경제규제와 법 (Journal of Law & Economic Regulation)
제9권 제1호 (통권 제17호). (Vol. 9. No. 1). 2016. 5. pp.94~117

특집 | 사물인터넷(IOT) : 초연결사회 구현을 향한 법제도적 과제

사물클라우드 : 클라우드 컴퓨팅과 사물인터넷의 교차점에서의 영국의 정보보호와 소비자법†*

Clouds of Things : Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom

Guido Noto La Diega** · 이 범 수(Bumsoo Ee)(역)***

목차

〈국문초록〉

본 논문은 사물인터넷, 그리고 사물인터넷과 클라우드 컴퓨팅 간의 교차점인 이른바 사물클라우드에 대하여 비판적으로 분석한다. '사물'은 물리적 세계와 직접적으로 인터페이스되는(즉, 센서 기능 그리고/또는 기기를 작동하게 하는(actuating) 기능) 연결기능을 갖춘 물리적 개체로 이해된다. 또 다른 관점에 따르면(특히 제조물책임의 관점), '사물'은 하드웨어, 소프트웨어 그리고 서비스 간의 불가분의 혼합체로 이해될 수 있다.

기본적인 요소들에 대한 논의와 함께, 사물클라우드의 복잡성의 여섯 가지 요소에 대해 논의하고 가능한 규제방법들(규제, 공동규제(co-regulation), 자기규제(self-regulation), 전체론적 접근, 세분화)을 조명한다.

영국의 법제도에 초점을 맞추어, 본 논문은 영국에서 사물클라우드의 발달현황을 설명하고 사물클라우드로부터 제기되는 주요한 기술적, 법적 쟁점들 몇몇에 관해 다루도록 한다. 특히 정보보호, 프라이버시 그리고 소비자법을 중점적으로 논한다. 이 주제들은 규제당국에 의해 가장 중요하게

† 투고일자 2016. 3. 13, 게재확정일자 2016. 5. 30.
* 본 논문은 다음 논문에 대한 수정본이다: G. Noto La Diega, 「사물인터넷에 대한 영국의 시각. 사물클라우드-의료 사례를 중심으로(British perspectives on the Internet of Things. The Clouds of Things-Health use case, in Internet of Things: Legal Issues and Challenges towards a Hyperconnected World)」 서울대학교 공익산업법센터 국제학술세미나, 미국 호놀룰루, 2015.11. 27., 45-150.
** Buckinghamshire New University의 법학과 부교수이자 이 대학 지적재산권법의 리더; 'Ital-IoT'의 의장; University of Palermo의 지적재산권법 및 사법 전문가(휴직 중). Ian Walden 교수(Queen Mary University of London) 그리고 Jatinder Singh 박사(University of Cambridge Computer Laboratory)에 대해, 그들과 함께 한, 스마트홈 관련 사물인터넷 계약 및 사물인터넷-의료에 관한 공동의 학제적 연구에 대하여 특별한 감사의 마음을 전한다. 필자는 Honolulu 세미나에 참가한 모든 분들의 값진 기여에 신세를 지고 있다; 이원우 교수(서울대학교), 윤혜선 교수(한양대학교), Pierre-Jean Benghozi 교수(Université Paris-Saclay and ARCEP), 허성욱 교수(서울대학교), 이희정 교수(고려대학교), 임종인 교수(고려대학교), Deirdre Mulligan 교수(UC Berkeley), Hans-Heinrich Trute 교수(Universität Hamburg), 강성주 국장(미래창조과학부 인터넷융합정책관) 그리고 이한노 씨(Naver). 그러나 본 논문에서의 주장과 부족함은 모두 필자의 몫이다. 논문에 관한 코멘트는 noto.la.diega@gmail.com 또는 트위터 @guidonld로 보내주기 바란다.
*** 번역프리랜서(freelance translator)

다뤄지는 것이기도 하다.

관련 법적 쟁점들을 철저히 검토하고 영국의 사례를 참고한다면, 한국은 사물클라우드에 관한 그 잠재력을 실현시킬 수 있을 것이고 세계에서 가장 스마트한 국가로서 그 지위를 유지할 수 있을 것이다.

주제어: 사물인터넷, 사물클라우드, 클라우드 컴퓨팅, 용도변경, 규제

Ⅰ. 서론

기술적 발전을 '혁명'[1]으로 지칭하는 것은 '혁명'이 '지각변동의(disruptive)' 혁신[2]으로 이어질 것이라고 이야기하는 것만큼이나 흔한 일이 되고 있다. 사물인터넷[3]은 주목할 만한 현상이 되고 있다. 그로 인한 경제적 파급효과와 사회적 가능성이 대단히 클 수 있기 때문이다.[4] 그러나 사물인터넷이 우리의 삶을 어느 정도로 바뀌게 할지 그리고 법적인 관점에서, 현행 규칙이 변경되고 새로운 규칙이 마련되어야 하는지 여부 및 그러한 변경의 정도를 가늠하는 것은 아직은 시기상조이다.

따라서 순진한 찬사 대신, 본 논문은 사물인터넷, 그리고 사물인터넷과 클라우드 컴퓨팅 간의 교

1) 사물인터넷과 관련하여 다음을 참조: 국제전기통신연합(International Telecommunication Union, ITU), 「사물인터넷(The Internet of Things)」, ITU Internet Reports 2005, 2005.11. http://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf에서 이용 가능. 이에 의하면 "사물인터넷은 컴퓨팅과 통신의 미래를 대표하는 기술적 혁명으로서, 사물인터넷의 발전은 무선 센서에서부터 나노 기술에 이르기까지 많은 중요 분야에서의 역동적인 기술혁신에 달려 있다." 또한 다음을 참조하라: 기술전략위원회(Technology Strategy Board), 「사물인터넷과 사물간(M2M) 통신의 당면 과제와 기회: 최종보고서(Internet of Things (IoT) and Machine to Machine Communications (M2M) Challenges and opportunities: Final paper)」, May 2013. 다음의 사이트에서 볼 수 있다: https://connect.innovateuk.org/documents/3077922/3726367/IoT+Challenges,%20final+paper,%20April+2013.pdf/38cc8448-6f8f-4f54-b8fd-3babed877d1a. 이에 따르면, 사물인터넷은 "상호 간에 그리고 웹에 연결되는 다른 가젯(gadget)과의 네트워킹과 통신할 수 있는 기능을 갖춘, 인터넷에 연결될 수 있는 점점 더 많은 장치들의 등장으로부터 증명되는, 이미 진행 중인 혁명"이다.

2) 이에 관하여 S. Amyx, 「사물인터넷은 왜 모든 것에 혁신을 일으키는가(Why the Internet of Things Will Disrupt Everything)」, 2014.7., http://www.wired.com/insights/2014/07/internet-things-will-disrupt-everything/ 그리고 SRI Consulting Business Intelligence, 『혁신 기술의 세계동향 2025 (Disruptive Technologies Global Trends 2025)』, 「부록 F: 사물인터넷 F: The Internet of Things)」을 참조. http://www.internet-of-things.eu/resources/documents/appendix-f.pdf에서 이용 가능.

Clayton M. Christensen의 지각변동의 혁신 주장(그의 저서 『혁신자의 딜레마: 새로운 기술이 뛰어난 기업들을 실패하도록 만든 사례(The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail)』 Harvard Business School Press, Boston, 1997)에 대한 최근의 비판과 관련하여서는, A.A. King-B. Baatartogtokh, 「지각변동의 혁신 이론은 얼마나 유용한 것일까?(How Useful is the Theory of Disruptive Innovation)」, MIT Sloan Management Review, 2015 가을호. http://sloanreview.mit.edu/article/how-useful-is-the-theory-of-disruptive-innovation/에서 이용 가능.

3) 사물인터넷과 같은 개념 또는 동종의 관념을 나타내는 여러 표현들이 사용되고 있다. 그 주요한 것들로서, 산업인터넷(industrial internet), 스마트장치(smart devices), 연결된 사물(connected things), 유비쿼터스 컴퓨팅(ubiquitous computing), 피지컬 컴퓨팅(physical computing), 피지컬 인터넷(physical Internet), 사이버-피지컬 시스템(cyber-physical systems), 스마트 공간(smart spaces), 에브리웨어(everyware), 미래인터넷(future Internet), 만물인터넷(Internet of Everything), 편재형 컴퓨팅(pervasive computing), 편재형 인터넷(pervasive Internet), 주위공간 지능(ambient intelligence), 주위공간 미디어(ambient media), 촉각 컴퓨팅(haptic computing), 사물간 통신(Machine to Machine, M2M), 전파식별(radio-frequency identification, RFID), 네트워크연결 환경(Connected Environments), 스마트 도시(smart cities), 스파임(Spimes) [space + time], 연결된 세계(Connected World), 무선센서 네트워크(Wireless Sensor Networks), 상황 컴퓨팅(Situated Computing), 사물간 웹(web of things), 시맨틱 웹(semantic web), 웹3.0(web 3.0), 사물 네트워크(net of things), 자기 모니터링(quantified self). 실제로, 이들 중 일부는 사물인터넷의 일종을 표현하고 있고(가령, 자기 모니터링), 또 어떤 것들은 유사근접 영역을 지칭하고 있다(가령, 사물간 통신). 그러나 이들 대부분은 정확한 표현이 아니며 과학담론에서 그 사용을 지양해야 할 것이다. 이와 관련하여, 필자는 과학계에 'smart'와 'intelligent (지능이 있는)'라는 표현을 더 이상 사용하지 않기를 요청한다. 많은 사물클라우드 어플리케이션이 상당히 daff하다는 사실과 별개로, 지능과 스마트함은 전형적으로 인간에 속하는 속성이고 의인화의 우를 범하지 말아야 할 것이다. 게다가 이는 의미론적 전략에 관한 물음이기도 하다. 이 표현들은 이전 세대의 사물을 '사물'과 구별하는 의미를 내포하고 있다(가령, 이전의 미터와 스마트 미터의 대비). 그러나 몇 년 내에 대부분의 물체가 센서 기능 그리고/또는 기기를 작동하게 하는(actuating) 기능을 갖추게 될 것이고 그렇게 되면 이전의 것들은 쓸모 없어진 것처럼 보일 수 있기 때문이다.

4) 미국 연방거래위원회는 그 보고서 「사물인터넷. 연결된 세계에서의 프라이버시와 보안(Internet of Things. Privacy & Security in a Connected World)」(2015.1.)에서 "이 산업은 상대적으로 초기 단계에 있다"고 언급하며 균형 잡힌 의견을 내놓았다. 이 현상이 가지는 차원에 관해 수많은 보고서들이 쏟아져 나오고 있다; 최근 한 연구는 영국의 기업 절반 이상이 그들이 점점 더 많이 지출하게 되는 사물인터넷 비용에 대한 계획과 관리를 위해 이듬해에 최고사물인터넷책임자를 임명할 것을 제안했다(A. Scroxton, 「영국의 기업 절반이 사물인터넷을 관리할 역할을 찾고 있다(Half of UK businesses looking for internet of things lead roles)」, ComputerWeekly.com, 2016.2.17.).

차점인 소위 사물클라우드를 정의하려 한다. 기본적인 요소들에 대한 명확한 규정과 함께, 사물클라우드 복잡성에 관한 여섯 요소에 대해 논의하고 가능한 규제방법들(규제, 공동규제, 자기규제, 전체론적 접근, 세분화)을 다루도록 하겠다.

영국의 법제도에 초점을 맞추어, 영국에서의 발달현황[5]에 대해 설명하고 사물클라우드로부터 제기되는 주요한 기술적[6], 법적[7] 쟁점들 몇몇을 다루도록 한다. 규제당국이 보다 중요하게 생각하는 주제들, 즉 정보보호, 프라이버시, 소비자법을 특히 더 중점적으로 논의하겠다.

관련 법적 쟁점들을 철저히 검토하고 영국의 사례를 참고함으로써 한국은 사물클라우드에 관한 그 특별한 잠재력을 실현시킬 수 있을 것이고[8] 세계에서 가장 스마트한 국가로서 그 지위를 유지할 수 있을 것이다.[9] 드론, 무인자동차 그리고 생명공학에 대한 규제를 완화하겠다는 박근혜 대통령의 2016년 5월 18일의 발언은 이러한 방향으로의 움직임을 보여주고 있다.

Ⅱ. 사물인터넷, 그 정의와 가능한 규제방법들

클라우드[10]와 달리, 사물인터넷에 관하여는 일반적으로 받아들여지는 정의 또는 분류체계가 존재하지 않는다.[11] 그러나 최근 ICO와 IEC는 사물인터넷을 "물리적인 세계와 가상의 세계의 정보를 처리하고 그에 반응하는 것을 가능하게 하는 지능적인 서비스와 결합된, 상호 연결된 대상, 인간, 시스템 그리고 정보 자원의 인프라"[12]로 정의했다. ICO와 ICE의 정의가 출발점으로서 유용하겠지만, '마이크로소프트 클라우드컴퓨팅연구센터'는 '사물(Thing)'[13] 부분에 주목한다. 이들은 '사물'을 물리적 세계와 직접적으로 인터페이스 되는(즉, 센서 기능 그리고/또는 기기를 작동하게 하는(actuating) 기

5) 본 논문은 사법(私法)의 관점을 취한다. 그러나 영국에서는 다른 법 분야의 관점에서도 사물인터넷이 논의되어 왔다. 그 흥미로운 예의 하나가 내무성(Home Office), 「사물인터넷: 범죄 가능성과 그 예방 방법(Internet of things: potential risk of crime and how to prevent it)」, 2015.3.10. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/410117/Internet_of_things_-_FINAL.pdf에서 이용 가능.

6) 관련 문헌이 방대하게 존재하지만, 가장 좋은 예는 J. Singh-T. Pasquier-J. Bacon-H. Ko-D. Eyers, 「클라우드가 지원되는 사물인터넷에 관한 20가지의 보안 검토사항(Twenty security considerations for cloud-supported Internet of Things)」, Internet of Things Journal, 미국 전기전자기술자협회(IEEE), 2015, 99, 1.

7) 본 논문은 법적 쟁점에 관하여는 깊게 논의하지 않는다. 다음을 참조: Hon, W. Kuan and Millard, Christopher and Singh, Jatinder, 「사물인터넷에 관한 20가지의 법적 검토(Twenty Legal Considerations for Clouds of Things)」(January 4, 2016), Queen Mary School of Law Legal Studies Research Paper, No. 216/2016. http://ssrn.com/abstract=2716966에서 이용 가능.

8) 한국의 미래창조과학부 장관의 언급과 같이(「초연결 디지털혁명으로 이끌 사물인터넷 종합계획(Master Plan for Building the Internet of Things (IoT) that leads the hyper-connected, digital revolution), 2014.5.8., http://www.rfid-alliance.com/KOREA-IoT%20Master%20Plan.pdf에서 이용 가능), 비록 한국이 사물인터넷 경쟁력에서 주요국들에 비하여 뒤처져 있기는 하지만, 최상의 정보통신기술 인프라와 제조생산능력을 갖춘 한국은 세계시장의 선두로 올라설 잠재력(미국에 이어 두 번째)을 가지고 있다.

9) OECD, 「과학, 기술 그리고 산업 지표(Science, Technology and Industry Scoreboard 2015)」, 2015.10.19. http://www.oecd.org/sti/oecd-science-technology-and-industry-scoreboard-20725345.htm에서 이용 가능.

10) P. Mell-T. Grance, 「클라우드 컴퓨팅에 관한 미국 국립표준기술원의 정의. 미국 국립표준기술원의 권고(The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology)」. NIST Special Publication 800-145, 2011, 2. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf에서 이용 가능.

11) 2015년 3월, 필자가 사물인터넷에 관한 현존하는 정의들을 조사한 결과 64개의 정의 시도들을 찾았으나, 이들 중 어느 것도 그다지 설득력을 가지지 못했다. 이제 그 숫자가 두 배로 늘어났다고 해도 놀랍지 않을 것 같다. 미국 국립표준기술원 역시 이에 대한 정의를 시도하고 있다. 「사이버-피지컬 시스템의 틀에 관한 초안(Draft Framework for Cyber-Physical Systems)」(September 2015)에서 사물을 정의하며, 물리적 요소에 대한 언급 없이 정의되는 '물리적 개체('physical entity')'를 언급하는 것에 주목할 필요가 있다(가상의 사물 또한 모니터링과 제어 조작을 받을 수 있다; 개체에 가령 하위시스템이 존재하기 위해서 그것이 꼭 물리적이어야 하는 것은 아니다). 글 전체는 http://www.cpspwg.org/Portals/3/docs/CPS%20PWG%20Draft%20 Framework%20for%20Cyber-Physical%20Systems%20Release%200.8%20September%202015.pdf에서 이용 가능.

12) 국제표준화기구(International Organization for Standardization, ISO)와 국제전기표준위원회(International Electrotechnical Commission, IEC)의 합동기술위원회(Joint Technical Committee) 1, 「사물인터넷: 예비보고서 2014 (Internet of Things (IoT): Preliminary Report 2014)」, Geneva, 2015, § 4.1 (http://www.iso.org/iso/internet_of_things_report-jtc1.pdf). 그 '특별실무위원회 5'('사물인터넷')는 '사물인터넷에 관한 공통된 이해(理解)의 발전'을 위한 '특별그룹 1'을 만들었다. 이 '특별그룹 1'이 제안한 정의는 이후 '특별실무위원회 5'에 의하여 채택되었다.

13) 필자는 보통의 사물들로부터 구별하기 위하여 '사물(Thing)'이라고 지칭할 것이다.

능) 연결기능을 갖춘 물리적 개체로 이해한다.[14] 또 다른 관점에 의하면(특히 제조물책임), '사물'은 하드웨어, 소프트웨어 그리고 서비스 간의 불가분의 혼합체로 이해될 수 있다.[15]

'사물'은 착용될 수도 있고(가령, 웨어러블 기기(착용형 기기)) 임베디드(embedded)될 수도 있다(예를 들어, 스마트 심박조율기).[16] 이것들은 대개 합성물이다. 가장 간단한 예로 스마트폰, 또는 다른 기기 또는 네트워크와 연결된 자동차를 들 수 있다.[17] 그런데 '사물'을 "물리적 세계의 대상(물리적 사물) 또는 정보세계의 대상(가상의 사물)으로서, 식별되고 통신네트워크에 통합되는 기능을 갖춘 것"[18]이라는 ITU의 정의 방식에도 불구하고, 가상의 개체는 '사물'이 아니다. 인간과 동물은 '사물'이 아니다. 적어도 아직은 그렇지 않다. 인공기능향상(artificial enhancement)기술과 이식기술에서의 진화는 머지 않아, 인간 신체의 모든 부분이 인공의 기관(器官)과 세포조직으로 대체될 수 있고 손상을 입은 신체기능이 칩을 통해 치료되는 수준까지 발전할 것이다. 이것이 현실로 되는 순간(이는 과학소설(SF)에만 가능한 얘기가 아니다), 인간은 점차 안드로이드(인간 모습의 로봇)화(化)되고 '사물'화되면서 우리가 인간이 아니게 되는 것이 어느 지점부터인지가 불분명해질 것이다. 그런 때가 오면 우린 '사물'의 의미가 무엇인지 논쟁하는 대신, '인간'의 의미가 무엇인지 논쟁하게 될 것이다.[19]

관련 생태계(들)의 복잡성을 감안할 때, 이를 단순화하기 위한 한 가지 해법은 부문에 관한 분류체계를 통해 세분하고, 이를 통해 의료(가령, 로봇수술), 도시계획("스마트" 도시), 제조(가령, 3D 프린팅), 유통(특히, 공급사슬을 추적하기 위한 전파식별(RFID)의 이용), 운송(가령, 무인자동차, 자동차-자동차 간 시스템), 에너지(가령, "스마트" 그리드와 "스마트" 미터), 레저(가령, 게임, 드론), 그리고 농업(관개시스템) 등을 따로 떼어 하나씩 검토하는 것이다.

Hans-Christian Trute 교수[20]는 이러한 복잡성과 관련하여 사물인터넷에 대한 필자의 전체론적인 규

14) Hon-Millard-Singh (7), 4.

15) 보다 광범위한 것으로는, Noto La Diega, Guido and Walden, Ian, 「'사물인터넷'에서의 계약: Nest의 사례연구(Contracting for the 'Internet of Things': Looking into the Nest)」(2016.2.1.), Queen Mary School of Law Legal Studies Research Paper, No. 219/2016. http://ssrn.com/abstract=2725913에서 이용 가능.

16) 또한 '사물'은 인간과의 어떠한 물리적인 접촉도 가지지 않을 수 있다. 로봇을 생각해보라. 그러나 인간 가까이에서 작동하는 것이 '사물'의 고유한 특징이다. 이는 필자로 하여금 Walter Benjamin이 했던 지적을 돌아보게 한다. 「기계적 재생산 시대에서의 예술작품(Das Kunstwerk im Zeitalter seiner technischen Reproduzierbarkeit)」, 『사회연구(Zeitschrift für Sozialforschung)』, 1936, 5, I, 41-68. http://www.arteclab.uni-bremen.de/~robben/KunstwerkBenjamin.pdf에서 이용 가능. 영어 번역문은 https://www.marxists.org/reference/subject/philosophy/works/ge/benjamin.htm.); Benjamin에 따르면, "사물을 공간적으로 그리고 인간적으로 "보다 가까운 곳으로" 가져오려는 현대의 대중의 욕구는, 그것의 재생산을 기꺼이 인정함으로써 모든 현실의 독특함을 극복하려는 대중의 성향만큼이나 강렬한 것이다."

17) 스마트폰에는 많은 센서가 포함되어 있고, 앞서 기술한 '사물'의 부분들(하위 '사물'(sub-thing))에 어떤 결함 또는 부정확한 요소가 있는 경우 피해가 발생할 수 있다. 합성물인 '사물'을 책임지고 있는 주요 행위자에게 법적 책임을 물어야 하는지 또는 하위 사물 관련 행위자가 법적 책임을 져야 하는지 여부가 항상 명확한 것은 아니다. 일반적인 차원에서 보면 그리고 반대되는 증거가 제출되지 않는 경우, 필자는 첫 번째 가설에 찬동한다. 그 이유는 (i) 최종생산자가 합성물인 '사물'의 보안과 안전에 관하여, 그것을 시장에 내놓을 때 그리고 서비스 제공 중에, 이를 재차 확인해야 할 의무를 부담하기 때문이고, 또한 (ii) 소비자가 공급사슬을 추적하여 개별 하위 사물에 대하여 책임이 있는 자를 찾아내는 것은 불가능할 수 있기 때문이다. 그 결론은 시스템의 개방·폐쇄 여부에 따라 달라질 수 있다(예를 들어, 애플(Apple) 사(社)는 그 앱스토어를 통해 서드파티(third-parties) 앱들을 컨트롤할 수 있는 반면, 안드로이드 스토어는 개방되어 있어서, 그와 같은 컨트롤이 가능하지 않을 수 있다). 합성물인 '사물'에 포함된 하위 사물들의 숫자에 관하여(가령, 항공기와 전구(電球)에서의 차이와 같이), 그리고 '사물'이 이용되는 활동의 종류에 관하여(세동제거기는 생명유지와 관련되기 때문에 보안과 검사에 관하여 보다 엄격한 기준이 요구된다), 법원이 어떤 지침을 마련해 줄 수도 있을 것이다.

18) 국제전기통신연합 국제전기통신표준화부문(International Telecommunication Union Standardization Sector), 「사물인터넷에 대한 개관(Overview on the Internet of Things)」, Y.2060, 06/2012, § 3.2.3. https://www.itu.int /rec/T-REC-Y.2060-201206-I/en에서 다운로드 가능.

19) 동시에, '사물'은 기계학습(machine learning) 기술과 이른바 인공지능의 발달 덕분에 점점 더 자율적으로 될 것이다. 그러나 '사물'이 인간과 같은 것이 되지는 않을 것임을 유의해야 한다. '사물'이 인간과 비슷하게 보일 수는 있겠으나, 이는 인간중심적인 관점의 결과이다. '사물'이 완전히 그리고 적절하게 자율적으로 되었을 때(이는 실현 불가능한 가정이 아니다), '사물'의 지능은 인간의 지능과 공통된 부분이 많지 않을 것이다.

20) 본 논문에서 달리 명시하지 않고 거론하는 경우, 사물인터넷에 관하여 하와이에서 이루어졌던 토론 내용을 언급하는 것이다.

제 제안에 비판적인 의견을 제시하였다(필자는 특정한 경성법 수단이 사물인터넷 관련 법제에 우스꽝스러운 해법이 될 것이기 때문에, 그 대신 관련 요소들을 명확하게 밝혀내기 위한 지침을 이야기하고자 했었다).[21] 그러나 대부분의 부문들 간에는 상당한 정도의 중첩된 부분이 존재한다(드론과 BYOD (bring your own device)만 생각해보는 것으로 족하다. 이들은 어느 범주에도 들어갈 수 있다). 이는 그중에서도 규제당국들이 그들이 사물인터넷을 규제하려 할 때 그들에게 권한이 없는 경우와 맞닥뜨린다는 사실로부터 증명된다. 이는 주로, 이러한 중첩이 여러 규제당국들 간의 권한의 중복이기도 하기 때문이다(가령, 통신과 정보보호).[22]

나아가, 그리고 아마도 가장 중요하게도, 사물인터넷 시스템의 중요한 특징은 용도변경이다. 필자는 '용도변경'을 '사물'이 일정 목적을 위하여 만들어지고/만들어지거나 제공되었지만, 다른(예견되지 않았던 것일 수 있는) 목적으로 이용되는 현상으로 이해한다. 즉, (i) 관련 생태계 내에서의 그리고 클라우드에서 처리되는 하위시스템들 간의 통신이 단일의 '사물'이 해낼 수 없는 기능 수행 또는 정보 산출로 이어질 수 있고, (ii) 일정 상황(가령, 응급상황) 하에서 그 시스템은 자동으로 또는 사용자에 의해서 설정이 변경될 수 있는 것이다.[23]

그렇다면 사물인터넷에 대한 최선의 규제방법은 무엇인가? 최근의 연구들은 자기규제(self-regulation)가 만족스러운 방법이 아니라는 것을 보여주었다.[24] 그러나 전통적인 규제방식은 지속적으로 변화하는 기술적 지형에 요구되는 유연성이 부족하다. 따라서 공동규제(co-regulation)가 적절한 수단으로 보인다.[25] 일반적인 규칙의 틀을 명확하게 제시하되 그 실행은 사적인 이해당사자들에게 맡기는 것이다. 그런데 사물인터넷에 관하여 일반적으로 적용되도록 제정된 규제와 세부화된 규제 사이에 어떻게 균형점을 찾을 것인가? 이에 관한 모범 사례는 이탈리아에서 찾아볼 수 있다. 이탈리아에서는 최근 사물간(M2M) 통신[26]에 관한 상임위원회가 설립되었고 여기서 규제기관과 장관들이 그들의

21) FTC (4), 50에 따를 때; "사물인터넷에 특수한 입법이 필요한 것은 아니지만, 그 워크숍은 의회가 일반적인 정보보안 입법 [그리고] 일반적인(사물인터넷에 특수한 것이 아닌) 프라이버시 입법을 제정할 필요가 있다는 또 하나의 증거가 되었다."

22) Pierre-Jean Benghozi 교수는 이것이 프랑스의 사례라고 말했다(그는 전기통신위원회(Autorité de Régulation des Communications Électroniques et des Postes, ARCEP)의 위원이다).

23) 목적은 특히 법적 책임과 정보보호의 규칙과 관련하여, 법적 관점에서 핵심적인 역할을 담당한다. 그러나 이 주제는 또 다른 연구에서 다뤄져야 할 것이다.

24) McCarthy, D. & Morling, P., 「최후수단으로서의 규제: 자발적인 접근방식의 이행에 대한 평가(Using Regulation as a Last Resort: Assessing the Performance of Voluntary Approaches)」(2015), 왕립조류보호협회(Royal Society for the Protection of Birds). 대부분의 자기규제 계획은 82%의 이행에 그치고 있다. 반면 FTC (4) 49에 따를 때, 미국의 규제기관은 "특정 산업들에 대해 설계된 자기규제 프로그램의 발전이 프라이버시와 보안에 민감한 실무가 정착되도록 촉진하는 수단으로서 유용할 것으로 생각한다."

25) 공동규제는 유럽연합 집행위원회에 따를 때에도 최선의 수단으로 꼽히고 있다. 유럽연합 집행위원회, 「사물인터넷의 구조(IoT Architecture)」. http://ec.europa.eu/information_society/newsroom/cf/dae/document. cfm?doc_id=1750에서 이용 가능.

26) Machine Type Communication (MTC)라고도 불리는 사물간 통신은 "모바일 전기통신망에 지대한 영향을 미칠 잠재력이 있는, 급속히 성장하는 분야이다. 사물간 통신은 장치들이 인간의 개입 없이 상호 통신하는 수많은 영역들을 포괄한다."(국제전기통신연합 국제전기통신표준화부문(ITU-T), 「사물간 통신과 비(非)사물간 모바일 데이터 어플리케이션의 모바일 네트워크에 대한 영향(Impact of M2M communications and non-M2M mobile data applications on mobile networks)」, 2012.6.15. http://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-IOT-2012-M2M-PDF-E.pdf에서 이용 가능.)

사물간 통신이 사물인터넷의 선구자 격으로 이해되어야 하는지 또는 사물인터넷의 일종으로 이해되어야 하는지에 관하여는 의견이 일치되어 있지 않다. 예를 들면, 「전기통신에 관한 유럽 단일시장과 연결된 대륙(a Connected Continent)의 형성을 위한 그리고 지침 2002/20/EC, 2002/21/EC 그리고 2002/22/EC, 그리고 규칙 (EC) No 1211/2009 and (EU) No 531/2012 {COM (2013) 627 final} {SWD (2013) 332 final}, 11.9.2013, SWD (2013) 331 final, 8.2.2을 개정하는 조치에 관한 유럽연합 집행위원회 유럽연합 의회와 이사회의 규칙에 관한 제안서」에 부속된 "유럽연합 집행위원회 영향평가(Commission Staff Working Document Impact Assessment)"에 따르면, "점점 더 많은 부문에서, 장치들이 연결되고 그 연결을 통해 상호작용하는 '사물인터넷' 또는 사물간 통신 기술이 도입될 예정이다." 반면, "사물인터넷은, 물리적 환경에 그 기초를 두고 있으면서 인터넷에 연결된 사물의 신흥 조류에 관한 기술, 시스템 그리고 설계 원리에 대하여 광범위하게 이용되는 용어이다. […] 사물간 통신과 달리, 사물인터넷은 또한 그러한 시스템과 센서가 보다 광범위한 인터넷에 연결되어 있다는 것, 그리고 일반적인 인터넷 기술이 이용되고 있다는 것 또한 표현한다."(J. Höller et al., 「사물간 통신으로부터 사물인터넷으로: 지능의 새로운 시대에 대한 개설(From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence), Oxford (MA), 2014, 14.)

계획을 조정하도록 하였다.[27]

영국정부 과학분야 최고고문(Government Chief Scientific Adviser, GCSA)[28]은 "입법은 사물인터넷의 활용을 촉진하기 위하여 요구되는 최소한의 수준으로 유지되어야 한다"[29]는 점을 지적하였다. 그러나 새로운 규제 과제들(주로, 프라이버시와 법적 책임 관련)이 등장할 것이고, 따라서 "새로운 과제를 예상하고 이에 대처하기 위하여 적절한 규제와 입법이 필요할 것"[30]이라고 하였다. 필자는 연역적 접근, 사전적 규제, 경성법적 수단 등에 전적으로 동의하지는 않는다.

접근방식은 점진적이고, 경험적이고, 문제중심적인 것이어야 한다. 그럼에도 불구하고 필자는 "정책, 실행, 운용계획에서 새로이 출현하는 기술들의 영향을 체계적으로"[31] 고려하려는 의도는 환영한다. 보다 일반적으로 말해서, 전지구적인 온라인 활동이, 행위에 대한 세세한 규정 대신 기본적인 규범적 원칙에 기초하여, 국제적인 합의가 이루어진 다음에만 적절하게 규제될 수 있다는 몇몇 학자들의 최근의 지적에 동의한다.[32] 그러나 우리는 국제적인 합의가 이뤄지기까지 얼마나 오랜 시간이 걸리는지 알고 있으며, 우리는 조치를 취해야 한다. 그렇지 않으면 말이 달아난 후에 마구간 문을 닫는 우를 범할 수 있다.

Ⅲ. 사물클라우드

앞서 언급한 바와 같이 필자는 사물클라우드,[33] 즉 "클라우드에 의하여 매개되는 사물간 통신을 비롯하여 '사물'과 클라우드 간에 통신이 이루어지는 생태계"[34]를 주 논의대상으로 삼을 것이다. 사물인터넷의 일부가 현재 클라우드 기술에 기초하고 있지는 않으나, 클라우드 기술은 점점 더 보편화되고 있고 주목할 만한 쟁점들을 제기하고 있다.

사물인터넷과 클라우드 컴퓨팅 간의 관계는 지금까지 불명확한 채로 남아 있다.[35] 관련 문헌의 결함은 사물인터넷의 법적 측면에 관한 단행본으로서 현존하는 유일한 서적을 펼쳐보는 순간 명백해진다. 이 책의 저자는 "실세계의 '사물'들과 사물인터넷에서의 이것들의 배치는 클라우드 컴퓨팅에 의해 다뤄지지 않는다"[36]고 주장하는데, 이는 사물인터넷을 가능하게 하는 것이 클라우드라고 단언하는

27) 2015년 11월 25일, '사물간 통신 서비스 상임위원회(Comitato permanente per i servizi di comunicazione Machine to Machine)'가 발족하였다. 그 구성은, Autorità Garante delle Comunicazioni (AGCOM, 통신규제기관), the Autorità per l'energia elettrica, il gas e il sistema idrico (전기, 가스, 물 관할기관), the Autorità di Regolamentazione dei Trasporti (운송 관할기관), the Agenzia per l'Italia Digitale (디지털 의제 담당기관) and the Ministero dello Sviluppo Economico (경제발전부 장관). AGCOM, Delibera n. 459/15/CONS을 참조하라. http://www.agcom.it/documents/10179/2409164/Delibera+459-15-CONS/6c9ac9f2-e46f-4df6-9f25-66205d6b7620?version=1.0에서 이용 가능.

28) 영국정부 과학분야 최고고문은 과학과 기술 관련 활동·정책에 관한 총리와 내각의 고문이다.

29) 영국정부 과학분야 최고고문(GCSA), 「사물인터넷: 제2차 디지털혁명에 대한 최대한의 활용(The Internet of Things: making the most of the Second Digital Revolution)」, 2014.12.18., 9 (Blacket Review로도 알려져 있다).

30) GCSA (29), 9.

31) ibid.

32) C. Reed-D. Stefanatou, 「법과 규제에 관한 최근현황-국제적인 법적 틀에 책임문제를 임베드하기(Legal and Regulatory update – embedding accountability in the international legal framework)」(근간). 원고를 보내준 저자에게 감사의 말을 전한다.

33) '사물클라우드'는 2015년 10월 26-27에 Windsor에서 열린 '마이크로소프트 클라우드컴퓨팅연구센터'의 제2차 연례학술대회에서 그 주제로 다루어졌다. http://cloudofthings.org/를 참조. 또한 사물클라우드 플랫폼은 기업이 자체브랜드의 사물인터넷 솔루션을 개발하는 것을 가능하게 한다(여기에는 종점(endpoint) 장치에 대한 소프트웨어 개발 키트(SDKs), insight-driven 빅데이터 클라우드 백엔드(insight-driven big-data cloud backend), 그리고 모바일 제어 어플리케이션을 위한 소스코드를 자동적으로 생성시키는 엔진이 포함된다. https://www.cloudofthings.com/welcome/을 참조.). 본 논문에서 사물인터넷이라 하고 달리 단서가 붙지 않는 경우, 사물클라우드를 지칭하는 것으로 이해하기 바란다.

34) Hon-Millard-Singh (7), 7.

35) 필자는 A. Botta et al., 「클라우드 컴퓨팅과 사물인터넷의 통합(On the Integration of Cloud Computing and Internet of Things)」(2014 미래 사물인터넷과 클라우드에 관한 국제회의(2014 International Conference on Future Internet of Things and Cloud, Barcelona, 2014.8.27-29., 23.)과 의견을 같이 한다. 이 문헌에서는 사물인터넷과 클라우드를 각각 따로 논의하고 있지만, 새로운 도전과 쟁점의 기초가 되는 기술들(그들은 'CloudIoT'이라 부른다)의 통합에 관해 명확히 해야 할 것이다.

36) R.H. Weber and R. Weber, 「사물인터넷, 법적 관점에서의 고찰(Internet of Things. Legal Perspectives)」, Springer, Heidelberg-Dordrecht-London-New York, 2010, 17.

이들과 모순되는 관점인 것이다.[37] 이 둘 사이에서 절충된 입장이 채택되어야 할 것이다.

여기서 검토되고 있는 기술들 간에는 명백한 연관성이 존재한다: 오늘날 모든 사물인터넷 어플리케이션이 클라우드를 기반으로 하고 있는 것은 아니지만, 클라우드는 더욱더 사물인터넷을 가능하게 하는 당연한 일부로 되고 있다. 이는 무엇보다도 '사물' 간의 매개자이자 조정자로서의 클라우드의 역할 때문이다. 그렇다면 이제 빅데이터,[38] 분석학,[39] 그리고 (클라우드 아웃소싱을 핵심적인 것으로 만드는) '사물'에 탑재된 기능들(정보의 저장, 처리 그리고 배터리)에 대해 생각해봐야 할 것이다. 특히 시스템을 대규모 수준에서 고려할 경우, 클라우드는 '사물'들의 (발전 중에 있는) 사회적 네트워크[40]이자 개방적인 공유[41]의 초석이라는 것이 명백해진다. 뿐만 아니라, 클라우드가 어디에서나 접근 가능하다는 것은 많은 '사물'이 착용되거나 일상생활의 일부가 되어 있다는 것이고, 따라서 이용자(들)[42]이 현재 어느 장소에 있건 서비스와 어플리케이션에 접근할 수 있는 것이 결정적으로 중요하다.[43] 그리고 새로운 클라우드 기술은 매우 획기적인 속도로 가상의 컴퓨터(virtual machine)가 차지하는 공간을 줄이며, 이는 클라우드가 매우 소규모의 '사물'에도 적용되는 것을 가능하게 한다.[44] 다른 최근의 컴퓨팅 패러다임들은 사물클라우드, Cloudlet,[45] 포그 컴퓨팅(fog computing),[46] 그리고

37) Harvard Business Review, 「사물인터넷: 과학소설 혹은 업계의 현실?(Internet of Things: Science Fiction or Business Fact?)」, Harvard Business Review Services Report, 2014, 1. 그러한 요소는 연결성의 급속한 확산 및 센서와 통신 칩의 소형화와 함께 이해되어야 한다.

38) Cf. M. Aazam et al, 「사물클라우드: 사물인터넷과 클라우드 컴퓨팅의 통합 및 관련 쟁점(Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved)」, 2014 (Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th - 18th January, 2014, 414). 여기서는, 사물인터넷이 "고도로 편재함에 따라 이를 클라우드 컴퓨팅과 통합하는 것이 중요해지고 있다. 왜냐하면, 사물인터넷이 생성시킬 수 있는 데이터의 양으로 인하여, 그리고 저장용량 및 가상의 자원의 활용의 특권의 요구 그리고 사물인터넷에 의해 생성되는 데이터를 보다 유용하게 이용하고 이용자를 위한 스마트 어플리케이션을 개발하는 것의 요구로 인한 제약이 존재하기 때문이다."고 지적하고 있다.

39) 예를 들면, 클라우드가 없이는 다수의 센서와 다수의 '사물'로부터 수집된 데이터의 분석이 거의 가능하지 않을 것이다.

40) Cf. L. Atzori et al., 「사회적 사물인터넷 - 소셜네트워크와 사물인터넷의 만남: 개념, 구조 그리고 네트워크(The Social Internet of Things (SIoT) - When social networks meet the Internet of Things: Concept, architecture and network characterization)」, in Computer Networks 56 (2012) 3594 and P. Deshpande et al., M4M. 「사물인터넷에서 소셜네트워크 기초의 공유를 가능하게 하는 모델(A model for enabling social network based sharing in the Internet of Things)」, in 7th International Conference on Communication Systems and Networks (COMSNETS), 6-10.1.2015 Bangalore, India, 미국 전기전자기술자협회(IEEE) Proceedings, 2015. 사물인터넷의 기본 개념에 관해서는 http://www.social-iot.org/를 참조.

41) 이러한 융합의 한 예가 소위 클라우드 생산(cloud manufacturing), 즉 '클라우드가 기초된 기술을 통하여 가치사슬을 가로지르는 혁신과 협업을 위한 제조업의 새로운 방향'이다(Y.-K. Lu-C.-Y. Liu-B.-C. Ju, Cloud Manufacturing Collaboration: An Initial Exploration, 2012 Third World Congress on Software Engineering, Wuhan, 6-8.11.2012, 163).

42) 「Advances in Clouds. Research in Future Cloud Computing」, Commission of the European Communities, Information Society & Media Directorate-General, Software & Service Architectures, Infrastructures and Engineering Unit (edited by L. Schubert and K. Jeffery, 2012, 12.)에 의하면, 이용 가능성, 탄력성 그리고 자원활용의 향상과 함께, 다중이용권은 클라우드 컴퓨팅의 고유한 한 특징이다(http://cordis.europa.eu/fp7/ict/ssai/docs/future-cc-2may-finalreport-experts.pdf에서 이용 가능). 그러나 또한 사물인터넷에 관해서도 이는 더욱더 중요하다.

43) 이에 관한 흥미로운 연구로는, Y. Benazzouz et al., 「클라우드의 장치 Sharing User IoT devices in the Cloud」, 미국 전기전자기술자협회(IEEE), World Forum on Internet of Things (WF-IoT), 2014, 373. 그들은 클라우드 컴퓨팅에 기초한 사물인터넷 중심의 소셜 장치 네트워크를 제안하는데, 그건 바로, 그 탈중심화된 성격, 고도의 신뢰성 그리고 시공간의 제약을 받지 않는 접근성 덕택에 가상 실행 환경이 제공되기 때문이다.

44) Cf. http://unikernel.org/.

45) S. Bouzefrane et al., 「Cloudlets Authentication in NFC-Based Mobile Computing」, in 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)(8-11 April 2014, 268-269.)에 의하면, 이는 "원거리 클라우드 서버에 연결된 공적 인프라에 설치된 멀티코어(multicore) 컴퓨터이다. 따라서, 낮은 수준의 지연과 고(高)대역폭을 유지하는 가운데 cloudlet은 작업량을 절감하기 위하여 모바일 장치에 의하여 이용된다." 이 용어는 M. Satyanarayanan et al.에 의하여 만들어졌다(「모바일 컴퓨팅에서 가상의 사물이 기초가 된 cloudlet에 관한 사례」, IEEE Pervasive Computing 8 (2009), 14-23.). 사물인터넷과 관련하여 cloudlets (또는 edge computing)의 이용에 초점을 맞춘 최근의 연구(가령, M. Satyanarayanan et al., 「Edge Analytics in the Internet of Things」, in IEEE Pervasive Computing, Volume:14 , Issue: 2, Apr.-June 2015, 24-31)는 Giga Sight 구조, 인터넷의 edge에서 비디오 분석을 수행하는(따라서 클라우드로의 진입 대역에 대한 요구를 감소시키는) 가상의 사물이 기초가 된 cloudlet의 연합시스템에 관해 기술하고 있다.

개인 클라우드(personal cloud)[47]의 발달을 예견하게 한다.

사물클라우드가 가지는 이론적 중요성은 예를 들어, 이 주제[48]에 관한(또한 ClouT[49]에 의한) 학회로부터 증명된다. 이 학회는 유럽과 일본의 공동 프로젝트로서, 클라우드 서비스 및 '사물'의 접근과 관리를 가능하게 하는 공동의 가상화(virtualization) 층위를 규정하고 개발하는 것을 목표로 하고 있다. 이와 관련하여 특히, 사물클라우드 인프라는 저렴하고 관리가 용이하고 오픈소스를 기초로 하며 호환 가능하고 다른 플랫폼 및 서비스와 상호정보교환이 가능하다는 것이 증명되었다.[50]

우린 현재 유비쿼터스 컴퓨팅으로부터 유비쿼터스 센싱(sensing)과 유비쿼터스 액츄에이팅(actuating, 기기를 작동하게 하는 것)으로 이행하는 국면에 있다. 대단히 명백하게도, 예를 들어 "클라우드와 사물인터넷을 매끄럽게 통합할 새로운 네트워크 구조, 그리고 사물인터넷으로부터 클라우드로 빅데이터의 연속적 전송을 용이하게 할 프로토콜"[51]의 필요성이 제기되기 때문에 새로운 해결과제가 등장하고 있다. 또한, 클라우드 관련 모든 법적 쟁점이 사물인터넷 관련 맥락에서 등장하거나 사물인터넷 맥락에서 동일한 의미를 가지는 것은 아니다. 보안이 양자의 경우 모두 중요하다는 점을 생각해야 하지만, 클라우드에 대한 해킹이 데이터에 영향을 미치는 데에 그치는 반면[52] (물론 개인정보의 침해가 실질적인 방해행위가 될 수 있기는 하다), 스마트 기기에 접속하여 원격으로 제어하는 것은 시민들의 건강과 삶을 위태롭게 하며 세계에 영향을 미칠 가능성을 가지고 있다.[53] 또한 클라우드는, 특히 그

46) 이 용어는 2012년 Cisco의 연구자들에 의하여 만들어졌다. 특히, F. Bonomi et al., 「포그 컴퓨팅과 사물인터넷에서의 그 역할(Fog Computing and Its Role in the Internet of Things)」, http://conferences.sigcomm.org/sigcomm/2012/paper/mcc/p13.pdf. 이에 따르면, "포그 컴퓨팅은 클라우드 컴퓨팅 패러다임을 네트워크의 끝까지 확장한다. 그럼으로써 새로운 어플리케이션과 서비스가 산출될 수 있도록 한다. 포그의 특징은, a) 짧은 회전 지연(latency)과 무선기기의 위치파악 소요시간, b) 광범위한 지리적 분포, c) 이동성, d) 매우 많은 수의 노드, e) 무선 접근이 지배적인 역할을 함, f) 스트리밍과 실시간 어플리케이션이 큰 비중을 차지, g) 이질적인 여러 종에 의한 구성."

보다 최근의 연구로는, S. Sarkar-S. Chatterjee-S. Misra, 「사물인터넷 맥락에서의 포그 컴퓨팅의 적합성에 평가(Assessment of the Suitability of Fog Computing in the Context of Internet of Things)」, in IEEE Transactions on Cloud Computing, Volume: PP, Issue: 99, 1.10.2015, 1.

실시간 서비스를 요구하는 어플리케이션 수가 증가함에 따라, 포그 컴퓨팅 패러다임이 기존의 클라우드 컴퓨팅을 능가하고 있다(포그 컴퓨팅에서의 전체적인 서비스 지연(latency)이 50.09% 감소했다). 따라서 사물인터넷의 맥락에서, 지연에 민감한 어플리케이션이 큰 비중을 차지하는 까닭에 포그 컴퓨팅이 기존의 클라우드 기술에 비하여 보다 우수한 것으로 되고 있다.

47) 개인 클라우드에 힘입어, '사물' 중심의 모바일 클라우드 컴퓨팅이 이용자 중심의 클라우드 컴퓨팅 경험으로 옮아가고 있다. 이로써 이용자는 원활하게 다수의 '사물'에 대하여 앱을 통하여 자신의 디지털 자산에 접근할 수 있다(A. Kazi-R. Kazi-R. Deters, 「개인 클라우드에 대한 지원(Supporting the personal cloud)」, in 2012 IEEE Asia Pacific Cloud Computing Congress (APCloudCC), 14-17 Nov. 2012, 25-30).

48) 이를테면 세 개의 학회의 결과물인 '미래의 사물인터넷과 클라우드(Future Internet of Things and Cloud)'를 참조하라 (http://www.ficloud.org).

49) http://clout-project.eu/에서 볼 수 있는 것과 같이, 사물클라우드의 전체적인 개념은, 도시를 "보다 스마트하게" 만들기 위하여 그리고 효율적인 에너지 관리, 경제성장과 발전 같은 새로운 과제들을 처리하기 위하여 모든 가능한 정보가 이용되는 효율적인 통신·협업 플랫폼을 구축하고, 클라우드 컴퓨팅을 이용하여 서비스 인터넷을 통해 사물인터넷이 '사람들의 인터넷'과 연결될 수 있도록 하는 것이다(또한, https://vimeo.com/112706883을 참조).

50) 특히, P. Wright-A. Manieri, 「클라우드에서의 사물인터넷. 그 이론과 실무(Internet of Things in the Cloud. Theory and Practice)」, CLOSER 2014, 4th International Conference on Cloud Computing and Services Science, Barcelona, 3-5.4.2014.

51) IEEE, Internet of Things Journal Special Issue on Cloud Computing for IoT.

52) 여기서 '클라우드'는, 사물인터넷 통신의 매개체로서가 아니라, 클라우드 컴퓨팅의 이용 그 자체를 의미한다. 클라우드가 '사물'을 제어하고 있는 경우 – 명령을 통해 직접적으로이건, 실세계의 사물들의 동작들인 '사건'을 기술하는 간접적인 방식에 의한 것이건 – '클라우드에 대한 해킹'이 실세계의 보안에 문제를 일으킬 수 있다는 것은 분명하다.

53) 영국정부 과학분야 최고고문(GCSA)(29)은 두 가지 예를 제시하고 있다: 자동차의 조종과 제동을 제어하는 사이버 공격, 그리고 해커가 baby monitor[아기 상태에 귀 기울이기 위한 무선청취장치]를 이용하여 잠자는 아기에게 고성을 지르는 사례. 그러나 이 외에도 많은 사례들이 존재한다: 가령, 주유소 관련, http://www.theregister.co.uk/2015/02/11/anonymous_hacks_fuel_station_monitoring_system/.

사이버보안에 관한 일반 가이드라인이 나올 때까지 기다려야겠으나, 최근 European Union Agency for Network and Information Security(ENISA)가 사이버 위협으로부터 스마트홈 환경을 안전하게 하기 위한 한 연구를 발표했다. 이 연구는 제품의 라이프사이클의 모든 단계에 적용되는 모범적인 실무 사례를 강조하고 있다. ENISA, 「Security and Resilience of Smart Home Environments」, 2015.12.1., https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/smart

매개자이자 조정자로서의 역할 덕분에, 시스템의 보안을 강화하는 데에도 중요한 역할을 할 수 있다. 사실, 데이터가 클라우드의 승인절차를 거치도록 하면, 클라우드는 악의적인 '사물'의 연결을 끊을 수 있거나 그것의 입력을 차단할 수 있다. 또한 오직 유효한 데이터만이 시스템에 접근할 수 있도록 할 수 있고 그를 통해 데이터의 완전성을 보장할 수 있다.[54]

Ⅳ. 사물클라우드 생태계의 복잡성

필자는 사물클라우드의 복잡성의 요소가 최소 여섯이라고 생각한다. 부문으로의 세분화에 관해서는 이미 언급하였다.

두 번째 요소는 '상호 단절된 영역들의 인터넷(Internet of Silos)'의 문제점으로 표현할 수 있다. 인증(certification) 장치가 발달초기 상태에 있고 공통의 표준과 프로토콜이 부재하기 때문에 상호정보교환(interoperability)을 어렵게 하고 있다.[55] 상호정보교환은 사물클라우드의 핵심적인 측면으로서, 그 본질은 감지(sense)하고 통신하고 기기를 작동시키는(actuating) '사물'들의 시스템을 만들어낸다는 데에 있다. 사물클라우드에서는, 개별 '사물'이 아니라 그 시스템에 주목하여야 한다. '시스템'의 차원은 현재,[56] 클라우드와 달리,[57] 여러 사물클라우드 부문들에서의 각각의 서비스가 상호 단절되어 있기 때문에 온전하게 작동하지 못하고 있다; 그런 이유로 관련 '사물'들과 서비스들 간에 정보가 연결되는 것이 거의 불가능하다. 사물클라우드 시스템들 간의 통신에 유리한 환경을 조성하려는 노력들이 있었음에도 불구하고,[58] 현재 사물클라우드 서비스들을 서드파티(third-party) 형식으로 통합하겠다는 제안은 이루어지지 못하고 있다. 그러나 본 논문에서 필자는 장기적 관점에서, 시스템 간의 통신이 어떠한 장애물도 없이 가능하다는 가정 하에 논의를 진행시킬 것이다.

세 번째로, 기술적인 복잡성의 문제가 있다.[59] 관련 기술들이 일반 시민들에게 알려져 있지 않은 것이 보통이라는 것, 즉 지금은 클라우드 컴퓨팅의 의미가 많은 시민들에게 익숙해졌겠지만 전파식별(RFID), 근거리무선통신(Near-Field Communication, NFC), 또는 저전력 블루투스(Low Energy Bluetooth) 개념 등은 아직 생소할 수 있다는 것이다. 사물클라우드에 대한 인식을 제고하고 그럼으로써 신뢰를 제고하기 위해 교육이 필요하다. 기술적 복잡성은 또한 컴퓨터 과학자와 기술자가 몇몇 기술적 측면 때문에 어려움을 겪고 있다는 것을 의미한다. 예를 들어, 하드웨어 관련 제약(낮은 수준의 인터페이스, 에너지 자율성의 감소, 암호화에서의 어려움), 다중이용권(multi-tenancy; 모든 '사물'은 여러 사람에 의하여 다른 여러 – 상충의 가능성이 있는 – 방식으로 제어될 수 있다), 그리고 시스템 전체의 흐름

-homes/security-resilience-good-practices에서 이용 가능.

54) Singh et al. (6), 1.

55) 예를 들어, K. Kreuzer,「사물인터넷과 스마트홈의 가로 막혀 있는 기술들(Eclipse Technologies for the Internet of Things and the Smart Home)」, 2013.5.12., http://kaikreuzer.blogspot.co.uk/2013/05/eclipse-technologies-for-internet-of.html. 그가 클라우드 관련 사물이라고 부르는 것에 관하여, 그는 "이 가젯(gadget)들은 인터넷에 연결되어 있으나, 이 가젯들은 사실상 상호 연결이 완전히 끊겨 있다."고 강조한다(그러나 그가 사물인터넷을 사물간 통신, 클라우드 관련 사물 그리고 사물인트라넷으로 3분하고 있는 것은 논쟁의 여지가 있다). 또한 다음을 참조, B. Di Martino-G. Cretella-A. Esposito,「다수의 클라우드 간의 어플리케이션의 이식성과 서비스의 상호정보교환에서의 진보(Advances in Applications Portability and Services Interoperability among Multiple Clouds)」, in IEEE Cloud Computing, March/April 2015, 22. 그는 특히, 이식성과 상호정보교환을 위한 즉시 이용 가능한 솔루션의 이용을 제안한다(이름하여, Docker, ElasticBox 그리고 Cloudify).

56) 이는 어디까지나 최근의 기술상황일 뿐이다. 적어도 장기적으로는, 이것이 문제가 되지 않는 시점이 올 것으로 예상할 수 있다.

57) 인터넷의 모든 웹사이트가 연결되어 있고 링크가 가능하다는 것, 그리고 모든 이메일 시스템(웹메일 방식이건, 데스크탑 이메일 클라이언트 방식이건)은 원리상 상호 연동되어 있다는 것을 생각해 보면 바로 이해할 수 있을 것이다.

58) 가령, 전하는 바에 따르면 Google Weave는 한 지역 내에서 그리고 클라우드를 통해서 '사물' 간의 원활하고 보안이 이루어진 통신을 제공한다; 이것은 '사물'의 제조자가 준수해야 하는 인증(certification) 프로그램을 통하여 제조업자(가령, Nest)들 간의 상호정보교환을 추진할 것이다. 보다 자세한 내용은 https://developers.google.com/brillo/?hl=en를 참조.

59) 상호정보교환은 기술적인 문제로 이해될 수 있으나, 그 이상의 것이기도 하다.

(flow)을 통한 데이터 추적의 중요성(따라서 완전성과 유효성을 보장하는 것(가령, IFC, 데이터에 부착된 이용조건(sticky policies) 등))의 측면 등이 있다.

네 번째 요소는 필자가 계약의 수렁(contractual quagmire)이라고 부르는 요소이다. '마이크로소프트 클라우드컴퓨팅연구센터'에서 Ian Walden 교수와 필자는 온도조절장치, 연기탐지기 및 보안 카메라를 공급하는 사물클라우드 회사인 Nest가 소비자에게 제공하는 법적 문서(legals)[60]에 대한 실증적인 연구를 통해, 스마트홈(domotics)에 관해 가능한 시나리오를 연구했다. 이 연구[61]의 결과를 참고하도록 하겠다. 이 연구를 통해 증명된 것의 하나는, 하나의 (단순한) 제품에 대하여 무수히 많은 계약, 허가, 통지 등이 존재한다는 것이다. 이 문서들은 찾아내기 어렵고(인쇄되지 않는 경우도 있다) 이들 문서들을 읽고 종합하여 해석하는 것은 거의 불가능하기 때문에 단일한 수준의 보호를 제공하지 못한다. 뿐만 아니라, 사물클라우드 공급자는 기업의 여러 부서들 그리고 가장 중요하게, 소프트웨어, 하드웨어 그리고 서비스 간의 허위의 구별('사물'은 이 셋의 불가분의 혼합체이다)의 허점을 이용하여 모든 종류의 책임을 회피하려는 경향을 보인다.

다섯 번째는 수많은 규제의 미로라는 요소이다. 수없이 많은 문서들(의견, 지침, communication)이 존재하고 이것들 중 어느 것도 구속력이 없고 전체론적인 접근을 위한 포괄적이고 일관된 구조를 가지고 있지 못하며 부문별 접근을 위한 세밀하고 구체적인 규정으로 구성되지 못하는 것이 일반적이다.[62] 지나치게 많고 지나치게 모호한 것이다.

마지막으로, 하지만 가장 덜 중요한 것은 아닌 요소는 사물클라우드의 행위자들에 관한 것이다. 그들은 누구이고 어떠한 종류의 관계가 그들을 구속하는가? 공급사슬에 관련된 극히 많은 행위자들이 존재하고 그들 간의 관계는 계약적일 수도 있고 비계약적일 수 있다. 사물클라우드 공급사슬을 조명하기 위하여 위에서 설명한 스마트홈 시나리오를 이용하도록 하겠다.

사물인터넷과 사물클라우드에 관한 문헌의 주요 결함의 하나는 모든 것이 '사물'에 관한 것인 것 같은 인상을 받는다는 것이다. 인간이 기술의 중심이라는 것 그리고 기술의 중심에 있어야 한다는 것을

60) 법적 문서(legals)는 '사물'을 구매하는 이들과 관련된 모든 법적인 문서를 말한다.

61) Noto La Diega-Walden (15).

62) 사물클라우드의 단 하나의 부문(의료)에 대한 유럽연합의 문서들 중 주요한 것들만 꼽아 보더라도, Directive 2011/24 on the application of patients' rights in cross-border healthcare; Green Paper on Mobile Health, 10.4.2014 (s. opinions ECOSOC 14.9.2014, CoR 4.12.2014); EDPS, opinion 1/2015 on Mobile Health, 21.5.2015; Comm. Staff WD on the existing EU legal framework applicable to lifestyle and wellbeing apps, 10.4.2014; Council EU, Conclusions on Safe and efficient healthcare through eHealth, 1.12.2009; 29WP, Health data in apps and devices, Annex to the letter to the Commission on 5.2.2015; 29WP, Opinion 3/2012 on developments in biometric technologies, 27.4.2012; 29WP, Working document on biometrics, 1.8.2003; 29WP, Opinion 6/2000 on the Genome Issue, 13.7.2000; Commun. "e-Health Action Plan 2012-2020 - Innovative healthcare for the 21st century", 6.12.2012 (s. Comm. Staff WD 6.12.2012, opinions EDPS 27.3.2013, ECOSOC 22.5.2013 and CoR 3.7.2013); Commun. on telemedicine for the benefit of patients, healthcare systems and society, 4.11.2008 (s. opinion ECOSOC 15.7.2009); Commun. "e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area", 30.4.2004 (s. opinion CoR 17.11.2004); Commission White Paper "Together for Health: A Strategic Approach for the EU 2008-2013", 23.10.2007; Commission Implementing Decision "providing the rules for the establishment, the management and the functioning of the network of national responsible authorities on e-Health", 22.12.2011; Commission Recommendation on cross-border interoperability of electronic health record systems, 2.7.2008; Council conclusions on a safe and efficient healthcare through e-Health, 1.12.2009; Council conclusions on early detection and treatment of communication disorders in children, including the use of e-Health tools and innovative solutions, 2.12.2011; ETSI, Applicability of existing ETSI and ETSI/3GPP deliverables to e-Health, May 2007; ETSI, e-Health; Architecture; Analysis of user service models, technologies and applications supporting e-Health, February 2009; CoR, Opinion "Active ageing: innovation - smart health - better lives", 4.5.2012; eHealth Network, Guidelines on ePrescriptions dataset for electronic exchange, 18.11.2014; eHealth Network, Guidelines on minimum/non-exhaustive patient summary dataset for electronic exchange, 19.11.2013; European Commission Decision C (2015)6776, Horizon 2020 Work Programme 2016 - 2017.8. Health, demographic change and well-being 13.10.2015.

잊은 것이다. 따라서 주요한 정보주체(이들은 때로 정보의 통제권자이기도 하다)인 최종 이용자(사물클라우드-의료의 이용 사례의 경우, 환자)로부터 시작하도록 하자. 최종 이용자는 곧 최종 이용자들이다. 이는 주로 두 가지 요인 때문이다. 첫째는 클라우드 컴퓨팅과 사물인터넷 양자의 중요한 특징인 다중이용권(multi-tenancy). 사실, '사물'의 최종 이용자는 가족구성원, 손님, 친구, 직원 등이 될 수 있다.[63] 그런데 '사물'에 서로 충돌하는 정보가 입력되어 피해가 발생하는 경우 문제가 발생할 수 있다. 두 번째 요인은, 우리 각자는 '사물'을 소유할 수도 있지만 또한 이용권자일 수도 있다는 점이다. 소유자와 이용권자 간의 차이는 또한 실제에서도 어떤 결과를 가져올 수 있다. 영국 계약법에서, 상품의 (이용권자가 아니라) 구매자는 "방해 받지 않고 소유물을 향유할"[64] 권리를 가진다는 내용의 계약조건이 법률의 해석상 인정되는데, 만일 '사물'이 연결되지 않거나 상품의 기능 일부가 작동하지 않는다면 이러한 계약조건이 침해되었다고 볼 수 있게 된다.[65]

최종 이용자가 공급사슬에서 실질적인 권능을 가지지 못하는 경우, '사물'의 제조자와 관련하여 상황은 달라지게 된다. 여기서도 역시 보다 적절히 표현하자면 제조자들이라고 해야겠다. 위에서 언급하였듯이, 대부분의 '사물'은 합성물이기 때문에, '사물'을 구성하는 '사물'에 대해 여러 다른 제조자가 책임을 진다. 설령 단순하게 하나의 '사물'이 존재하는 경우에도 제조과정에서 부품을 제공하고 생산공정을 용이하게 하는 등 여러 사람들이 관련된다.

신규업체와 중소기업이 일부 사물클라우드 분야에서 결정적인 역할을 할 수도 있겠지만, 하드웨어 요소가 포함된 제품을 생산하는 것은 소규모 기업이 감당할 수 없는 비용을 발생시킬 수 있다는 것이 명백하다. 어쨌건 이를 통해 IT 초국적 기업들이 사물클라우드를 어떻게 지배하고 있는지를 알 수 있다. 이는 관련 공급사슬에 적어도 두 가지 효과를 가져온다. 첫째, 고객의 입장에서는 관련 기업들의 구조가 어떠한지 이해하기 어려운 것이 보통이다. 한 예로, Nest가 구글에 의해 인수된 다음, Calico, Google Capital, Google Fiber, Google Life Sciences, Google Ventures, 그리고 Google X (이들 역시 그들의 자회사를 가지고 있다)를 지배하는 다국적 거대복합기업인 Alphabet의 일부가 되었다. Nest는 Nest (Europe) Ltd.를 지배하고, 최근 Dropcam Inc.를 인수하였다. 고객은 자신이 계약을 체결하는 상대방 당사자(또는 당사자들)의 정체를 이해하는 것이 항상 쉽지는 않은 것이다.

둘째, 소비자법과 경쟁법은 기업의 수직적 기업결합 계약을 긍정하는 방향으로 진화해 왔다. 이 법제도들에서 판매 전 단계와 판매 후 단계의 서비스가 중시되었던 것이 그 주된 이유였다. 그런 까닭에, 다수의 사물클라우드 기업이 재판매업 회사, 소매업 회사, 도매 유통회사 그리고 설치업 회사를 그 밑에 두고 있는 것이 놀랍지가 않은 것이다.

사물클라우드는 하드웨어 및 소프트웨어와만 관련되는 것이 아니며 서비스와도 관련된다.[66] 어느

63) 그와 별개의 쟁점이 '사물'을 계약체결에 이용하는 것이다. '사물'을 판매하는 '사물' 그리고 자기 스스로를 판매하는 '사물'에 관하여는, Hon-Millard-Singh (7), 12-13. 인공지능에 관하여 변호사들의 이목을 끄는 주제의 하나는 기계로 변호사를 대체할 수 있는가 하는 문제인 것으로 보인다(변호사들은 협상이 가지는 성격 때문에 그것이 불가능하다고 주장한다). 인공지능이 법에 대해 미치는 영향에 관한 보다 흥미로운 측면들은 완전히 자율적인 시스템에 의한 계약체결 문제(그러한 계약체결이 자연인 또는 법인을 구속할 수 있는가?), 그리고 자율적으로 수행된 행위에 대한 법적 책임의 문제(간단히 표현해서, 현재로서는 로봇을 체포한다는 것이 제 정신이 아닌 소리로 들리겠지만, 앞서 언급한 인공기능향상에 의해 향상되고 '사물'이 이식된 인간과 자율적인 '사물' 간의 수렴현상이 일어나게 되면 그때는 결론이 그와 같지 않을 것이다)를 제기한다.

64) E.g. UK, Sale of Goods Act 1979, s. 12(2)(b).

65) Rubicon Computer Systems Ltd. v United Paints Ltd (2000) 2 T.C.L.R. 453. Noto La Diega-Walden (15), 6은 이를 "연결이 끊긴 사물인터넷장치 쟁점"이라고 하고 있다. 우리는 흥미로운 또 다른 쟁점은 거론하지 않았다. 즉, 연결로부터 해제될 권리. 모든 사물이 연결되어 있고 사적인 '사물'이, 공적인 '사물'의 데이터 흐름과 동작에 필연적으로 간섭하는 데이터 흐름과 동작을 생성시키는 사회를 상상해보라. 그러한 사회의 경우, 시민들은 그러한 종류의 결정이 가지는 축척효과(scale effect)에 불구하고 연결로부터 해제될 권리를 주장할 수 있을까?

66) In Noto La Diega-Walden (15), 11. 우리는 '사물'이 하드웨어, 소프트웨어, 그리고 서비스의 불가분의 혼합체라고 주장한다.

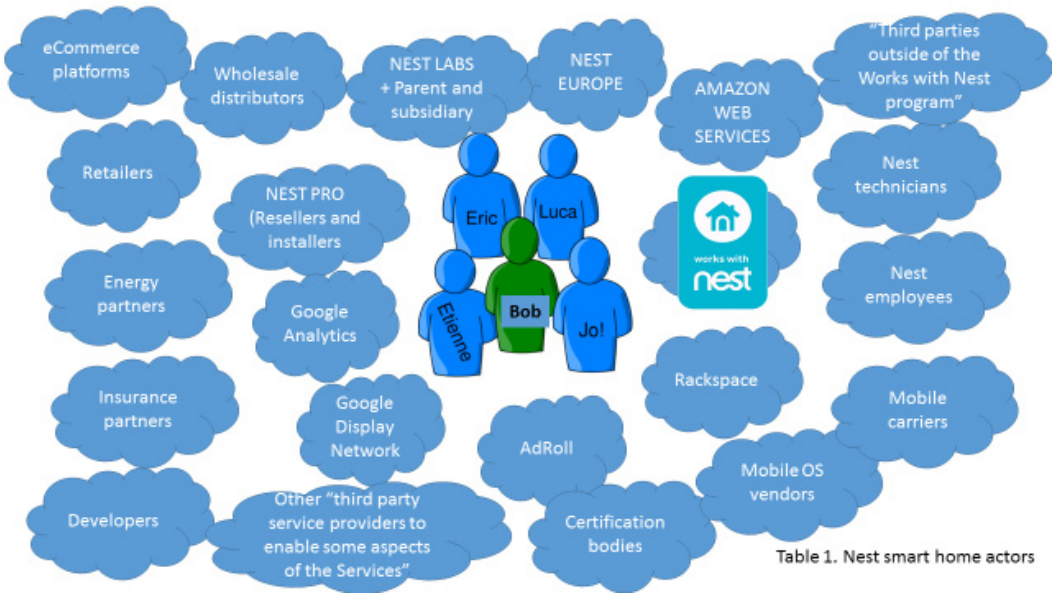

Table 1. Nest smart home actors

한 클라우드 공급자를 웹을 저장하는 데에 이용하고 다른 공급자를 redundancy (중복적 여분)를 위해 쓸 수 있다. 또한 빅데이터에 필수적인 분석도구(analytics tool), 온라인 지급서비스 공급자 그리고 광고서비스 공급자 등도 있다. 주된 서비스(Nest의 경우 스마트 열 탐지, 연기 탐지)와 함께, 사물클라우드 공급자는 부수적인 서비스를 제공하는 다른 기업들과 협력한다. 예를 들어 Nest는 '안전 보상(Safety Rewards)' 서비스에 관하여 보험회사와 협력하고[67] '러시아워 보상(Rush Hour Rewards)'과 '계절별 절약(Seasonal Savings)'에 관하여 에너지 공급업체와 협력한다.[68]

공급사슬에 대한 전체적인 그림을 완성하려면, 웹사이트 개발자와 웹마스터, '앱' 스토어, 임베디드 소프트웨어 개발자, 소프트웨어 공급자, '사물' 간의 통신을 용이하게 하는 서비스업자, 법적 권리의 보유자, 전자상거래 플랫폼, 그리고 네트워크 운영자 역시 언급해야 한다.

그러나 사물클라우드는 단일한 '사물'에 관한 것이 아니다. 사물클라우드는 시스템, '사물'들의 네트워크, 그리고 시스템 내에서의 통신 및 하위 시스템 간의 통신에 관한 것이다. 따라서 위에서 열거된 행위자들의 수(數)에다, 상호정보교환이 가능한 앱과 '사물'의 상응하는 행위자의 수를 곱해야 한다. (정보보호뿐 아니라 또 다른 목적들과 관련하여) 법적 책임의 분배 문제를 차치하더라도, 관련 행위자 전부를 인식하는 것은 쉽지 않다.

공급사슬은 의료서비스 분야에서 훨씬 더 복잡하다. 위의 연산에 의해 산출되는 숫자에, 다음을 추가해야 한다. 즉, 의사(내과의사, 외과의사, 물리치료사 등, 그리고 팀), 국민건강보험, 병원(특히 병원 관리자들), 지역 보건의(保健醫) 서비스, 간호사, 기타 직원들(예를 들어, 응급실), 연구원, 약국, 제약회사, 간병인, 데이터처리 전문가, 사회보장 담당자, 환자의 가족과 친구, 생체의학 연구소, 방사선센터, 기타 전문 클리닉, 연구소 기술자, 의료용 가스 회사, 기타 보조적 서비스, 책임의료조직

67) Nest는 연기탐지기가 설치되어 있고 작동하고 있다는 것을 보험회사가 알도록 할 것이다. 그와 교환으로, 보험회사는 보험료의 5%를 떼어 갈 것이다.

68) 이 서비스들은 기계학습(machine learning) 기술(소위 'Auto-Tune')에 기초하고 있다. 이로부터 클라우드 컴퓨팅의 이용이 가능해진다('Auto-Tune'은 거대한 양의 메모리, 기억장치 그리고 처리능력(이들은 모두 클라우드에서 유지관리된다)을 필요로 한다," https://nest.com/support/article/What-is-Auto-Tune). 인공지능과 기계학습으로부터 제기되는 법적 책임의 문제는 본 논문의 범위를 벗어나는 것이다.

(Accountable Care Organization, ACO), 의료정보 교환(health information exchange, HIE), 지역의료 정보조직(regional health information organizations, RHIO), 기타 간병 관련 단체, 의료기기 공급자, 의약품 등. 아마도 몇몇 행위자를 빠뜨렸을 것이다.

환경의 이러한 복잡성은, 사물클라우드에 대한 시민의 신뢰를 쌓기 위해 필수적인 투명성과 책임 소재파악에 도움이 되지 않는다. 정부와 민간의 관계자들은 계약과 관련 규칙을 간단하게 만들기 위해 그리고 상호 정보교환과 보안을 보장하는 기준과 프로토콜을 개발하기 위해 협력해야 한다.

Ⅴ. 영국에서의 발달현황과 규제

사물클라우드는 영국에서 이미 가시화된 현실이다. 현재 영국에는 4천만 개 이상의 사물인터넷 장치가 이용되고 있다. 한 연구[69]에 의하면, 이 숫자는 2022년에 8배로 늘어나 3억 2천만 개의 사물인터넷 장치가 이용될 것으로 전망되며 매일 10억 개 이상의 데이터 transaction이 이루어질 것으로 예측된다.

그 주요한 예는 2020년 말, 약 5천 3백만의 "스마트" 미터가 영국의 모든 가정에서 이용될 것이라는 점이다.[70] 정부는 설치 중 판매를 금지함으로써, 그리고 방문 시 에너지효율성에 관한 조언을 제공하도록 함으로써, 그리고 만약 그 회사의 제품에 관해 홍보하려 한다면 미리 소비자의 허락을 받도록 함으로써 소비자를 보호하고자 한다. 프라이버시와 관련하여서는, 공급자는 30분 간격의 데이터(half-hourly data)에 접근하거나 마케팅 목적으로 데이터를 이용하기 위해서는 소비자의 동의를 받도록 하고 있다. 그러나 일일의 데이터(daily data)는 명시적인 반대의사가 표시되지 않는 한 접근할 수 있게 되어 있다.

영국의 사물인터넷은 상당한 공적인 투자 덕택에 본격적인 성장의 궤도에 접어 들었다. 2015년 7월 8일 통과된 영국의 하계(夏季)예산에서, 영국은 사물인터넷에 4천만 파운드를 쏟아부을 것으로 예상되며, 그 초점은 의료, 사회복지 그리고 스마트 도시에 놓일 것이다. 이를 실행하는 주요한 부분의 하나가 IoTUK [IoT+UK][71]라는 프로그램이다. 그리고 "인프라와 미래도시"를 위해 1억 4천만 파운드, "intelligent mobility"에 1억 파운드가 투입될 계획이다. 전체 2억 8천만 파운드(4억 2천 1백만 달러)에 이르는 중요한 재정적 투자인 것이다. 보다 최근에는, Ofgem (에너지 부문에 관한 영국의 규제기관)이 소비자를 위한 보다 더 스마트한 에너지 네트워크를 위해 6280만 파운드를 투입하겠다고 발표했다.[72]

하노버에서 열린 2014년 CeBIT박람회에서 수상은 영국정부 과학분야 최고고문(GCSA)에 대해 영국이 사물인터넷의 잠재력을 어떻게 활용할 수 있을지 검토해보도록 지시했다. 고문단, 여러 세미나 그리고 학계・산업계・정부의 120명 이상의 전문

69) Aegis Systems Ltd-Machina Research, 「사물간 통신 어플리케이션의 특징과 주파수대에 대한 영향, 최종보고서(M2M application characteristics and their implications for spectrum. Final report)」, 2606/OM2M/FR/V2, 2014.5.13., http://stakeholders.ofcom.org.uk/binaries/research/technology-research/2014/M2M_FinalReportApril2014.pdf에서 이용 가능. 이 보고서는 Ofcom으로부터 위임 받아 작성된 것이다.

70) 다음을 참조. Department of Energy and Climate Change, 「Smart meters: a guide」, 22.1.2013 (2013.10.8. 마지막 업데이트), https://www.gov.uk/guidance/smart-meters-how-they-work. The number is potential, given the opt-in system chosen by the Government. See also Department of Energy & Climate Change-Ofgem (Office of Gas and Electricity Markets, UK regulator of energy), 「Smart meters: information for industry and other stakeholders」, 22.1.2013, available at https://www.gov.uk/guidance/smart-meters-information-for-industry-and-other-stakeholders.

71) IoTUK 프로그램은 지도적인 성격의 협업적인 3개년 프로그램으로서, 사물인터넷에서의 영국의 역량을 최대화하기 위한 정부의 4천만 파운드 투자계획의 일부를 이루고 있다. Digital Catapult and the Future Cities Catapult에 힘입어, IoTUK는 산업계와 공공부문에서 높은 수준의 사물인터넷 기술과 서비스가 보다 많이 채택되도록 하고 있다. 관련 조직들에는 city demonstrator, 보안과 신뢰에 초점이 맞춰진 연구 허브(hub), a hardware accelerator, 그리고 의료 test bed[신기술의 성능시험 환경]이 포함된다. 보다 자세한 것은 http://iotuk.org.uk/about-us/을 참조.

72) 이 발표는 2015년 11월 3일에 이루어졌다(https://www.ofgem.gov.uk/publications-and-updates/ofgem-announces-62-8-million-deliver-smarter-energy-network-consumers을 참조.).

가의 참여를 통해 "사물인터넷: 두 번째 디지털 혁명의 최대활용검토서"(또한 'Blackett Review'라고도 불린다)[73]를 2014년 12월 18일 내놓았다. 이 검토서는 다섯 개 부문(운송, 에너지, 의료, 농업, 건축물)이 포괄되어 있고 세 개의 주요 목표를 설정하고 있다. 그 첫째는 사물인터넷의 잠재적인 경제적 가치의 실현을 위해 정부가 무엇을 지원할 것인가 하는 것이다. 둘째는 사물인터넷 어플리케이션이 정부의 사업 – 인프라 유지관리, 공적 서비스의 제공 및 시민의 보호 –을 향상시키기 위하여 할 수 있는 것을 제시하는 것이다. 셋째는 이러한 자료들로부터 권고사항을 제시하는 것이다. 영국정부 과학분야 최고고문은 리더십, 주파수대와 네트워크, 표준, 기술과 연구, 데이터, 규제와 입법, 신뢰, 그리고 조정에 관하여 열 가지 조치를 권고하고 있다.

이러한 와중에 2014년 7월 24일, 영국의 통신규제기관인 통신국(Office of Communications, Ofcom)은 "사물인터넷에 대한 투자와 혁신의 촉진"[74]이라는 보고서에서 정보·의견의 제공을 요청하였다. 이를 통해 사물인터넷에서의 투자와 혁신과 관련하여, 있을 수 있는 장애물(그리고 규제기관의 역할)을 확인하고자 하였다. "응답과 이후 단계에 대한 개요"[75]가 2015년 1월 27일 제출되었고 네트워크 어드레싱(network addressing), 주파수대, 네트워크 보안과 resilience, 프라이버시와 정보보호가 다루어졌다(여기서 그 이해관계자들은 뒤로 갈수록 그 중요도가 높아진다). 다음 절에서는 영국에서의 사물인터넷 프라이버시, 정보보호, 그리고 소비자법의 전체적인 그림을 제시하기 위하여 이를 활용하도록 하겠다. 본 절에서는 그 외의 다른 측면들에 대해 간략하게 설명하기로 한다.

당연하게도, 전화번호가 "대부분의 사물인터넷 서비스에 요구되지는 않을 것"인 것과 마찬가지로 네트워크 어드레싱이 대단히 중요한 것은 아니다. 그러나 Ofcom은 IPv4 망에서 IPv6 망으로 전환시킬 때 인터넷서비스제공자의 진행상황을 모니터링 할 것이다.

주파수대와 관련하여, 현재의 모바일 주파수대역에 대한 허가조건을 완화하는 것과 같은 계획들이 진행 중에 있다. 그러나 이것들이 주파수대에 관한 실제의 요구를 충족시킨다 하더라도 장기적으로는 그렇게 되지 않을 수 있다. 최근 Ofcom이 "사물인터넷을 위한 보다 확대된 무선 주파수대"[76]라는 보고서에서 자문을 제공했었다는 점을 지적하고 싶다(2015년 11월 12일 마무리된 이 보고서는 아직 미발간 상태이다). 그 목표는 사물간 통신 어플리케이션이, 보다 먼 거리에서도 무선으로 연결될 수 있게 하는 주파수대를 이용하도록 촉진하기 위한 것이다. 이러한 초단파(VHF) 스펙트럼은 사물인터넷에 이미 이용 중인 다른 주파수들과 다른 속성을 가지는데, 다른 주파수들이 도달하지 못할 수 있는 원거리 지역까지 도달할 수 있다.

컴퓨팅이 유비쿼터스해지고 빅데이터와 함께 결합되면서, 네트워크 보안과 resilience가 대단히 중요하다는 점에 대해서는 전혀 놀라울 것이 없다. Ofcom은 사물인터넷 데이터의 전송에 사용되는 네트워크의 resilience 그리고 '사물'에 의해 수집되는 데이터의 안전한 저장과 처리에 이용되는 방식과 관련하여 점점 더 강한 요구를 내놓고 있다. 사이버보안에 관하여, 유럽연합 집행위원회는 단일디지털시장(Digital Single Market) 전략[77]에 기초하여 온라인 네트워크 보안을 위한 기술과 솔루션 분야에서 사이버보안 정부-민간 파트너십을 구축할 예정이다. 또한 특히 중요한 것으로 보이는 기술과 영역에 초점을 맞춘 가운데 표준화와 관련하여 핵

73) 영국정부 과학분야 최고고문(GCSA)(29).

74) 텍스트 전체는 http://stakeholders.ofcom.org.uk/binaries/consultations/iot/summary/iot-cfi.pdf에서 볼 수 있다.

75) 이 응답의 요약본은 http://stakeholders.ofcom.org.uk/binaries/consultations/iot/statement/IoTStatement.pdf에서 이용 가능.

76) 이 자문의 전체 텍스트는 http://stakeholders.ofcom.org.uk/binaries/consultations/radio-spectrum-internet-of-things/summary/more_radio_spectrum_internet_of_things.pdf에서 이용 가능.

77) 유럽연합 집행위원회, 커뮤니케이션(communication) "유럽의 디지털 단일시장 전략(A Digital Single Market Strategy for Europe)", COM (2015) 192 final, 2015.5.6. 발표.

심 우선사항들을 선별하고 규정하기 위하여 통합된 표준화계획이 진행될 것이다.

정보보호와 소비자법에 대한 상론에 앞서, 전체로서의 사물인터넷에 관한 법적 문서들과 함께, 부문별 문서들(가령, ICO에서 발간된 전파식별(RFID)에 관한 안내서[78]와 스마트에너지규칙(Smart Energy Code)[79]) 그리고 소비자 관련 문서들(가령, 소비자권리법(Consumer Rights Act 2015)) 역시 존재한다는 것을 지적해야겠다. 후자(後者)가 비록 사물인터넷에 국한된 내용은 아니지만, 거기에서는 새로운 시장의 현실이 반영되어 있고 소비자를 위한 흥미로운 수단들을 언급하고 있으므로 이하의 분석에서 고려하기로 한다.

Ⅵ. 정보보호와 프라이버시

사물클라우드와 관련하여, 정보보호와 프라이버시가 중요 쟁점으로 부상하고 있다(놀랍게도, 보안문제는 별로 주목 받지 못하고 있다). 이는 주로 네 가지 요인으로부터 비롯한다. 첫째, '사물'은 개인의 신체 또는 사적인 영역과 관계되어 있을 수 있기 때문에(그래서 공적인 주체와 법집행기관이 접근 불가능한 정보를 수집할 수 있다), 처리되는 데이터가 거의 언제나 개인정보에 해당할 수 있다. 둘째, '사물'은 극히 많은 양의 데이터(소위 빅데이터)를 처리한다. 셋째, '사물'은 다른 '사물'들, 시스템들, 사람들과 지속적으로 통신할 수 있는 잠재력을 가지고 있다. 그런 까닭에 "가장 약한 고리"의 문제와 재조합(recombination)(가령, 장치 간 식별[80] 및 IPv6의 채택[81])의 문제가 대두된다. 마지막으로, 감시 관련 문제가 중대 현안으로 떠오르고 있다. 그 한 예가 Schrems 결정이다. 이 결정에서 유럽사법재판소는, Snowden사건[82], '승객성명기록(Passenger Name Record)[83]'의 이용에 관한 유럽연합지침안(案), 영국의 조사권 관련 입법초안[84] 그리고 영국 경찰청의 '자동차번호판 감지(automatic

78) ICO, 「Data Protection Technical Guidance Radio Frequency Identification」, 9.8.2006, https://ico.org.uk/media/for-organisations/documents/1590/radio_frequency_indentification_tech_guidance.pdf에서 이용 가능.

79) The Smart Energy Code (SEC)는 Data Communication Company's (DCC) 허가가 부여된 2013년 9월 23일 발효하였다(영국정부가 스마트 미터(smart meter) 계획에 착수하였을 때, 그들은 공급자와 다른 당사자들과 소비자의 활동장소의 스마트 미터 간의 통신과 관련된 새로운 허가 가능한 행위를 도입하였다). SEC는 DCC의 서비스 공급 조건을 제시한 다자간 계약으로서, 가스와 전기의 스마트 미터 측정을 단 대 단(end-to-end) 방식으로 관리하기 위한 규정을 두고 있다. SEC의 규정을 새롭게 만들기 위한 자문이 진행 중이다. Ofgem의 반응은 https://www.ofgem.gov.uk/publications-and-updates/ofgem-s-response-department-energy-and-climate-change-s-july-2015-consultation-new-smart-energy-code-content-and-related-supply-licence-amendments을 참조.

80) 일정 장치들을 은밀하게 추적하기 위하여 고주파 sound를 이용하는 것에 관하여는, C. Calabrese et al., 「Comments for November 2015 Workshop on Cross-Device Tracking」, Letter of the Center for Democracy & Technology to the Federal Trade Commission, 16.10.2015, available at https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf.

81) IPv4와 달리, IPv6 덕분에 모든 '사물'의 식별이 가능해질 것이고 그로 인하여 개인정보로서의 성격을 가질 것이다.

82) Judgment of the Court (Grand Chamber) of 6.10.2015, C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650. 위 법원은 미국이 유럽시민의 개인정보에 대하여 적절한 수준의 보호를 제공하지 못한다고 판결하였다.

83) Proposal for a Directive of the Council and the European Parliament on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, ST 14024 2015 INIT - 2011/023 (OLP). 2015년 12월 4일, 합의가 이루어졌다. PNR 시스템을 통해 승객 정보(성명, 연락처, 신용카드)에 대해 접근할 수 있다. 유럽연합으로 들어오거나 그로부터 떠나는 항공편 그리고 회원국 간의 항공편으로부터 정보가 수집된다. EU 프라이버시 규제기관인 '유럽정보보호감독관(European Data Protection Supervisor)'에 따르면, 이는 "유럽연합 역사에서 첫 번째로 이루어지는 대규모의 무차별적인 개인정보 수집"에 해당한다(N. Nielsen, EU counter-terror bill is 'indiscriminate' data sweep, in EuObserver, 9.12.2015, https://euobserver.com/justice/131457에서 이용 가능). EDPS, Opinion 5/2015, 「Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime」(2015.9.24.)을 참조. 특히, "한정된 목표특정 없이 대량으로 정보를 수집하고 처리하는 것은 일반적인 감시조치와 같은 것"이라고 지적하고 있다(par. 63).

84) Draft Investigatory Powers Bill, November 2015. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf을 참조. 특히 파리에 대한 ISIL의 공격 이후 다른 국가들에서도 유사한 법이 제정되고 있다.

number plate recognition)' 시스템 이후, Safe Harbour 협정을 무효로 선언했다. 이는 "세계에서 가장 대규모의 감시시스템 가운데 하나에 해당한다."[85] 감시의 증가는 테러방지와 관련된 것이라고 주장되고 있다. 실제로 유럽연합의 법과 정책에 관한 239개의 문서가 2001년에서 2013년 사이에 테러방지라는 명목 하에 채택되었다. 그중 88개는 법적 구속력이 있는 것이다.[86]

유럽은 이러한 문제들을 인식하고 있다. 예를 들어, 2016년 4월 27일 '일반정보보호규칙(General Data Protection Regulation)'이 채택되었다. 이 문서의 Recital 30 이하에서는, "자연인은 그의 장치, 어플리케이션, 인터넷 프로토콜 주소, 쿠키 식별자 또는 기타의 식별자(가령, RFID 태그)에 의해 제공되는 온라인 식별자에 의하여 식별당할 수 있다. 특히 독특한 식별자 및 서버가 수신한 다른 정보와 결합되는 경우, 개인에 대한 profiling과 개인을 식별하는 데에 이용될 수 있다.[87]

이에 대한 우려를 최소화하기 위해 무엇보다 필요한 것은 데이터 전송・저장 시 암호화되도록 하는 것이다. 사실 '사물'의 전력량 제한을 감안할 때 암호화에 에너지가 많이 소모되기 때문에 이를 피해야 되지 않겠느냐고 생각할 수도 있겠다. 그러나 몇몇 연구들에 따르면, AES (Advanced Encryption Standard, 고급[개량]암호표준) 알고리즘을 사용할 경우 에너지를 많이 소모하기보다는 오히려 절약할 수 있다.[88]

그리고 '사물'의 내부요소에 대한 보안을 위해 '사물'의 내부를, 그리고 모든 통신에 대한 보안을 위해 '사물'의 외부에 주목해야 한다. 새로운 인증(authentication)방식, 가령 多요소(multi-factor)에 의한 방식 같은 것이 극히 중요하다.[89] 시스템의 보안은 시스템을 폐쇄된 방식으로 운용하라는 것이 아니다. 개방성이 일정 정도 외부 공격에의 취약성으로 연결되는 것이 사실이기는 하다. 그러나 이는 다른 방식으로 처리될 수 있고 어쨌건 시스템의 폐쇄적 운용(즉 정보의 상호교환(interoperability)을 방해하는 것)은 '상호 단절된 영역들의 인터넷(Internet of Silos)'을 만들어내는 것(즉, 강화하는 것)과 같다.

또한, 기업들은 정보가 제3자에게 팔려 나가지 않도록 하기 위해 그 직원이 기밀유지계약에 구속되게 해야 한다.

사물인터넷에 관한 Ofcom의 보고서는 정보보호와 프라이버시와 관련하여 만족스럽지 못한 상황이다. 사물인터넷이 개인정보의 처리와 관계되는 한, 이는 정보보호법(Data Protection Act 1998)에 의해 규제될 것이다. 다른 한편, 어떠한 조건 하에서 데이터가 (타인과 공유하거나 타인이 이용하는) '사물'에 의해 수집되는가를 소비자가 쉽고 투명하게 허락할 수 있게 하는 공동의 틀의 도입이 요청

85) 영국의 감시카메라 관련 위원에 따르면, 이는 아무런 적절한 법적 규제를 없이 일어나고 있다(http://www.v3.co.uk/v3-uk/news/2437161/uk-number-plate-monitoring-one-of-the-worlds-biggest-surveillance-systems).

86) B. Hayes-C. Jones, 「Report on how the EU assesses the impact, legitimacy and effectiveness of its counterterrorism laws」, Statewatch SECILE report, December 2013, 28, available at http://www.statewatch.org/news/2013/dec/secile-how-does-the-EU-assess-its-counter-terrorism-law.pdf에서 이용 가능. 특히, "다른 이해관계자들에 비하여 법집행기관과 보안 관련 기관의 요구에 보다 큰 비중이 두어졌던 것으로 보인다."고 지적하고 있다.

87) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

88) Cf. F. Rao-J. Tan, 「Energy consumption research of AES encryption algorithm in ZigBee」, in International Conference on Cyberspace Technology (CCT 2014), 8-10 Nov. 2014, Beijing, 1-6. 향상된 AES 알고리즘이 코드의 크기를 줄일 뿐 아니라 ZigBee 네트워크의 전체적인 에너지 소모량 역시 감소시킨다는 점을 보여주고 있다.

89) 2-요소 방식의 인증(authentication)은 점점 더 불충분한 것이 될 것이다. 예를 들면, 안드로이드 휴대폰을 공격하는 악성소프트웨어(malware)는 수신되는 문자 메시지를 가로챌 수 있고, 그럼으로써 흔히 은행이 2-요소 인증의 한 형태로 고객에게 보내는 일회용 비밀번호를 훔치는 것을 가능하게 한다. 「Consumer advisory on malware targeting mobile banking」(2015.12.1.)(http://www.abs.org.sg/pdfs/Newsroom/PressReleases/2015/MediaRelease_20151201.pdf)을 참조. 그리고 E.J. Kennedy-C. Millard, 「Data Security and Multi-Factor Authentication: Analysis of Requirements Under EU Law and in Selected EU Member States」, Queen Mary School of Law Legal Studies Research Paper No. 194/2015 (2015.4.30.)(http://ssrn.com/abstract=2600795)과 비교.

된다. 사실, 처리의 조건과 목적에 관해 투명성이 결여되어 있다. 구글플레이 스토어에서의 앱에 대한 동의에 관한 최근의 한 연구[90]에 의하면, 앱들은 스마트폰 이용자로부터 235개의 다른 종류의 동의를 구할 수 있는 것으로 나타났다. 소비자들은 이러한 문제에 대해 우려하고 있으며, 그 결과 전체 스마트폰 이용자 가운데 앱을 다운로드한 이용자의 60%가, 앱을 이용하기 위하여 얼마나 많은 개인정보가 요구되는가를 확인한 뒤 설치되지 않았던 것으로 밝혀졌다.

ICO가 특별(ad-hoc)안내지침을 발표하지는 않았으나, 2014년 10월 1일자 Ofcom의 자문에 대한 응답에는 여러 유용한 내용이 포함되어 있다.

영국에서의 규칙은, '사물'로부터 정보를 수집하는 주체에 의하여 특정 개인이 식별되지 않는 한(또는 식별이 합리적으로 가능한 수준이 아닌 한), 당해 정보는 개인정보로 간주되지 않는다. 필자는 여기에, 다중이용권이 클라우드와 사물인터넷 양자의 특징으로 자리잡고 있는 만큼, 개인은 '사물'이 실제로 누구에 의해 사용되는가를 항상 알 수는 없다는 점을 덧붙여야겠다. 그럼에도 불구하고, 시스템의 모든 '사물'에 의해 생산되는 데이터의 재조합의 결과, 추론에 의한 데이터의 중요성이 더해간다는 것 또한 사실이다.

정보보호법은 '사물'에서의 모든 처리에 대해 적용되지는 않는다. 그러나 개인적인 '사물'과 덜 개인적인 '사물'로 구분한 ICO의 분류에 대해 전적으로 찬성하지는 않는다. 스마트폰이 그 전형이라고 할 수 있는 전자(前者)의 경우 그로부터 생산되는 데이터는 그 수집 주체가 데이터 컨트롤러(controller)이기 때문에 정보보호법의 규제 하에 놓인다. 반면, 비개인적인 '사물'(가령, TV)은 그 정보 처리에 대해 정보보호법의 적용을 받지 않는다.

사실, 사물인터넷으로 인하여 데이터 컨트롤러와 데이터 처리자의 역할이 역동적으로 변하고 따라서 누가 컨트롤러인가를 파악하는 것이 불가능한 경우가 빈번히 발생한다(물론 정보흐름제어(information flow control)와 같은 도구가 도움이 될 수는 있겠지만). 더군다나, 용도변경의 문제도 있다. 따라서 TV는 개인정보를 처리하지 않도록 설계될 수도 있으나, 개인정보(심지어 민감한 정보, 가령 건강 관련)에 대한 처리를 중지하도록 하는 것 역시 가능하다.

여하튼 정보보호법이 적용되지 않는 부분에 대해, ICO는 산업실무수칙 또는 기타의 연성법 수단의 도입을 제안한다. 특정 부문에 관한 것이지만 흥미로운 보기로서, 모바일 의료(mHealth) 어플리케이션과 관련하여 프라이버시에 대한 실무수칙 초안(Draft Code of Conduct)[91]을 들 수 있다.

바람직하게도, ICO가 강조하는 한 측면은 '사물'이 개인과 상호작용할 수 있는 물리적 인터페이스 기능을 전혀 가지지 않을 수도 있다는 점이다. 그 결과 개인이 관련 정보를 잘 이해한 상태에서 그로부터 유효한 동의를 얻어내는 것이 어려워질 수 있다. 이것이 사실이기는 하지만, 때로 기술은 그 자신이 유발한 문제를 해결하기도 한다. 그 한 예가 홀로그램 컴퓨터이다. 홀로그램을 통해 전통적인 방식의 인터페이스를 쉽게 대체할 수도 있을 것이다.[92]

그러나 홀로그램 기술이 아직 널리 쓰이고 있지 못한 현실을 고려할 때, 인터페이스가 별로 안 되

90) K. Olmstead-M. Atkinson, 「Apps Permissions in the Google Play Store」, 10.11.2015, available at http://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-play-store/.

91) 이 산업실무수칙은 2015년 12월 7일 Hans Graux에 의해 제안되었다. http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=12378. 개발자에만 의무를 부과하는 것에 대해서는 이론의 여지가 있다.

92) 가령, https://www.microsoft.com/microsoft-hololens/en-us을 참조. 법의 실행수단으로서의 홀로그램의 이용에 대해서는 보다 깊은 연구를 요한다. 예를 들어, 홀로그램 기술은 사기방지 목적으로 이용될 수 있다. 다음을 참조: P.S. Divya-M.K. Sheeja, 「Security with holographic barcodes using Computer generated holograms」, in 2013 International Conference on Control Communication and Computing (ICCC), 13-15.12.2013, IEEE, Thiruvananthapuram, 162-166.

유럽 상표개혁조치에 의하여 상표의 개념이 새롭게 정의된 덕분에, 홀로그램은 상표로 등록될 수 있게 되었다. Directive (EU) 2015/2436 of the European Parliament and of the Council (2015.12.16)의 제3조의 (b)항을 참조. 이는 회원국들 간 상표 관련 법 간의 이질성을 감소시키기 위한 것이다.

거나 전혀 되지 않는 '사물'의 경우 가령 노트북 같은 다른 '사물'을 이용하여 정보에 접근할 필요성이 있을 수 있다. 따라서 컴퓨터에서 구동되는 환경설정 소프트웨어가 안전하게 암호화되어야 할 것이다.

일반적으로 말해서, 물리적 인터페이스가 보다 제한적일수록 그리고 그 기저를 이루는 기술상황이 보다 복잡할수록, '사물'이 GDPR에 의해 제시된, 미리 계획된 바에 의해 그리고 프라이버시 원칙이 '사물'에 기본적으로 구현되도록 하는 것이 보다 중요해진다. 그럼에도 불구하고, 적어도 세 가지 문제가 제기된다. 첫째, 전술한 접근방식을 강력하게 시행할 경우 시스템이 폐쇄적으로 작동하게 될 수 있다. 이로 인하여 정보의 상호교환, 혁신 그리고 사물인터넷 시스템의 기능이 방해 받을 수 있다. 둘째, 설계에서 프라이버시를 구현하기 위해서는, 제조자 또는 개발자가 미리 처리목적에 관하여 알 수 있어야 한다. 그러나 본 논문에서 다루어지는 용도변경으로 인하여 항상 그런 문제가 발생하는 것은 아니다. 셋째, deep learning과 인공지능 기술이 널리 채택되면서, 문제되고 있는 쟁점과 관련하여, '사물'이 스스로 자신을 재프로그래밍할 수 있게 됨으로써 프라이버시 설정을 삭제할 수 있다는 것이다.

만약 이용자가 관련 정보를 적절하게 고지 받지 못하는 것을 무릅쓴다고 한다면, 용도변경 같은 현상과, 예측분석(predictive analytics)·증강현실(augmented reality) 같은 데이터와 기술의 결합(특히 사물클라우드와 빅데이터의 맥락에서)은 정보의 과부하라는 그 정반대의(그러나 양자는 서로 얽혀 있다) 문제를 발생시킬 수 있다. 그 최종결과는 같을 것인데, 왜냐하면 이용자는 역시 적절하게 정보를 고지 받지 못할 것이기 때문이다.

일곱 번째의 또 다른 중요한 정보보호원칙은, 불법적인 처리와 개인정보의 손실을 막기 위한 적절한 기술상의, 조직상의 조치를 취하도록 하는 것이다. 그러나 사물클라우드 생태계의 복잡성으로 말미암아, 보안상의 미비점이 있다고 하더라도 실제로 그에 책임 있는 행위자를 파악하기가 항상 용이한 것은 아니다.

오래된 스마트폰 모델과 태블릿을 소유한 사람들에게 익숙한 또 다른 문제가 존재한다. 소프트웨어 라이프사이클(lifecycle)이 하드웨어보다 훨씬 더 짧고 소프트웨어에 대한 지원이 머지않아 종결된다는 것이다. 보안 업데이트가 보다 길게 제공될 경우 보안상의 위험이 보다 커진다(이러한 불일치로 인하여 오래된 사물의 기능이 멈추는 것은 별론으로 하더라도). 이에 대한 하나의 해법이 하드웨어의 명세(specification)를 공개하는 것이다(오픈소스 하드웨어). 그리고 2015년 7월 Chrysler가 오류를 수정하기 위해 1백 4십만 대의 자동차를 리콜 조치한 것에서 또 다른 해법을 이끌어낼 수 있다. 전파를 통한(over-the-air) 업데이트, 즉 새로운 소프트웨어 또는 데이터를 무선으로 전송하는 방안이다. 그러나 그러한 우회로가 보안 문제와 관련하여서만 이용되도록 하는 주의가 필요하다(마이크로소프트사(社)의 최근의 업데이트에서는 그와 다른 사태가 벌어졌던 것으로 보인다). 이에 대한 시사점은 또한 애플사와 FBI 사이에서 얼마 전 벌어진, FBI의 테러리스트의 아이폰에 대한 잠금해제 요구에 대해 애플사가 이를 거부한 사건으로부터도 간취할 수 있다. Tim Cook의 말을 빌리자면, "FBI는 우리에게 몇몇 중요한 보안요소들을 우회하여 새로운 버전의 아이폰 운영체제를 만들어, 이를 복구된 아이폰에 이를 설치하라고 요구한다. 나쁜 의도를 가진 사람이 이 소프트웨어를 이용할 경우 타인의 손에 들어간 아이폰의 잠금이 해제될 수 있다."[93]

ICO는 2020년경 500억 개의 '사물'이 이용될 것을 고려할 때, IPv4 망에서 IPv6 망으로의 전환이 대단히 중요하다는 것을 지적하는 것으로 끝맺고 있다. 대략 2^{124}개의 IP주소가 사용되면 IP주소는 시공간에 존재하는 어떤 것이라도 식별해 낼 수 있을 것이고 따라서 개인정보와 같은 것이 될 가능성이 높다.

93) T. Cook, 「A Message to Our Customers」, 16.2.2016, at http://www.apple.com/customer-letter/.

본 논문의 개정작업이 막바지에 이르렀을 때, ICO가 프라이버시 관련 통지를 보다 자주 해야 할 필요성에 초점을 맞춘 실무규칙을 발표하였다.[94] 이 실무규칙은 사물인터넷에 대한 보다 성숙한 접근으로서(사물인터넷에 관해 한 절이 할애되어 있다), 가령 "개인정보의 처리에 복수의 데이터 컨트롤러가 개입되는 경우가 빈번히 발생하는데, 이들 각각은 이용자에 대하여 프라이버시 통지를 해야 할 의무를 부담한다."는 지적에서처럼 사물인터넷의 독특한 특징을 제대로 인식하고 있다. 이 실무규칙은 피트니스(fitness)용 '사물'의 사례를 제시하면서 그 제조자, 서드파티 앱의 개발자, 소셜네트워크 플랫폼 그리고 의료보험회사를 그 예로 지적하고 있다. "모든 프라이버시 이용내역 정보를 한 데 종합하여 단 대 단(end to end)방식으로 이용자에게 제공하는 공동수단"에 의하여 개별 프라이버시 통지를 보완할 것을 제안하고 있다. 희망컨대, 기업들이 사물클라우드의 협력적인 성격을 충분히 활용할 수 있을 것으로 본다.

프라이버시와 정보보호는 또한 앞서 언급된 Blackett Review의 핵심이기도 하다. 영국정부 과학분야 최고고문(Government Chief Scientific Adviser)은 세계 73억 인구에 250억 개의 '사물'이 존재하는 현실 그리고 보안과 프라이버시에 대한 침해 가능성이 극히 높다는 점(baby monitor[아기 상태에 귀 기울이기 위한 무선청취장치]에 대한 해킹 사례가 언급되고 있다)을 강조하는 데에 논의를 국한시키고 있다.[95] 정책 제안의 차원에서 덧붙이자면, 활용을 촉진하기 위해 입법을 최소 수준으로 제한하려는 주장에 대해서는 반대의견들도 적지 않을 것이다.

94) 이 실무규칙은 Data Protection Act 1998의 제51조에 의거하여 Information Commissioner에 의해 2016.2.2. 발표되었다. "Privacy notices, transparency and control – a code of practice on communicating privacy information to individuals" 관련 자문이 진행 중이며 2016.3.23. 마무리될 예정이다. https://ico.org.uk/media/about-the-ico/privacy-notices-transparency-and-control-0-0.pdf.

95) (53)을 참조.

Ⅶ. 소비자보호와 재산권

일반인의 언어 습관에 의할 때, 정보보호와 프라이버시는 소비자보호의 한 부분으로 생각될 수 있다. 그러나 엄밀히 말해서 전자(前者)는 정보주체와 정보 컨트롤러(특히 '일반정보보호규칙(General Data Protection Regulation)'에 의할 때 정보처리자) 간의 관계에 적용되는 반면, 후자(後者)는 B2C (기업과 소비자 간) 관계에 적용된다.[96]

최근의 한 보고서는 소비자법 관점에서 제기되는 많은 과제들을 거론하고 있다. 하이브리드 제품의 발달, 소유권 규범의 약화, 원거리 계약 집행, 투명성의 결여, 복잡한 법적 책임 구조, 제품과 시스템에서의 lock-in (전환비용이 커서 기술전환이 안 되는 상황), 그리고 보안 등.[97]

'소비자권리 지침(Consumer Rights Directive)'[98]은 사물클라우드의 발달로부터 상당한 영향을 받은 것으로 보인다. 유형적인 매체에 의하여 (달리 표현해서, '사물'에 의하여) 전달되는 디지털 콘텐츠는 이제 '상품(good)'으로 규정되고 있다(제2조 (3)항). 게다가, '디지털 콘텐츠'는 "다운로드 받은 것이건 스트리밍 방식이건, 유형적 매체에 의한 것이건 여타의 모든 방식에 의한 것이건 관계없이"(Recital 19, 강조는 필자) 디지털 형식으로 생산 또는 제공된 데이터를 의미한다. 개인은 그가 소유한 어떤

96) The directives refer to consumer-trader relationship. Under art. 2(1) of the CRD, 'consumer' means "any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession", whereas 'trader' means "any natural person or any legal person, irrespective of whether privately or publicly owned, who is acting, including through any other person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession in relation to contracts covered by this Directive" (art. 2(2) CRD).

97) Consumers International, Connection and protection in the digital age. The Internet of Things and challenges for consumer protection, April 2016.

98) Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.

'사물'에 담겨 있는 콘텐츠에 대해 그 소유의 다른 '사물'을 이용하여 접근할 수 있는데, 이 경우에도 역시 '소비자권리 지침'의 구제를 구하는 것이 가능하다.

제5조 (1)항 g)호 내지 h)호 그리고 제6조 (1)항 r)호 내지 s)호에 의하면, 소비자가 어떤 계약 또는 교신된 청약에 구속되기 전에, 상인은 소비자에 대하여 기능과 상호정보교환 가능성(interoperability)에 관한 정보를 제공해야 한다(원거리 계약 또는 영업장 이외의 장소에서의(off-presmises) 계약과 다른 계약들에 대해서는, "당해 정보가 문맥으로부터 이미 명백하지 아니한 경우"라는 단서가 붙는다). 전자(前者)는 "이를 테면 소비자 행동의 추적 따위를 위해, 디지털 콘텐츠가 이용될 수 있는 방식"(Recital 19)을 의미하고 후자는 "디지털 콘텐츠가 호환이 되는 표준 하드웨어・소프트웨어 환경"(같은 조항)으로 정의된다. 기술적인 보호방안이 지적재산권법의 문제에 보다 가까운 것이지만, 이들은 B2C 관계에서 힘의 불균형을 악화시킬 뿐만 아니라 사물클라우드의 파편화를 심화시킴으로써 '상호단절된 영역들의 인터넷(Internet of Silos)'의 결과를 빚어낸다는 점을 감안할 때, 정보에 관한 여러 의무들이 그것들 역시 포괄하도록 하는 것이 바람직하다(제5조 (1)항 g)호 및 제6조 (1)항 r)호).[99]

'소비자권리 지침'의 개선을 위해 필자가 무엇보다 지적하고 싶은 것은 몇몇 계약의 경우 소비자들은 제9조에서 제15조에 규정된 철회권이 현실적으로 행사되지 못하고 있다는 것이다. 그것들 가운데 둘은 사물클라우드의 맥락에서 특히 주목할 필요가 있다. 첫째, '서비스 계약'에서, "채무의 이행이 소비자의 사전의 명시적인 동의에 기하여 시작되었고 계약이 상인에 의하여 완전히 이행되고 난 뒤에는 철회권이 소멸한다고 하고 있는데, 서비스가 완전하게 이행된 경우" 철회권은 인정되지 않는다(제16조 (a)항). 둘째, 아마도 가장 중요한 것으로서, 디지털 컨텐츠의 제공을 위한 계약에서, "채무의 이행이 소비자의 사전의 명시적인 동의에 기하여 시작되었고 계약이 상인에 의하여 완전히 이행되고 난 뒤에는 철회권이 소멸한다고 하고 있는데, 당해 디지털 컨텐츠가 유형적인 매체에 의하여 제공되지 아니한 경우" 철회권은 인정되지 않는다(제16조 (m)항). 이와 같이, 소비자는 음악 또는 비디오 동영상 다운로드 등의 디지털 컨텐츠의 구매 시 철회권을 보유하지만, 이는 다운로드 과정이 실제로 시작되기 전까지에 한해서만 그러하다. '사물'의 이용자들은 다운로드가 시작되는 시점이 언제인가를 거의 알지 못한다. 이 부분이 가장 약한 고리이다.

'소비자권리 지침'은 영국에서 '소비자권리법(Comsumer Rights Act 2015)'으로 개정되어 시행되고 있다.[100] 본 법은 디지털 컨텐츠(가령, 온라인 영화・게임, 전자책)에 흠결이 있을 때 그 교정 또는 교체의 권리의 기초로서 중요한 의미를 가지고 있다. 서비스는 합의된 내용에 부합하여야 하며, 그렇지 못할 경우 계약내용에 맞도록 서비스를 제공할 의무를 부담한다. 단, 이것이 현실적으로 부적합한 경우 소비자에게 배상의 권리가 인정된다. '소비자권리법'의 구제 범위에는 사물클라우드도 포함되어 있다. '소비자권리법'의 가장 약한 고리로부터 소유권과 정보보호 간의 독특한 관계를 읽어낼 수 있다. 사실, '소비자권리법'은 오직 판매계약, 물품임대계약, 할부매매계약, 물품이전계약에만 적용된다. 판매계약은 위 법에 의하여 일반적으로 정의되고 있지 않으나, '소비자권리 지침'에 따를 때 이 계약은 "상인이 소비자에게 물품의 소유권을 이전하는 채무를 부담하고 소비자는 그에 대한 대가를 지불하거나 지불하는 채무를 부담하는 모든 계약으로서, *물품과 서비스를 그 대상으로 하는* 계약을 포함한다"(제2조 (5)항, 강조는 필자)로 정의된다.

그러나 '소비자권리법'은 "물품이 제공되어, 소비자에게 소유될"(제5조 (2)항 b)호) 경우에만 적용

99) 보다 자세한 내용은 http://europa.eu/rapid/press-release_MEMO-11-450_en.htm?locale=en.

100) 본 법에 대한 마지막 개정은 The Consumer Rights Act 2015 (Commencement No. 3) (Wales) Order 2015에 의하여 이루어졌다.

되고, 소유권은 "단지 특수재산권[용익권 등]이 아니라, 일반적인(전면적인) 소유권"을 의미한다(제4조 (1)항). 소비자가 하드웨어에 대해 재산권을 가지는 경우(소비자가 이용권만을 가지는 경우를 흔히 볼 수 있다)조차도, 그 소비자가 소프트웨어와 서비스에 대하여 소유권을 가지는 것은 아니다. 그 결과, 개인이 '사물'에 대해 일반적인 소유권의 존재를 주장하는 것은 거의 불가능할 것이고 따라서 당해 소비자는 '소비자권리 지침' 하에서 구제를 받을 수 없다.

Ⅷ. 결어

본 논문에서는 사물클라우드로 대표되는 기술적 발전이 법적 책임(특히, 결함이 있는 제품과 관련하여), 정보보호 그리고 소비자보호의 문제에 관한 전통적인 개념들을 재고하도록 요구한다는 것에 대하여 논의하였다. 이는 사물클라우드가 가지는 속성으로부터 유래하는 것이다. 사물클라우드에서 나타나는, 가령 '용도변경' 같은 특징적인 현상을 통해 사물클라우드가 가지는 성격에 대해 분석해 보았다.

용도변경 현상이 특히 시사하는 바는, 사물인터넷/사물클라우드에 대한 부문별 분류 시도는 유용하지 않다는 것이다. 그 생태계의 독특한 특징의 하나가, '사물'이 어떤 목적을 위해 제조되고/제조되거나 제공되지만 이후 예상되지 않았던 방식으로 작동하거나 정보를 생산해낸다는 것이기 때문이다. 따라서 이상적으로는, 규제기관들이 합동하여 점진적으로 그리고 연성법 등의 수단을 통해 개입하는 것이 바람직하다. 이탈리아의 '사물간 통신에 관한 상임위원회'가 그 좋은 예이다.

본 논문은 계속 진행 중인 연구의 중간 결과물로서, 앞으로의 연구는 '사물'들 간의 상호작용, 클라우드 컴퓨팅 그리고 인공지능 기술에 중점을 두어야 할 것이다. 사실, '사물'이 스스로를 (재)프로그래밍하고 적절한 자율적 결정을 내릴 수 있는 때가 오면(이미 일정 정도 실현되고 있다), 용도변경과 재조합이 미칠 효과는 말 그대로 상상 불가일 것이다(책임에 관한 측면 역시 물론이다).[101]

사물클라우드는 법원리에만 영향을 미치는 것이 아니며, eHealth라는 이름 하에 행해지는 광범위한 영역에도 영향을 주고 있다. 사물클라우드-의료는 eHealth에서 여태껏 탐구되지 않은 부문으로서, 의료서비스의 새로운 시대 – 탈중심화되고 환자 중심적이고 역동적인 시대 – 를 열어 보일 가능성을 품고 있다. 건강 관련 빅데이터의 활용과 '사물'에 의해 생성되는 플로우(flow)의 이용은 대단한 가치를 지니고 있으나, '상호 단절된 영역들의 인터넷(Internet of Silos)'을 극복하고 사물클라우드를 사회의 인식과 신뢰 제고를 통해 유용하고 포함적이고 안전한 생태계로 만들기 위해서는 법학자와 의료전문가와 컴퓨터 과학자가 공동으로 노력해야 한다. "가장 심원한 기술은 사라져 보이지 않게 되는 기술"[102]이라는 지적이 옳은 것이라면, 우리는 아주 세심한 주의를 기울여야 하는 것이다.

점점 더 많은 '사물'이 연결되고 가치 있는 정보를 생산하게 되면, 우리는 인터넷에 대한 접근권을 얻기 위해 분투하는 대신, 연결로부터 해제될 권리를 위해 분투해야 할 것이다. 상시적인 감시의 세계를 목전에 둔 현재, 그러한 권리는 아직 실현되지 않고 있다.

---

101) 자율적인 기계에 대한 선구적인 주장은 N. Wiener, 「The Machine Age」, vers. 3, MIT, 1949, 8: "만약 기계가 학습하고 그 행동이 경험에 의해 수정되도록 만든다면 우리는 우리가 기계에 부여하는 모든 수준의 독립성이 우리의 희망에 대해 있을 수 있는 저항의 정도라는 사실과 맞서야 할 것이다. 병 안에 갇혔던 지니는 병 속으로 기꺼이 돌아가려 하지 않을 것이며 지니가 우리의 처분에 맡겨진다고 기대할 이유도 없는 것이다. (…) 우리는 겸손한 마음가짐으로 기계의 도움을 받아 만족할 만한 삶을 살 수도 있고, 거만한 자세로 죽을 수도 있는 것이다." 글 전체는 http://monoskop.org/images/3/31/Wiener_Norbert_The_Machine_Age_v3_1949.pdf.

102) M. Weiser, 「The Computer for the 21st Century」, Scientific American Ubicomp Paper after Sci Am editing, 1991. https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf.

〈참고문헌〉

Aazam, M. et al., *Cloud of Things: Integrating Internet of Things and Cloud Computing and the Issues Involved*, Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th – 18th January, 2014, 414.

Aegis Systems Ltd. and Machina Research, *M2M Application Characteristics and Their Implications for Spectrum. Final Report*, 2606/OM2M/FR/V2, 13.5.2014.

Amyx, S., *Why the Internet of Things Will Disrupt Everything*, July 2014, http://www.wired.com/insights/2014/07/internet-things-will-disrupt-everything/.

Atzori, L. et al., *The Social Internet of Things (SIoT) – When Social Networks Meet the Internet of Things: Concept, Architecture and Network Characterization*, in *Computer Networks* 56 (2012) 3594.

Benjamin, W., *Das Kunstwerk im Zeitalter seiner technischen Reproduzierbarkeit*, in *Zeitschrift für Sozialforschung*, 1936, 5, I, 41.

Botta, A. et al., *On the Integration of Cloud Computing and Internet of Things*, 2014 International Conference on Future Internet of Things and Cloud (FiCloud), Barcelona, 27-29.8.2014.

Calabrese, C. et al., *Comments for November 2015 Workshop on Cross-Device Tracking*, Letter of the Center for Democracy & Technology to the Federal Trade Commission, 16.10.2015.

Christensen, C.M., *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*, Harvard Business School Press, Boston, 1997.

Cook, T., *A Message to Our Customers*, 16.2.2016, at http://www.apple.com/customer-letter/.

Department of Energy and Climate Change, *Smart Meters: a Guide*, 22.1.2013.

Divya, P.S. and Sheeja, M.K., *Security with Holographic Barcodes Using Computer Generated Holograms*, in *2013 International Conference on Control Communication and Computing (ICCC)*, 13-15.12.2013, IEEE, Thiruvananthapuram, 162-166.

ENISA, *Security and Resilience of Smart Home Environments*, 1.12.2015.

FTC Staff Report, *Internet of Things. Privacy & Security in a Connected World,* January 2015.

GCSA, *The Internet of Things: Making the Most of the Second Digital Revolution,* 18.12.2014.

Hayes, B. and Jones, C., *Report on How the EU Assesses the Impact, Legitimacy and Effectiveness of its Counterterrorism Laws*, Statewatch SECILE report, December 2013.

Höller, J. et al., *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*, Oxford (MA), 2014.

Hon. Kuan, W. and Millard, C., and Singh, J., Twenty Legal Considerations for Clouds of Things (January 4, 2016). Queen Mary School of Law Legal Studies Research Paper No. 216/2016. Available at SSRN: http://ssrn.com/abstract=2716966.

International Organization for Standardization (ISO) and the International Electrotechnical

Commission (IEC) Joint Technical Committee (JTC) 1, *Internet of Things (IoT): Preliminary Report 2014*, Geneva, 2015.

ITU (International Telecommunication Union), *The Internet of Things*, ITU Internet Reports 2005, November 2005.

International Telecommunication Union Standardization Sector (ITU-T), *Overview on the Internet of Things*, Y.2060, 06/2012.

Kennedy, E.J. and Millard, C., *Data Security and Multi-Factor Authentication: Analysis of Requirements Under EU Law and in Selected EU Member States*, Queen Mary School of Law Legal Studies Research Paper No. 194/2015, 30.4.2015, available at http://ssrn.com/abstract=2600795.

King, A.A. and Baatartogtokh, B., *How Useful Is the Theory of Disruptive Innovation?*, in *MIT Sloan Management Review*, Fall 2015.

McCarthy, D. and Morling, P., Using *Regulation as a Last Resort: Assessing the Performance of Voluntary Approaches*. Royal Society for the Protection of Birds: Sandy, Bedfordshire, 2015.

Mell, P. and Grance, T., *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-145, 2011.

Ministry of Science, ICT, and Future Planning (Republic of Korea), *Master Plan for Building the Internet of Things (IoT) that leads the hyper-connected, digital revolution*, 8.5.2014.

Noto La Diega, G., *British Perspectives on the Internet of Things: The Clouds of Things-Health Use Case*, in *Internet of Things: Legal Issues and Challenges towards a Hyperconnected World*, Proceedings of the International Conference of the Center for Law & Public Utilities, Seoul National University, Honolulu (US), 27.11.2015, 45-150.

Noto La Diega, G. and Walden, I., Contracting for the 'Internet of Things': Looking into the Nest (February 1, 2016). Queen Mary School of Law Legal Studies Research Paper No. 219/2016. Available at SSRN: http://ssrn.com/abstract=2725913.

OECD, *Science, Technology and Industry Scoreboard 2015*, 19.10.2015.

Reed, C. and Stafanatou, D., *Legal and Regulatory Update - Embedding Accountability in the International Legal Framework*, forthcoming.

Sarkar, S., Chatterjee, S. and Misra, S., *Assessment of the Suitability of Fog Computing in the Context of Internet of Things*, in *IEEE Transactions on Cloud Computing*, Volume: PP, Issue: 99, 1.10.2015, 1.

Satyanarayanan, M. et al., *Edge Analytics in the Internet of Things*, in IEEE Pervasive Computing, Volume:14, Issue: 2, Apr.-June 2015, 24-31.

Advances in Clouds. Research in Future Cloud Computing, Commission of the European Communities, Information Society & Media Directorate-General, Software & Service Architectures, Infrastructures and Engineering Unit, edited by L. Schubert and K. Jeffery, 2012.

Scroxton, A., *Half of UK Businesses Looking for*

Internet of Things Lead Roles, in *ComputerWeekly.com*, 17-2-2016.

Singh, J., Pasquier, T., Bacon, J., Ko, H., and Eyers, D., *Twenty Security Considerations for Cloud-Supported Internet of Things*, in *Internet of Things Journal, IEEE*, 2015, 99, 1.

SRI Consulting Business Intelligence, *Disruptive Technologies Global Trends 2025*, Appendix F: The Internet of Things, available at http://www.internet-of-things.eu/resources/documents/appendix-f.pdf.

Technology Strategy Board, *Internet of Things (IoT) and Machine to Machine Communications (M2M) Challenges and Opportunities: Final paper*, May 2013.

Weber, R.H., and Weber, R., *Internet of Things. Legal Perspectives*, Springer, Heidelberg-Dordrecht -London-New York, 2010.

Weiser, M., *The Computer for the 21st Century*, Scientific American Ubicomp Paper after Sci Am editing, 1991.

Wright, P. and Manieri, A., *Internet of Things in the Cloud. Theory and Practice*, CLOSER 2014, 4th International Conference on Cloud Computing and Services Science, Barcelona, 3-5.4.2014.