物聯網及網路型社會時代：臺灣面臨的重大產業、行為與法律議題[1]

The Age of the IoT and Networked Society: Major Industrial, Behavioral and Legal Issues Facing Taiwan

Shin-yi PENG[1], Galit SHMUELI[2], Soumya RAY[3,] Mei-Chih HU[4], Chung-Kai LEE[5], and Pao-Lien CHEN [6] and CY WONG[7]

[1]Institute of Law for Science and Technology
[2-3]Institute of Services Sciences
[4-7] Institute of Technology Management
E-mail: sypeng@mx.nthu.edu.tw

We appreciate the support from both the MOST and the NTHU's "Higher Education Sprout Project" which allow us to work together and explore collaborative and interdisciplinary solutions. As stressed in our MOST reports, we offer policy recommendations below:

1. Strengthening the IoT Clusters

Southeast Asian countries are actively connecting with global technology, talent and funding, as well as building a well-rounded supply chain network. Against this backdrop, Taiwan is in the position to create cross-border systems to support IoT in the process of ASEAN's industrial upgrade and transformation. At policy level, the government should continue to expand bilateral arrangements between Taiwan and ASEAN economies because formal agreements would ensure Taiwan's firms to do business in these countries with a favorable environment and the operations could be protected. At firm level, Taiwan's firms need to adapt their advanced technologies to local context so as to develop "localized innovative applications" that are dedicated to solve local social problems. Overall, main efforts should be devoted to achieving synergies between research and innovation, bringing together the innovation and entrepreneurship ecosystem around Asian countries, and increasing ecosystem resources and startup success. Taiwan has the very important chance to be an agenda- setters for the consolidation of a cross-border regional approach to IoT cluster development. It is also significant for the firms with the development goal to explore business opportunities associated with IoT and networked-device services to renew their existing internal and external relationships. In order to shape the formation of IoT industry architecture, firms should be prepared to go through intense transformation.

2. Enhancing the Awareness of IoT Users and Big Data Researchers

Taiwan startups continue to grow and improve their data collection systems, resulting in more possibilities and opportunities for using analytics. One common type of big data are large collections of time series that arise from measurements over time from many IoT devices or

[1] MOST106-2420-H-007-019, MOST107-2420-H-007-003, MOST 108-2420-H-007-002.

other methods that collect behavioral data. We have developed scalable methods for clustering and forecasting large collections of time series, and hierarchical series, which provide transparent, accurate, and interpretable results. We have also studied simulation-based approaches for sharing sensitive IoT data -- these directions should be further studied and tested in practice. Another aspect is the growth in the collection of behavioral big data, where fine-grained data is collected on individual users with many indirectly-identifying features such as time and location. At the same time, the EU' GDPR impacts Taiwan companies who have EU customers. We have also been working with Taiwan startups to help integrate big data analytics efforts within the new GDPR scope. Finally and critically, we have highlighted the user behavior and security. IoT and networked-device services will require artificial intelligence to process and engage with the user in real time basis, even when the user is not initiating the interaction. Users might increasingly see IoT devices not simply as computers or responsive devices, but as intelligent others whose decision-making they must also accounted for.

3. Calling for IoT-Specific Guidance

Given the fact that IoT has a cross-cutting character, we have applied an issue-by-issue approach to the assessment and concluded that although IoT regulations in most jurisdictions remain fragmented. In this context, IoT-specific policies are emerging in some areas. IoT regulatory issues connect areas that have been developed as sectoral regulations such as transport (CAVs), healthcare (wearable medical devices), energy and resources (smart grids). For example, the U.S. IoT Cybersecurity Improvement Act requires the NIST to publish "IoT device cybersecurity capability core baseline" so as to address cybersecurity issues of IoT devices, data, systems, and ecosystems. It is evident that IoT-specific guidance of the kind would be useful to provide both public and private sectors more guidance in identifying the opportunities and risks brought by the IoT technologies. That being said, overreaching rules could pose significant obstacles to IoT development. Sectoral regulators should aim to minimize mandatory governmental intervention and favor industry-driven approaches. After all, policy framework for IoT and big data requires cooperation between public and private sectors. This privatization of governance is driven, to some extent, by sectoral regulators' lack of requisite technical and legal expertise to deal with the complex IoT ecosystems. Co-regulation will fulfill an important role in the IoT/big data governance.