Editorial

The Digital Economy and Cyber Security

Leith H. Campbell
Managing Editor

Abstract: This editorial comes in three parts: some remarks on developing a cyber security architecture for the digital economy; a note on changes to the *Journal*'s editorial team; and a brief introduction to the papers in this issue.

Keywords: Digital economy, Cyber security, Editorial

The Digital Economy and Cyber Security

As I write this editorial, Australia is reeling from the revelation of a security breach at Optus, one of the country's leading telcos. A great deal of personal identity information on Optus customers may have been stolen. About 40% of Australia's population may have been affected in some way and about 10% of the population may have had data used for personal identification (such as passport numbers and driver's licence details) compromised. The full ramifications of the data breach are yet to be made publicly available. Meanwhile, a rather unseemly "debate" about who to blame continues.

This incident brings into stark relief the ubiquity of online services as the basis of a modern economy. Data breaches like this should not occur – but they do occur, both because of human error and because of new technologies or operations that open up unforeseen opportunities for malicious actors. The digital economy makes personal identity data particularly valuable for those who wish to take over others' accounts. Unfortunately, the expansion of the digital economy also expands the opportunities for illegal exploitation. We publish a paper on one such example in this issue (Mauladi, Jaya & Esquivias, 2022).

Personal identity information was being kept by Optus because Australian law requires that the identity of prepaid SIM-card users be verified (ACMA, 2022). This is a common requirement in many countries. It has benefits for law enforcement and to restrict illegal activity via mobile services, but it causes databases of identity information to be kept by telcos

http://doi.org/10.18080/jtde.v10n3.631

and other service providers. This, then, creates a potential vulnerability that can be exploited, as in the current incident.

In the general Internet and Web, in contrast to mobile services, identity is a weak concept. It is easy to acquire an email address and build an identity online that bears little relationship with one's real-world identity. This feature can provide benefits for some people. It can allow one to segment one's online activities between different hobbies or businesses, for example; or it can help to isolate unwanted messages from advertisers or social-media platforms. It does, of course, also open up opportunities for fraud.

Trust in identity is important in many instances. Customers need to be sure that they are dealing with legitimate businesses. A business needs to know that a customer can be held liable to pay for delivered goods or services. But, in the real world, there is a large sphere of activity where privacy and anonymity can be maintained and are often expected. Online, however, it is hard to maintain true anonymity – made harder by the dominance of multinational companies, like Google and Facebook, that have built vast businesses on constructing detailed profiles of all users who interact with them. Initiatives that may have led to enhanced privacy and anonymity online, such as Bitcoin, seem largely to have failed.

Now that the digital economy and digital society are so pervasive, governments must take the lead in defining an online identity architecture that is fit for purpose and does not require personal identity data to remain in the hands of private companies where it may be vulnerable to theft, while also maintaining privacy wherever possible.

There are no current off-the-shelf solutions available, but there is progress in some countries. Estonia is recognized as an "e-state" ('e-Estonia', 2022) but its architecture is probably not acceptable in other jurisdictions with a different democratic history. The Indian government has been developing India Stack ("National plumbing for the Internet Age") for more than a decade. It aims "to unlock the economic primitives of identity, data, and payments at population scale" ('India Stack', 2022) and it appears to be succeeding. In the Netherlands, there are a number of proof-of-concept projects on "Self-sovereign identity" ('Self-sovereign identity', 2022), which aims to give a user "control over which personal and other data is shared and with whom". The Australian government has made a start – for example, IDMatch (Australian Government, 2022), which provides for online verification of official documents – but much more is needed. It will require trials in a variety of countries before an acceptable architecture has been discovered – and it will be a challenge in many jurisdictions where governments are not very "cyber aware".

In addition, there will be a need to regulate data *operations* to ensure that data is maintained safely and accurately. We have seen the rise of detailed and far-reaching "health and safety"

http://doi.org/10.18080/jtde.v10n3.631

regulation for real-world safety: we need something similar and as pervasive for digital identities and private data. Again, there is a start – see, for example, ACMA (2020) – but much more is needed.

Incidents like the Optus data breach show us that something better is required. It is now time for governments and regulators to step up and provide a "health and safety" framework for the digital society.

New Section Editor

It is a pleasure to announce that Dr Frank den Hartog from the University of New South Wales (UNSW) Canberra has recently taken up the role of Section Editor for Telecommunications. He brings a long history of research in telecommunications, both for industry and academia, to this position. We welcome submissions to the section on all aspects of Telecommunications, including technology, operations and planning.

Dr Michael de Percy, who has been a Section Editor for a number of years, now takes up the role of Section Editor for Public Policy. His new position will strengthen our focus on policy issues and, we hope, lead to a continuing stream of submissions in this area.

In This Issue

Continuing our series of outputs from TelSoc's Broadband Futures Forums, we publish in the Public Policy section a summary of progress in *Regional Connectivity and Shared Infrastructure in NSW and New Zealand* from a Forum held in April 2022.

In the Digital Economy section, we have five papers. Two papers are from Indonesia: *Exploring the Link Between Cashless Society and Cybercrime in Indonesia*; and *Supporting Logistics Management to Anticipate Covid 19 Using the "Retail Direct Order" Concept*. Three papers examine the existing literature to discern themes and to identify gaps: *Technology Acceptance Model (TAM): A Bibliometric Analysis from Inception*; *Digital Marketing Strategies Driven by Wellbeing in Virtual Communities*; and *Mapping Top Strategic E-commerce Technologies in the Digital Marketing Literature*.

In the Telecommunications section, we publish two papers. *Denial-of-Sleep Attack Detection in NB-IoT Using Deep Learning* describes a solution for an issue with IoT devices. *Latency Analysis for Mobile Cellular Network uRLLC Services* examines ultra-reliable, low latency services in future 5G networks.

In the Biography section, we publish an obituary of Rollo Brett, who had been an influential head of the PMG Research Laboratories and had held a number of other senior positions in Telecom Australia.

http://doi.org/10.18080/jtde.v10n3.631

As always, we encourage you to consider submitting articles to the *Journal* and we welcome comments and suggestions on which topics or special issues would be of interest.

References

ACMA [Australian Communications and Media Authority]. (2020). Privacy guidelines for broadcasters. Available at https://www.acma.gov.au/publications/2016-09/guide/privacy-guidelines-broadcasters

ACMA [Australian Communications and Media Authority]. (2022). The ACMA's rules on ID checks for prepaid mobiles. Available at https://www.acma.gov.au/acmas-rules-id-checks-prepaid-mobiles

'e-Estonia'. (2022). Information System Authority, Estonia. https://www.id.ee/en/rubriik/e-estonia/

'India Stack'. (2022). Available at https://indiastack.org/

Mauladi, K. F., Jaya, I. M. L. M., & Esquivias, M. A. (2022). Exploring the Link Between Cashless Society and Cybercrime in Indonesia. *Journal of Telecommunications and the Digital Economy*, *10*(3), 58–76. https://doi.org/10.18080/jtde.v10n3.533

'Self-sovereign identity'. (2022). Self-sovereign identity: a simple and safe digital life. TNO. Available at https://www.tno.nl/en/technology-science/technologies/self-sovereign-identity/