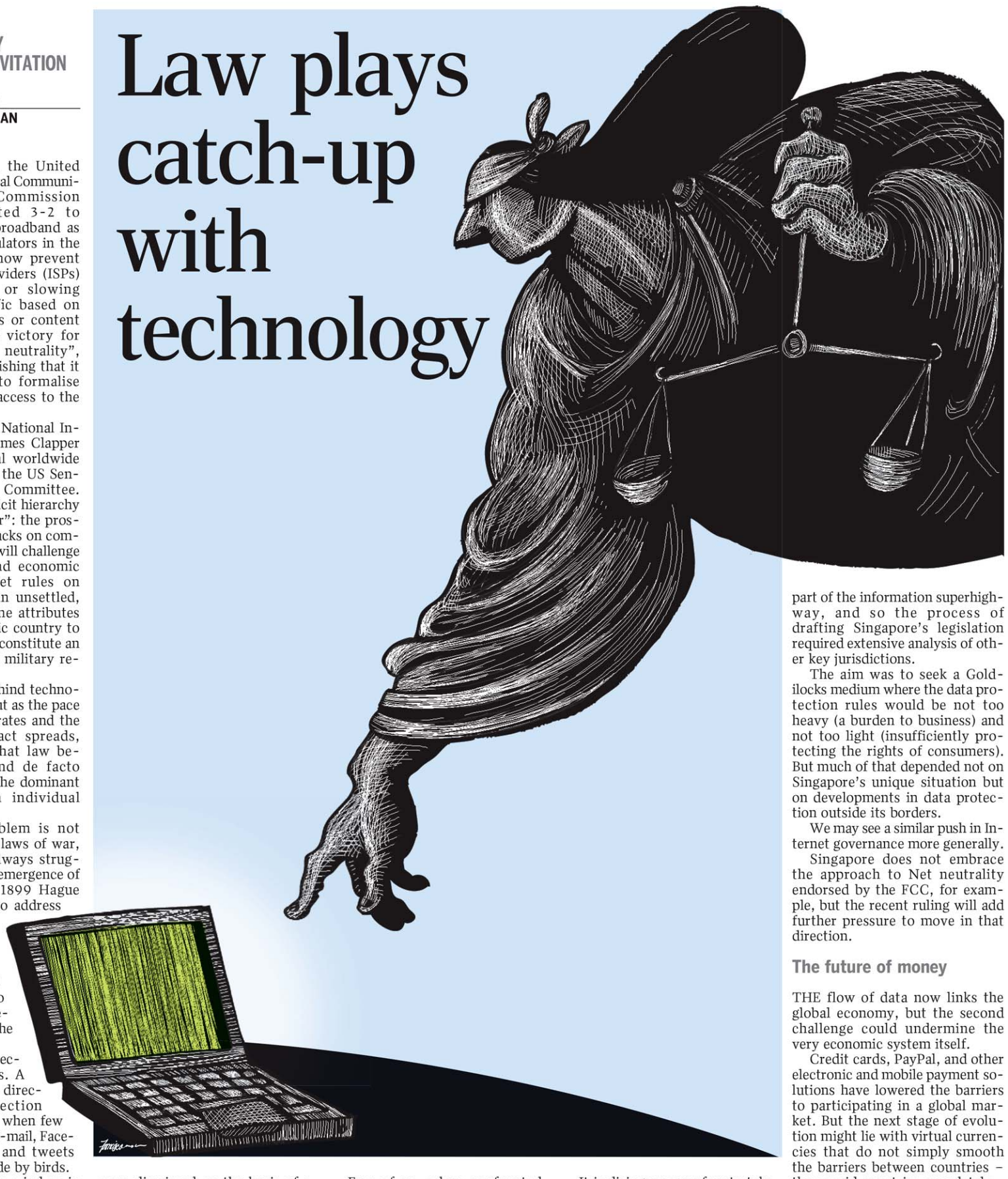
Source: *The Straits Times,* pA42
Date: 7 March 2015

Regulating technology requires the law to keep abreast of rapidly changing trends. The explosion of personal information and the growth of virtual currencies pose particular challenges.

BY INVITATION

By SIMON CHESTERMAN
FOR THE STRAITS TIMES

Law plays catch-up with technology



LAST week, the United States Federal Communications Commission (FCC) voted 3-2 to reclassify broadband as a public utility. Regulators in the United States can now prevent Internet service providers (ISPs) from speeding up or slowing down Internet traffic based on fees from consumers or content providers. It was a victory for proponents of "Net neutrality", but it was also astonishing that it had taken so long to formalise such basic rules on access to the Internet.

On the same day, National Intelligence director James Clapper presented his annual worldwide threat assessment to the US Senate Armed Services Committee. At the top of an implicit hierarchy of threats was "cyber": the prospect of sustained attacks on computer networks that will challenge national security and economic competitiveness. Yet rules on cyber warfare remain unsettled, ranging from how one attributes an attack to a specific country to whether hacking can constitute an "attack" justifying a military response.

Law often lags behind technological innovation. But as the pace of innovation accelerates and the breadth of its impact spreads, there is a danger that law becomes irrelevant and de facto rules will be set by the dominant actors rather than individual states.

The general problem is not new, of course. The laws of war, for example, have always struggled to deal with the emergence of new weapons. The 1899 Hague Regulations sought to address this by introducing the "Martens clause", which provided that the principles of international law applied even to circumstances not specifically covered by the convention.

Such flexibility is necessary in other areas. A key European Union directive on data protection dates back to 1995 – when few people had access to e-mail, Facebook did not exist, and tweets were still sounds made by birds.

When such matters wind up in front of a judge, he or she is often in the difficult position of trying to apply old rules to radically different circumstances.

Take your cellphone, for example. Some recent cases in the United States have held that the police cannot order you to unlock your phone by entering a password because the Fifth Amendment to the US Constitution protects against self-incrimination.

But if your phone uses fingerprint ID, the police can compel you to unlock it because there is no prohibition on taking a suspect's fingerprints.

The new technology does not have to be cutting edge, though.

Early legal challenges to wheel-clamping by private actors were dismissed on the basis of a creative analogy to the mediaeval remedy of distressed damage feasant. This centuries-old doctrine allows a land owner to tether an animal that strays onto his or her land as security for compensation.

Such games of legal catch-up will doubtless continue. Nevertheless, two of the more recent challenges to the law do not merely question its currency. They question the very idea of rules that apply only to the fixed territory of the state that adopts them.

Big data

FIRST, globalisation and technology have radically changed the way we think about information.

Few of us, when confronted with a factual question (say, "What is the capital of Burkina Faso?") would go to a library and look it up in an atlas. Instead, we would pull out our phone and google the answer, or perhaps ask a virtual assistant like Siri.

But we also now expect our own information – our contacts, our files, our photographs – to be available to us anywhere in the world and on whatever device we happen to be holding. As the number of smart devices increases, the "Internet of Things" will make many tasks more efficient and convenient. At the same time, however, the information being gathered by those devices about our daily activities will grow exponentially.

It is disingenuous of us to take all the benefits of this brave new world and complain about a lack of privacy. But laws to regulate the flow of data struggle to keep up with this new world. In an attempt to be "future-proof" and avoid the need for frequent amendments, Singapore's 2012 Personal Data Protection Act uses the word "reasonable" 47 times – a modern variation of the "Martens clause" that leaves detailed application of the law to be worked out in practice.

There is a fundamental tension, however, in trying to use a statute – adopted by the legislature of one country – to regulate data that now flows seamlessly across borders. Consistency with global norms is essential to being part of the information superhighway, and so the process of drafting Singapore's legislation required extensive analysis of other key jurisdictions.

The aim was to seek a Goldilocks medium where the data protection rules would be not too heavy (a burden to business) and not too light (insufficiently protecting the rights of consumers). But much of that depended not on Singapore's unique situation but on developments in data protection outside its borders.

We may see a similar push in Internet governance more generally.

Singapore does not embrace the approach to Net neutrality endorsed by the FCC, for example, but the recent ruling will add further pressure to move in that direction.

The future of money

THE flow of data now links the global economy, but the second challenge could undermine the very economic system itself.

Credit cards, PayPal, and other electronic and mobile payment solutions have lowered the barriers to participating in a global market. But the next stage of evolution might lie with virtual currencies that do not simply smooth the barriers between countries – they avoid countries completely.

The best-known such virtual currency is bitcoin, a peer-to-peer payment system that allows value to be transferred directly from one entity to another without going through a bank or a government regulator.

"Mined" through complex mathematical processes, the value of one bitcoin approached US$1,000 in late 2013 but has sunk to about US$260 (S$356) today. The collapse of the Mt Gox bitcoin exchange a year ago was interpreted by some as the bursting of the bitcoin bubble, but the decentralisation and anonymity of bitcoin has made it a favourite of libertarians – with additional breathless speculation that it will soon become the currency of choice for terrorist groups like the Islamic State in Iraq and Syria.

Much of this is overblown, as bitcoin does not provide true anonymity. Although it does allow the use of pseudonyms, the history of transactions is maintained and can be accessed through the "block chain", a public ledger that records bitcoin transactions.

Indeed, it is the block chain that is now generating as much interest as bitcoin itself. Central to the current economic system is the role of trusted third parties like banks and governments, which regulate transactions. If their role is replaced by an algorithm, enthusiasts see a faster and freer world of direct exchange between individuals. Others are more sceptical, because those third parties also help resolve disputes when property is lost or stolen.

It is too early to see what impact bitcoin will have. While it is essentially treated as a form of currency in the United States, here the Inland Revenue Authority of Singapore considers its sale to be a supply of services – meaning that GST is payable. Other countries outlaw bitcoin completely, or remain on the fence.

The currency of law

SO HOW can and should the law respond to such challenges?

The first thing to acknowledge is that those with legal training are unlikely to be the experts.

One commentator recently compared judges sitting on high-tech cases to asking people who had never heard of marriage to adjudicate divorce proceedings. That's a bit extreme, but recognition of the need to reach out can be seen at Technology Law Conference 2015: The Future Of Money And Data. Organised by the Singapore Academy of Law (of which I am a vice-president) on June 29 and 30, it will bring together not just lawyers and regulators, but also entrepreneurs and innovators.

Second, the law needs to be flexible. For legislatures, that means a principled approach to regulation that establishes rules that are clear but do not micromanage. For courts, it often means deciding only that which needs to be decided in a given case.

A third observation is that the law should be current but not reactive; it should proceed with caution and rigour, rather than fits and starts. It should be sufficiently up-to-date to deal with emerging technology, but it should not seek to lead those changes.

Lastly, and inevitably, law must pay due regard to other jurisdictions. Globalisation has already brought with it much harmonisation of the different legal systems developed by different societies across the planet. Moving forward that trend will continue – not towards some platonic ideal law, but perhaps converging on certain principles on which the vast majority agree.

So law will continue to lag behind technology, but as the ability of individual countries to chart their own paths diminishes, "crowdsourced law" may see the emergence of legal rules and principles that can truly be called global.

stopinion@sph.com.sg
The writer is the dean of the National University of Singapore Faculty of Law.