Telecommunications Policy xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Telecommunications Policy

journal homepage: www.elsevier.com/locate/telpol

Big data, the Internet of things, and the interconnected society

Information and communications technology has transformed the communications industry and provided many opportunities in the rapidly-developing broadband world. However, at the same time this aggressive transition is posing significant challenges that have the potential to reduce trust in the online environment. With the rapid spread of big data within various fields, there are many innovative applications related to smart manufacturing, smart cities and smart living that have been created, but big data has also raised concerns surrounding privacy and data security. The Internet of things (IoT), which is the network of physical objects connected to the Internet that can allow objects to be controlled remotely, resulting in improved efficiency (Samad, 2016), needs data that it can process and the spectrum to connect its components. Therefore, big data, the IoT, and the spectrum are essential components of an interconnected society.

In June 2016, the 21st ITS Biennial Conference was held in Taipei, Taiwan with the theme "Interconnecting Everything: Harnessing Business, Policy and Smart Societies." The conference, which was hosted by Yuan Ze University, National Chengchi University, Shih Hsin University and the Taiwan Communications Society, presented an opportunity to investigate the many opportunities, challenges and risks posed by the rapid transformations in the digital age, with particular emphasis on being "well connected." There were 122 presentations at the conference. Right after the conference, an open call for papers for a special issue of Telecommunications Policy was announced. After the blind review process, six papers related to Big Data, the IoT, and the shared use of spectrum resources and universal service were accepted.

1. Big data to decipher societal complexities

Big data is defined as massive, complicated data and is beyond the capability of the software technology to process (McKinsey Global Institute, 2011). It can help both industry and government to analyze their data, which can be transformed into information that can serve as a reference for both business productivity and decision-making (Brynjolfsson, 2012). There are analytical tools and software that can help data owners de-identify or re-identify users. De-identification can help protect consumer privacy, while re-identification can help reconstruct the profiles of the users (Podesta, Pritzker, Moniz, Holdren, & Zients, 2014). Obviously, the analysis and application of big data has a great impact on consumer privacy. If the relevant privacy regulations are too strict, they will impede the development of innovative services. Therefore, it is very important to balance the application of big data with the need for consumer privacy protection.

The first paper "Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers" by Chih-Liang Yeh, provides several definitions for data brokers such as "companies that collect consumers' personal information and resell or share that information with others" (FTC, 2014), and "a company or business unit that earns its primary revenue by supplying data or inferences about people gathered mainly from sources other than the data subjects themselves" (Upturn, 2016). The paper explains how data brokers compile personal data from different sources and sell them to businesses. In doing so, they may harm consumers by revealing consumers' personal information in a way that can be re-identified later.

This paper analyzes how data brokers can use big data analytics to generate more revenue and provide personalized products, but at the same time explains how they can also expose consumers to the risks of privacy invasion. It stresses that consumers usually do not read service providers' privacy policies (Solove, 2013); therefore, their privacy self-management is ineffective.

By comparing the relevant laws and policies with regard to data brokers in the US and the European Union, the paper concludes that the US has failed to regulate data brokers, whereas the European Union has asked data brokers to obtain the consumers' consent before they use their data for specific purposes. The paper suggests that the European Union's data protection framework is more effective than that of the US. Since the self-regulation of data privacy is not reliable, the paper strongly proposes that data brokers should be regulated under a comprehensive legal framework.

2. IoT prepares for the all-connected society

The Internet of things (IoT) is defined as the all-connected network of physical devices such as smart phones, home appliances,

https://doi.org/10.1016/j.telpol.2018.03.014

vehicles, etc. “Things” in this sense refer to an “inextricable mixture of hardware, software, data and service (Wigmore, 2014)” that allows for autonomous data exchange and service provision. It is estimated that the IoT will consist of about 30 billion objects by 2020 (Nordrum, 2016) and the global market value of the IoT will reach $7.1 trillion by 2020 (Hsu & Lin, 2016). The IoT marks an unlimited extension of telecommunication services into every corner of our lives and is changing the market landscape. Regulators should be alert to IoT developments and the consequent policy trends.

The second paper is entitled “The Internet of Things as an accelerator of advancement of broadband networks: A case of Thailand” written by Tatcha Sudtasan and Hitoshi Mitomo. Because the authors found that the great availability of broadband access in Thailand does not stimulate broadband penetration there, they inquired into the reasons why people there subscribe for broadband access. In recognizing the IoT's role in the “Thailand 4.0 plan,” the authors hypothesized that the IoT influences people's willingness to access broadband and conducted an empirical study in light of this.

The authors first categorized five domains of consumer-led IoT: home appliance applications, lifestyle, mobility, health, and security. Since the IoT inevitably changes the ways in which people interact through physical devices, the likely changes apply to their choice of communication access as well. By controlling individual characteristics, the authors modeled the causal relationship as to whether or not people's intention to adopt ultra-high-speed broadband access (5G or FTTH) has been increased upon their acquiring knowledge about the IoT. The data employed in this study were collected via an online survey in urban areas in Thailand where the penetrations of mobile broadband communications and the demand for high-end devices are higher.

The bivariate probit model shows that “respondents who used both mobile and fixed broadband tended to have a higher intention to choose both 5G and FTTH. In addition, respondents who were using only one network were also more likely to choose both options”. The policy implication lies in that both advanced mobile and fixed broadband infrastructure should be deployed to match the demand for the IoT services. Moreover, the policy-makers can also simultaneously promote IoT applications in building both networks. Thailand's case study presents us with an inspiring policy endeavor that other developing economies can model for themselves.

The third paper “User preference for an IoT healthcare application for lifestyle disease management” is written by Suwon Kim and Seongcheol Kim. It explores the most prominent area of IoT—healthcare—and presents a roadmap of service development from a user perspective. Because IoT healthcare services are still at a premature stage, people have little understanding of them. That is, people's true perceptions and willingness to adopt the services can hardly be measured. The authors have therefore employed a conjoint analysis that postulates 18 profiles so as to allow respondents to reveal their preferences hypothetically.

The authors selected lifestyle diseases as the scenario for the conjoint analysis because these diseases are highly affected by adults' lifestyles that require constant monitoring. Based on Gronroos's research, Kim and Kim identified five attributes for the conjoint analysis: 1. Profession of service providers; 2. Service scope (monitoring, diagnosis or treatment); 3. Devices (integrated or *ad hoc*); 4. Expert support; and 5. Personal medical data sharing (the proxy for the privacy concern). The data were collected via an online survey website in S. Korea in May 2016 and the sample respondents were chosen on a first-come-first-served basis.

The results show that, for the people who experienced lifestyle diseases, the two attributes that they valued the most were expert support and the profession of service providers when deciding whether or not to subscribe to IoT healthcare services. As for the non-patient group, there was a relatively greater emphasis placed on the provider's profession and devices although they still valued expert support.

Being aware of the validity limits in this research due to the hypothesized profiles, the authors cautiously demonstrated a plausible buildup of the IoT healthcare ecosystem. The authors also suggested policy approaches that could serve as the blueprint in developing IoT healthcare services. That is, the government should intensify the monitoring of unfair market behaviors and prepare for public medical data management.

3. Incentives to enhance the shared use of the spectrum

According to the FCC's Spectrum Policy Task Force Report released in November 2012, there are three spectrum usage models: the command-and-control model, the exclusive use model and the commons (or open access) model. The three models usually co-exist (Federal Communications Commission, 2012). Recently, a spectrum sharing model has been proposed that can provide an alternative to the exclusive use model. When higher bands are extensively used, the shared use of the spectrum can allow incumbents to use the assigned spectrum and also let secondary users have the chance to use the band on a coordinated basis. It not only increases the efficiency in using the spectrum but also reduces the cost for the incumbents (Matyjas, Kumar, & Hu, 2016).

Technically speaking, the IoT, especially the narrow band IoT, does not need more bandwidth to provide service. Therefore, if the incumbent can share the spectrum with the secondary user, it will benefit both. The fourth paper “Mechanisms to incentivize the shared-use of the spectrum,” written by Richard Marsden and Hans-Martin Ihle, provides ideas on how to increase spectrum availability as more of the spectrum is demanded by mobile users. The paper introduces three forms of spectrum sharing: (1) Unlicensed spectrum: Users can access some spectrum bands if there is no interference; (2) Licensed Shared Access (LSA): This allows the secondary user to use the spectrum already used by the incumbent, but the user has to reach an agreement with the incumbent; (3) Spectrum Access System (SAS): This has been proposed by the FCC and covers three tiers: Incumbent, Priority Access and General Authorized Access. A Priority Access license is offered in an auction (Cui & Weiss, 2016; Cui, Gomez, & Weiss, 2014). Their paper argues that a laissez-faire approach is unlikely to lead to an efficient allocation. Therefore, the European regulators' LSA approach, which leaves the incumbents and secondary users to negotiate, is not effective in terms of encouraging spectrum sharing.

Since the incumbent needs incentives to share the spectrum and the potential user also needs transparent information to reach an agreement with the incumbent, the paper proposes a two-step mechanism. First, the LSA licenses should be auctioned. Second, the