이 유용하게 개발될 수 있을 것이다.

일반 개인정보보호규정(GDPR) 초안이 접근권의 변형으로서 만들려고 하는, 소위 “이전권(right to portability)"이 이용자 “고착(lock-in)” 상황을 확실히 종결시키는 것을 지향하고 있기 때문에 그러한 조치는 더더욱 관련이 된다. 이 점에 대한 유럽 입법자들의 야심은 경쟁에 대한 장애물을 해제하고 새로운 플레이어들이 시장에서 혁신할 수 있도록 돕는 것이다.

5.2 동의를 철회하고 반대할 가능성

정보주체는 특정 데이터 처리에 대한 사전 동의를 철회하거나 자신과 관련된 데이터 처리를 거부할 수 있어야 한다. 그러한 권리의 행사는 어떠한 기술적 또는 조직적 제약이나 장애없이 가능해야 하며, 이러한 철회를 등록하기 위한 도구는 접근 가능하고 가시적이며 효율적이어야 한다.

철회 제도는 세심하게 설계되어야 하며, 다음을 포괄해야 한다 : (1) 특정한 물건에 의해 수집되는 모든 데이터 (예 : 기상 관측소가 습도, 온도 및 소음 수집을

중지하도록 요청) (2) 무엇에 의해서건 수집된 특정 유형의 데이터 (예 : 이용자는 수면 추적기든 기상 관측소든 소리를 녹음하는 모든 장치에서 데이터 수집을 중단할 수 있어야 한다). (3) 특정 데이터에 대한 처리 (예: 이용자는 그의 만보계와 시계가 그의 발걸음을 카운트하는 것을 중단하도록 요구할 수 있다).

또한, 웨어러블 "연결된 사물"은 통상의 기능을 제공하는 기존의 품목을 대체할 가능성이 있기 때문에, 개인정보처리자는 그 물건의 "연결" 기능을 해제하고 애초의, 연결되지 않은 형태로 작동할 수 있는 옵션을 제공해야만 한다. (예. 스마트 시계나 안경에서 연결 기능의 해제) 작업반은 정보주체가 제공되는 서비스를 "종료하지 않고도, (자신의) 동의를 계속해서 철회할 수 있는" 가능성을 가져야 한다고 이미 명시한 바 있다.

> 사례 : 한 이용자는 자신의 아파트에 연결된 화재경보기를 설치하였다. 이 경보기는 점유 센서(occupancy sensor), 열 센서, 초음파(ultrasonic) 센서 및 광 센서를 사용한다. 센서들 중 일부는 화재 탐지에 필요하지만, 다른 센서는 단지 추가적인 기능만을 제공하며, 그는 이에 대해 사전고지를 받았다. 그 이용자는 화재 경보만을 사용하기 위해 다른 기능들은 비활성화할 수 있어야 하며, 이 기능들의 제공에 사용되는 센서를 연결에서 분리할 수 있어야 한다.

흥미롭게도, 이 분야에서 최근의 일부 발전은, 예를 들어, 부착 정책(sticky policies) 혹은 프라이버시 프록시(privacy proxy)의 이용을 통해, 정보주체에게 동의 관리 기능에 대한 더 많은 통제권을 부여함으로써 이용자의 권한을 강화하려고 하고 있다.

6. 결론 및 권고

몇 가지 권고가 아래 서술되어 있다. 작업반은 이 권고들이 유럽법상의 요건을

지금까지 서술한 사물인터넷에 적용하는 데 유용할 것으로 생각한다.

아래 권고들은 우리 작업반이 기존에 채택한 문헌들에 덧붙인 안내일 뿐이다.

이 점에 있어 작업반은 스마트기기의 앱에 대한 이전 권고에 특별히 주목할 것을 바란다. 스마트폰은 사물인터넷 환경의 일부이며, 양쪽 생태계가 비슷한 이해관계자를 포함하기 때문에 이 권고들도 사물인터넷과 직접 관련된 것들이다. 특히 앱 개발자들과 기기 제조사들은 적절한 수준의 정보를 최종 이용자(end user)에게 제공하고, 가능한 한 단순한 옵트아웃이나 세분화된 동의를 제공해야 한다. 나아가, 동의를 받지 못했을 경우 개인정보처리자는 개인정보를 다른 목적으로 사용하거나 제3자에 제공하기 전 익명화해야 한다.

7.1 모든 이해관계자에 공통적인 권고

- 사물 인터넷에 새로운 애플리케이션을 시작하기 전에 항상 프라이버시 영향평가를 수행해야 한다. 이 영향평가의 방법론은 작업반이 2011년 1월 12일 채택한 RFID 프라이버시/개인정보 영향평가 체제에 기반할 수 있다. 적절하고 실현가능한 방식으로 이해관계자는 일반 대중이 관련 영향평가 결과에 접근할 수 있도록 하는 것을 고려해야 한다. 예를 들어 스마트시티 등 특수한 사물인터넷 생태계에 맞춘 특정한 영향평가 체제가 개발될 수 있다.
- 많은 사물인터넷 이해관계자들은 총계값만을 필요로 하고 사물인터넷 기기가 수집하는 원본 데이터(raw data)를 필요로 하는 것은 아니다. 이들은 자신들의 정보 처리에 필요한 데이터를 추출한 후 원본 데이터를 가능한 한 빨리 삭제해야 한다. 원칙적으로, 원본 데이터 수집으로부터 가장 근접한 지점에서 삭제해야 한다. (정보가 처리된 스마트기기 자체에서 처리후 삭제하는 등)
- 모든 사물인터넷 이해관계자들은 프라이버시 중심설계 및 기본설정 원칙을 적용해야 한다.

• 이용자 권한강화는 사물인터넷 맥락에서 필수적이다. 정보주체와 이용자는 자신들의 권리를 행사할 수 있어야 하고, 개인정보 자기결정권의 원칙에 의거하여 언제든지 정보를 '통제할 수 있는' 상태여야 한다.

• 정보 제공, 거부권 안내, 동의 요청의 방식은, 가능한 한 이용자 친화적인 방식으로 이루어져야 한다. 특히 정보와 동의 정책은 이용자가 이해할 수 있는 정보에 중점을 두어야 하며, 개인정보처리자 웹사이트에 게시된 일반적인 프라이버시 정책에 국한되어서는 안된다.

• 또한 기기와 애플리케이션은 이용자 및 이용자 외 정보주체에게 정보를 제공할 수 있도록 설계되어야 한다. 예를 들어 기기의 물리적인 인터페이스를 통해서나 무선 채널을 통해 신호를 내보내는 방식 등이 있을 수 있다.

6.1 운영체제 및 기기 제조사

• 기기 제조사들은 이용자들에게 감지 장치(센서)가 수집하여 처리하는 데이터의 유형에 대한 정보를 제공해야 한다. 또한 수신하는 데이터의 유형들과 이것이 어떻게 처리되고 결합될지에 대해서도 정보를 제공해야 한다.

• 기기 제조사들은 정보주체가 동의를 철회하거나 정보처리를 반대하는 즉시 관련된 모든 이해관계자들에게 이를 알려야 한다.

• 기기 제조사들은 애플리케이션에 대한 접근을 허용할 때 세분화된 선택지를 제공해야 한다. 이는 수집된 데이터의 분류와 관련된 세분화 뿐 아니라 데이터가 수집되는 시간대와 빈도에 대한 세분화도 포함한다. 스마트폰의 "방해금지" 기능과 유사하게, 사물인터넷 기기는 스케줄에 따르거나 센서를 신속 비활성화시키는 "수집금지" 선택을 제공해야 한다.

• 위치추적을 방지하기 위해, 기기 제조사들은 사용되지 않을 때 무선 인터페이스를 비활성화함으로써 기기의 지문채취를 제한해야 한다. 또한 위치추적을 위해

지속적인 식별자가 사용되는 것을 방지하기 위해, 와이파이 네트워크를 스캔할때 임의의 맥주소(MAC address)를 쓰는 등 임의의 식별자를 사용해야 한다.

• 투명성과 이용자 통제권을 강화하기 위해, 기기 제조사들은 데이터가 어떠한 개인정보처리자에게 전달되기 전에 해당 공간에서 데이터를 읽고 편집하고 수정할 수 있는 도구를 제공해야 한다. 나아가 기기가 처리하는 개인정보는 데이터 이동성을 보장하는 형식으로 보관되어야 한다.

• 이용자들은 자신의 개인정보에 대한 접근권을 가진다. 자신의 개인정보를 구조적이고 통상적으로 사용되는 형식으로 손쉽게 내보낼 수 있는 도구를 제공받아야 한다. 따라서 기기 제조사들은 총계값 및 여전히 보관되어 있는 원본 데이터 모두를 얻고자 하는 이용자에게 이용자 친화적 인터페이스를 제공해야 한다.

• 기기 제조사들은 보안상 취약점이 발견되었을 때 이를 이용자에게 고지하고 기기를 업데이트할 수 있는 손쉬운 도구를 제공해야 한다. 기기가 뒤떨어지거나 더이상 업데이트되지 않을 때, 기기 제조사는 이를 이용자에게 고지해서 기기가 더이상 업데이트 되지 않을 것이라는 사실을 알수 있게끔 해야 한다. 취약점에 의해 영향을 받을 수 있는 모든 이해관계자에게도 고지되어야 한다.

• 기기 제조사들은 보안 중심설계(Security by Design) 절차를 따라야 하고 몇몇 요소들은 핵심 암호 기본요소로 지정해야 한다.

• 기기 제조사들은 기기에서 바로 원본 데이터를 총계값으로 전환함으로써 기기를 떠나는 데이터 양을 가능한한 많이 제한해야 한다. 총계값은 표준화된 형식이어야 한다.

• 스마트폰과 달리, 사물인터넷 기기들은 몇몇 정보주체가 공유할 수 있고 심지어 스마트홈과 같이 임대도 가능하다. 설정값은 같은 기기를 사용하는 서로 다른 개인들이 구분되도록 하여 서로의 활동을 알 수 없도록 해야 한다.

• 기기 제조사들은 표준화 기구와 데이터 플랫폼과 협업하여, 특히 눈에 띄지 않는 기기에 의해 데이터가 수집될 경우, 개인정보처리자의 데이터 수집 및 처리에

관련된 선호를 표현할 수 있는 공통 프로토콜을 지원해야 한다.

• 기기 제조사들은 지역적인 통제 및 처리 기기(소위 '개인정보 보호 프록시')를 사용하여, 이용자들이 자신의 기기에서 수집되는 데이터를 명확하게 알 수 있고, 기기 제조사에게 데이터를 전송할 필요없이 지역적인 보관과 처리가 가능하도록 해야 한다.

6.2 애플리케이션 개발자

• 센서가 데이터를 수집하고 있다는 사실을 이용자에게 자주 상기시킬 수 있도록 여러 고지문 혹은 경고문이 고안되어야 한다. 애플리케이션 개발자가 기기에 직접 접근할 수 없는 경우, 애플리케이션이 여전히 데이터를 기록하고 있다는 사실을 이용자가 알 수 있도록 애플리케이션은 주기적인 고지를 내보내야 한다.

• 애플리케이션은 사물인터넷 기기가 수집한 개인정보에 대한 정보주체의 열람, 정정 및 삭제권 행사를 용이하게 해야 한다.

• 애플리케이션 개발자들은 정보주체가 원본과 총계값을 표준적이고 가용한 형식으로 내보낼 수 있도록 도구를 제공해야 한다.

• 개발자는 처리되는 데이터의 유형과 그 데이터로부터 민감한 개인정보를 유추할 수 있는 가능성에 대해 각별한 주의를 기울여야 한다.

• 애플리케이션 개발자들은 데이터 최소화 원칙을 적용해야 한다. 총계값 사용으로 목적이 달성될 수 있다면 개발자들은 원본 데이터에 접근해서는 안 된다. 보다 일반적으로, 개발자들은 프라이버시 중심설계 접근방법을 따라야 하고 수집되는 데이터의 양을 서비스 제공에 필수적인 정도로 최소화해야 한다.

6.3 소셜 플랫폼

• 사물인터넷 기기에 기반한 소셜 애플리케이션의 기본설정은, 이 기기들에 의해

생성되는 정보를 소셜 플랫폼에 공개하기 전에, 이용자가 이를 검토하고 수정하고 결정하도록 물어보도록 해야 한다.

• 사물인터넷 기기들에 의해 소셜 플랫폼에 공개되는 정보는 검색 엔진에 노출되거나 색인이 생성되지 않도록 기본설정이 되어야 한다.

6.4 사물인터넷 기기 소유자 및 추가적인 수신자

• 인터넷에 접속된 기기 및 처리된 결과 데이터의 사용에 대한 동의는 충분한 설명에 기반해야 하고 자유롭게 이루어져야 한다. 이용자가 기기나 특정 서비스를 사용하지 않기로 결정했을 때 경제적으로 불이익을 받거나 자기 기기의 기능에 대한 접근에 제약을 받아서는 안 된다.

• 접속된 기기의 이용자와 계약 관계의 맥락에서 자신의 정보가 처리되는 정보주체는 (예를 들어 호텔, 건강보험, 차량 임대 등) 기기를 관리할 수 있는 위치에 있어야 한다. 계약 관계의 존재 여부를 불문하고, 모든 이용자 외 정보주체는 열람 및 거부권을 행사할 수 있어야 한다.

• 사물인터넷 기기의 이용자는 개인정보가 수집되는 이용자 외 정보주체에게 사물인터넷의 존재와 수집되는 데이터 유형에 대해 고지해야 한다. 또한 기기에 의해 자신의 정보를 수집당하지 않겠다는 정보주체의 선택을 존중해야 한다.

6.5 표준화 기구 및 데이터 플랫폼

• 표준화 기구 및 데이터 플랫폼은 서로 다른 당사자 사이의 데이터 전송을 용이하게 하고 사물인터넷 기기에 의해 자신에 대한 어떤 정보가 실제로 수집되는지 정보주체가 이해하기 쉽도록, 명확하고 자명할 뿐만 아니라 이동성과 상호운용성을 가진 데이터 형식을 촉진해야 한다.

• 표준화 기구 및 데이터 플랫폼은 원본 데이터의 형식뿐 아니라 총계값 데이터

형식의 출현에도 초점을 맞추어야 한다.

- 표준화 기구 및 데이터 플랫폼은 사물인터넷 데이터의 적절한 익명화를 촉진하기 위해 강력한 식별자를 되도록 적게 포함하는 데이터 형식을 촉진해야 한다.
- 표준화 기구는 정보주체를 위한 보안과 프라이버시 보호조치의 기준선을 수립하는 보증된 표준 제정에 힘써야 한다.
- 표준화 기구는 사물인터넷의 특수성에 부합하는 가벼운 암호 및 통신 규약을 개발해야 한다. 이는 기밀성, 완전성(integrity), 인증, 접근통제를 보장해야 한다.

메모

메모

메모