Smart rules needed to govern smart lamp posts

As they can gather huge amounts of data, a data ethics board is vital to prevent abuse.

Lim Sun Sun and Roland Bouffanais

For The Straits Times

Singapore looks set to welcome some new-fangled smart lamp posts that will transform its urban landscape. Leveraging the technology behind the Internet of Things, trials will begin in Buona Vista and Geylang of lamp posts that can track temperature and rainfall trends, engage in facial recognition of passers-by, position autonomous vehicles down to within a few centimetres, and even capture transgressions.

These lamp posts will communicate their data wirelessly or through fibre broadband, thus constituting the largest and newest cyber-physical system of its kind as part of the Smart Nation Sensor Platform (SNSP).

If successfully executed, this platform heralds Singapore's brave entry into a future of pervasive, hyperconnected intelligent devices with vast potential for urban planning and governance.

Commuting patterns, land use and crowd management can be more well-calibrated, informed by data that was previously too complicated or cumbersome to gather.

Indeed, such rich and detailed data holds exciting promises for scientific research, including:

- Identifying specific patterns of human dynamics at supreme resolutions and accuracies, thus reflecting high levels of predictability in most human activity, while alerting us to unexpected behaviour such as spikes in commuting patterns, e-mail activity and power consumption;
- Uncovering some possibly universal properties of face-to-face contact networks, allowing us to predict epidemiological spread;
- Enabling large-scale deployment of swarms of cooperative autonomous robots and vehicles equipped with sensors and cameras to ensure that every single centimetre square of Singapore is under observation, thus enhancing detection of illicit activity such as terrorist attacks, drug smuggling and drinking water contamination;
- Analysing crowd movements by demographic characteristics such as age, ethnicity and gender for better planning and design of urban spaces.

Unsurprisingly, though, concerns have been raised about the surveillance enabled by these connected devices. In particular, unlike the fixed surveillance cameras in widespread use today, these new-generation cameras can engage in active facial recognition using real-time artificial intelligence algorithms.

Despite the significant benefits this can mean for crime detection and enforcement, many may regard such facial indexing as a significant threat to individual privacy and liberty.

Another critical challenge to tackle is the sheer scale of the enterprise. The data collected and generated by such devices will be highly voluminous, such that we are dealing not just with big data, but also massive data.

To begin with, the task of even storing such data is a colossal one. For some, the prime concern would be cyber security, given the digital nature of the data.

But while protecting the data is obviously an issue, processing it is a far greater challenge. And the greatest risk in this specific endeavour is the lack of ethical guidelines associated with data analytics.

For such data to be useful, we need highly complex, fully automatised algorithms to make sense of it all. However, computer scientists have yet to collectively discuss and agree upon basic ethical rules associated with the automatised mining of massive data.

Comprehensive and robust regulations must thus be put in place to safeguard individual and societal interests to optimise such massive data.

As the recent exposes on data management breaches by Facebook amply manifest, data security should be the foremost priority and not a casual afterthought.

The Singapore Government can thus be path-setting in more ways than one. Beyond just leading the charge in strategically exploiting the Internet of Things for urban planning and governance, it can also strive to be an exemplar in terms of how it manages, utilises and shares the massive data that is generated.

First, to clarify the principles governing the use of such massive data, it would be tremendously helpful to establish a board akin to the Bioethics Advisory Committee (BAC) that the Cabinet set up in 2000. The BAC examines and makes policy recommendations on the ethical, legal and social issues arising from biomedical science research in Singapore. As Singapore's Smart Nation plans rapidly gather momentum, similar efforts must be made with regard to data science.

This proposed data ethics advisory board should provide clear direction on how the data generated by the SNSP should be stored, processed, anonymised and, of course, secured.

If Singapore is among the first to establish a national-level board of this nature, it would cement its position on the world stage as a far-sighted yet innovative city-state.

Second, the Government should identify various ways in which the massive data from the SNSP can be shared with key stakeholders to advance societal gain.

The Singapore Government can thus be path-setting in more ways than one. Beyond just leading the charge in strategically exploiting the Internet of Things for urban planning and governance, it can also strive to be an exemplar in terms of how it manages, utilises and shares the massive data that is generated.

Again, the recent Facebook experience offers some useful lessons. Chastened by the recent litany of criticisms, Facebook has introduced new initiatives to restrict access to its data.

While such attention to data security is long overdue, there are also emerging concerns that overly restrictive data protection can undermine academic research. Concrete recommendations must therefore be made as to how and under what conditions SNSP data can be shared for scientific research and policy analysis.

The Government faces a severe conundrum. On the one hand, restricting data sharing will hinder scientific breakthroughs that could potentially propel Singapore as the world leader in smart cities. On the other hand, failing to institute critical measures to manage massive data will almost inevitably lead to a Facebook-like crisis at some point.

A data ethics advisory board comprising domain experts from industry and academia would be well placed to help the Government navigate these uncharted digital territories.

Third, public concerns about the expansion of cyber-physical spaces in Singapore should be solicited and taken seriously, with misconceptions addressed through assiduous education efforts so that trust in digital technologies can be forged. Ultimately, if such technologies are to become part of our built environment, it is vital that the public understands how they work, and their implications for our everyday life.

By introducing rigorous measures that safeguard data protection, and that ensure effective use of massive data in the wider public interest, Singapore can make critical strides towards realising the vision of a Smart Nation.

stopinion@sph.com.sg

• Lim Sun Sun conducts research on the social impact of technology and Roland Bouffanais researches into swarm robotics, collective behaviours and artificial intelligence. They are both professors at the Singapore University of Technology and Design.