Journal of Telecommunications and the Digital Economy

Volume 9 Issue 2
June 2021

Published by
Telecommunications Association Inc.

ISSN 2203-1693

Journal of Telecommunications and the Digital Economy
Volume 9, Number 2
June 2021

Table of Contents

Editorial Team

The *Journal* is published by The Telecommunications Association (TelSoc), a not-for-profit society registered as an incorporated association. It is the Australian telecommunication industry's oldest learned society.

Editorial

Regulating the Digital Economy

Leith H. Campbell
Managing Editor

Abstract: This editorial comes in three parts: some observations on the growing need to regulate the digital economy more effectively; a brief introduction to the papers in this issue; and some updates on the editorial team that produces the *Journal of Telecommunications and the Digital Economy*.

Keywords: Internet, regulation, Editorial

Regulation and the Digital Economy

In this issue, we publish a significant paper by Derek Wilding (2021), co-Director of the Centre for Media Transition at the University of Technology Sydney. He outlines the policy considerations that lay behind the development of two recent initiatives for regulating digital platforms in Australia. Both were developed in response to Australia's Digital Platforms Inquiry (ACCC, 2019) but the outcomes were very different. He describes the formulation of regulation in these cases as 'haphazard'. We also publish a second paper (Hile, 2021) that questions the effectiveness of some aspects of the laws governing data breaches in Australia.

These are examples – and there are many others – of how the regulation of the digital economy has developed in a piecemeal and ad-hoc manner, in Australia and globally. Yet the digital economy is a key driver of significant economic growth across a wide range of countries, as another paper (Mgadmi *et al.*, 2021) in this issue shows. It is therefore important to develop a coherent and consistent approach to regulating the digital economy.

There is an obvious need at the basic level of law enforcement for greater government intervention in the digital economy. We hear regularly of 'ransomware' attacks and other types of criminality unique to the online environment. (In Australia, the ACCC's Scamwatch page (ACCC, 2021) reports AUD 30 million in losses for May 2021 and AUD 108 million in losses for the year to date.) In addition, there are many references to the 'dark web' and the

http://doi.org/10.18080/jtde.v9n2.425

marketplaces that are available there. Clearly, citizens and businesses are not as protected from criminality in the digital economy as they should expect to be.

In relation to regulation generally, it is common to consider issues at three levels: content, competition, and technical.

For content regulation on the World Wide Web, the internationally popular American websites keep 'objectionable' material off their sites in conformity with perceived social norms and American law. Other countries, including liberal democracies like Australia, then add further restrictions on hosting or disseminating such content. The control of some content is more contested, with, for example, 'hate speech' overlapping with 'free speech' in some people's minds. Yet, we see more and more stories of users, especially women and young people, being harassed online. This again gives rise to ad-hoc responses, with social media companies imposing their own rules, often belatedly and after publicly expressed concern. While there may also be legal restraints, they are often slow to be enforced, and therefore are often of limited effect.

On competition, the ACCC found (ACCC, 2019, chapter 2) that Google and Facebook are each dominant in several markets in Australia. This result would apply in many jurisdictions. The ACCC will be enquiring further about methods to lower the barriers to entry by competitors, including opening up user data held on dominant platforms to be accessed by other applications. It remains to be seen how effective or fundamental such changes could be.

At the technical level of 'control' of the Internet, the situation, while working surprisingly well, is not entirely satisfactory. The Internet Engineering Taskforce (IETF) has developed an 'open' system of development that keeps the Internet connected and working, but it does not – perhaps cannot – respond to all pressures on the network. For example, we have seen the rise of Content Delivery Networks (CDNs), essentially private internets, that work around performance deficiencies in the public Internet. Most of the content accessed every day by online users is handled by the CDNs; many large businesses depend on their websites and content being mirrored on the CDNs. Yet, again, the CDNs are largely hidden from public scrutiny except when a failure occurs.

At a more public level, there are often 'guarantees' that user data will stay within a jurisdiction; for example, that Australian government data on citizens should be stored and accessed only in Australia. On the Internet, however, there is no guarantee that data passed from one Autonomous System (AS) to another – the ASs are the building blocks of the wider Internet – will not transit via another country. While routing errors between ASs are rare (see, for example, Al-Musawi, Hassan & Alturfi, 2020), they do occur and could potentially be introduced with malicious intent.

http://doi.org/10.18080/jtde.v9n2.425

Confounding the need for greater regulation and a more coherent approach is the 'international' nature of the Internet and the World Wide Web, where no one government can regulate the entire system. Governments are starting to take coordinated action to amend tax laws, to overcome revenue-shifting by international companies, so there is hope that more international action on supporting the digital economy could be possible. This is tempered by fear in some quarters of governments with whose policies one does not agree (see, for example, Dupont, 2020) having undue control.

In conclusion, then, it is clear that the current methods, as they exist today, for regulating the Internet and Web are immature and incomplete. As the digital economy becomes an ever-larger part of the total economy, however, the need for more coherent and less ad-hoc regulation will grow. The response will undoubtedly have a profound effect on how the digital economy develops.

In this Issue

We publish in this issue three papers related to public policy. *The Broadband Futures Forum: Regional and Rural Broadband Access* continues our series of reports on TelSoc forums concerning the future of broadband access in Australia, this one from March 2021. *Regulating News and Disinformation on Digital Platforms: Self-Regulation or Prevarication?* describes the policy considerations behind recent changes in Australian law to regulate aspects of the digital economy and assesses the outcomes. *Dude, Where's My Data? The Effectiveness of Laws Governing Data Breaches in Australia* analyzes the laws governing liability in the case of data breaches and identifies a deficiency.

In our Digital Economy section, we publish one paper, *Revisiting the Nexus between Digital Economy and Economic Prosperity: Evidence from a Comparative Analysis*, which looks at the relationship between the digital economy and economic prosperity in developed and developing countries.

In our Telecommunications section, we publish two papers. *Policy-based Interaction Model for Detection and Prediction of Cloud Security Breaches* describes a new model to provide security for transactions in the cloud. *Australian Mobile Survey 2021: Mobile Buying and Churn Drivers Stable* continues our series on surveys of consumer attitudes.

In our History of Telecommunications section, *eLaunceston Revisited – A Novel Regional Research Project from 1999* reprints a paper looking back to a time before ubiquitous social media, when experiments were undertaken to assess the value of local content and the drivers for Internet take-up.

http://doi.org/10.18080/jtde.v9n2.425

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.

New Members of the Board of Editors

We continue to strengthen the Board of Editors, volunteers who give their time to encourage authors to submit to the *Journal*, assist with arranging reviews of submissions in our double-blind, peer-review process, and help with other tasks necessary to bring a new issue to you each quarter.

We welcome three new members of the Board of Editors: Associate Professor Sultana Lubna Alam from Deakin University, Australia; Dr Maria Massaro from Korea University, Republic of Korea; and Professor Ashraf Tahat from Princess Sumaya University for Technology, Jordan. A recent paper by Professor Tahat and his colleagues (Tahat *et al.*, 2020) was published in the *Journal* last year. The addition of these new editors will strengthen the regional and international perspectives of the *Journal*.

References

ACCC [Australian Competition and Consumer Commission]. (2019). Digital Platforms Inquiry – Final Report. Available at https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report

ACCC [Australian Competition and Consumer Commission]. (2021). Scam statistics. Scamwatch. Available at https://www.scamwatch.gov.au/scam-statistics (accessed 24 June 2021)

Al-Musawi, B., Hassan, M. F., & Alturfi, S. M. (2020). RDTD: A Tool for Detecting Internet Routing Disruptions at AS-Level, *Journal of Telecommunications and the Digital Economy*, *8*(2), 18–30. https://doi.org/10.18080/jtde.v8n2.244

Dupont, A. (2020). An Analysis of China's Proposal to Control and Centrally Manage the Internet, *Journal of Telecommunications and the Digital Economy*, *8*(2), 159–166. https://doi.org/10.18080/jtde.v8n2.298

Hile, J. (2021). Dude, Where's My Data? The Effectiveness of Laws Governing Data Breaches in Australia. *Journal of Telecommunications and the Digital Economy*, *9*(2), 47–68. http://doi.org/10.18080/jtde.v9n2.381

Mgadmi, N., Moussa, W., Béjaoui, A., Sadraoui, T., & Afef, G. (2021). Revisiting the Nexus between Digital Economy and Economic Prosperity: Evidence from a Comparative Analysis. *Journal of Telecommunications and the Digital Economy*, *9*(2), 69–90. http://doi.org/10.18080/jtde.v9n2.384

Tahat, A., Ersan, B., Al-Muhesen, L., Shakhshir, Z., & Edwan, T. A. (2020). A Compact 38 GHz millimeter Wave MIMO Antenna Array for 5G Mobile Systems. *Journal of Telecommunications and the Digital Economy*, *8*(3), 44–59. http://doi.org/10.18080/jtde.v8n3.299

Wilding, D. (2021). Regulating News and Disinformation on Digital Platforms: Self-Regulation or Prevarication? *Journal of Telecommunications and the Digital Economy*, *9*(2), 11–46. http://doi.org/10.18080/jtde.v9n2.415

The Broadband Futures Forum

Regional and Rural Broadband Access — City standards in 10 years?

Leith H. Campbell
Adjunct Professor, RMIT University

Abstract: On 24 March 2021, TelSoc hosted the sixth Broadband Futures Forum, held online, with a focus on regional and rural broadband access. Mr Gavin Williams from NBN Co, the developer of Australia's National Broadband Network (NBN), spoke about developments in Fixed Wireless and Satellite services and described NBN Co's commitment to ongoing enhancement of broadband access in regional and rural Australia. A question-and-answer session followed the presentation in which Mr Williams fielded a variety of questions on broadband access and technological developments.

Keywords: NBN, regional & rural, network development

Introduction

The NBN Futures Project (Holmes & Campbell, 2019), now renamed the Broadband Futures Project, has been organizing a series of public forums under the title Broadband Futures (formerly NBN Futures) to encourage debate, and potentially to build consensus, about the future of Australia's National Broadband Network (NBN) and a national broadband strategy (Holmes *et al.*, 2020) for Australia. The forums are hosted by TelSoc (the Telecommunications Association Inc, publisher of this *Journal*). The first forum was held in July 2019 (Campbell & Milner, 2019), the second in October 2019 (Campbell, 2019), the third in February 2020 (Campbell, 2020a), the fourth in August 2020 (Campbell, Smith & Brooks, 2020), and the fifth in November 2020 (Campbell, 2020b). The latter forum was to launch a report, *Towards a National Broadband Strategy for Australia* (Holmes *et al.*, 2020), from the Broadband Futures Group that argues for an overarching National Broadband Strategy for the decade to 2030.

http://doi.org/10.18080/jtde.v9n2.400

The sixth forum, held online on 24 March 2021, was to provide further insight into the potential for development of more capable broadband access in regional and rural areas. Specifically, NBN Co's annual reports had not provided much insight into the development of Fixed Wireless and Satellite access. The Broadband Futures Group had suggested the following test questions:

- What are the prospects of broadband speeds in the order of 100 Mbps/50 Mbps (that is, 100 Mbps downstream to end users; 50 Mbps upstream) and 1 Gbps/500 Mbps being provided to regional and rural Australia over the next 5 to 10 years?
- What are NBN Co's plans to bring rural access progressively up to city quality?
- What are the barriers to higher performance of fixed wireless access?
- To what extent will provision of enhanced fixed-line capabilities for business extend to consumers?

Gavin Williams, Chief Development Officer Regional & Remote in NBN Co, agreed to speak at the Forum.

The remainder of this paper summarizes the content of the Forum.

The NBN Futures Forum

The Forum was conducted online via Zoom. There were more than 100 people registered to attend and at least 87 of them were online at one time.

Introduction

Dr Jim Holmes, President of TelSoc and member of the Broadband Futures Group, chaired the Forum. He remarked that the activities of the Broadband Futures Group now flow from the issues identified in the Group's major report (Holmes *et al.*, 2020).

He introduced the speaker, Mr Gavin Williams, Chief Development Officer Regional & Remote in NBN Co.

Gavin Williams, NBN Co

By way of introduction, Mr Williams indicated a long association with TelSoc and its predecessor organizations. He had, for example, co-authored a paper in the *Telecommunication Journal of Australia* (a predecessor of this *Journal*) in 1992 (Williams & Altamore, 1992).

He noted that he was speaking at a time when severe weather and flooding were affecting parts of eastern Australia. The latest reports to hand indicated that about 6,000 NBN services were

http://doi.org/10.18080/jtde.v9n2.400

currently not working, mostly due to power outages, while 20,000 services had been restored. The infrastructure was holding up well with no major transmission assets affected.

Mr Williams said that the quality, reliability and speed of services in regional and rural areas is a core part of NBN Co's mission to lift the digital capabilities available to businesses and consumers across Australia. This is necessary, he maintained, for all stakeholders to capture the social and economic benefits flowing from broadband. He recognized that the Retail Service Providers (RSPs) had the same mission.

Partly in response to the government's regional telecommunications reviews (the latest in 2018) (RTIRC, 2018), NBN Co had established, in 2019, a Regional & Remote business unit, which Mr Williams heads, to give greater emphasis to development in regional areas. The unit includes "NBN local", a team working with communities and stakeholders to understand community needs and to build digital literacy and digital capabilities. There are also industry specialists targeting the needs of specific segments: agricultural technology, digital health, small business, tourism, education, the arts, and Indigenous inclusion. The emphasis is broader than connectivity, supporting digital transformation in each sector.

The understanding of needs helps to tune NBN Co's offerings. Mr Williams described how the Sky Muster (satellite) service had been evolved to Sky Muster Plus after community consultation as a means of delivering the best service to the 120,000 premises connected to satellite access, while recognizing the finite resources of the satellites.

Mr Williams noted that the Minister had declared the network "built and fully operational" in 2020, providing essentially ubiquitous broadband access across the Australian continent and many islands. The NBN had been rolled out past 12 million homes and businesses and had connected 8 million premises (covering about 17 million people). The lockdowns of 2020 had shown that NBN broadband could support working from home and schooling at home, which would not have been possible with the pre-NBN position of widespread ADSL or no Internet access at all.

The NBN, he suggested, had come through its biggest test well. He noted that average monthly downloads had increased from 40 GB in 2013 to 300 GB today, while average uploads had risen from 8 GB per month in 2013 to 30 GB per month now. He expected that these figures would continue to rise, with new use cases, such as video surveillance, raising greater expectations for uploads.

NBN Co's investment acceleration plans would continue to deliver greater capabilities, he contended, not just to metropolitan areas. Across the country, 75% of premises are passed by fixed-line technologies. The last corporate plan had described a $4.5B program to ensure that 75% of these accesses would be capable of the highest speed tier, NBN Ultrafast (with near

http://doi.org/10.18080/jtde.v9n2.400

Gigabit per second speeds). In that program, $2.9B will be spent to push fibre deeper into the Fibre to the Node (FTTN) footprint, which passes 4.5 million premises (of which 3.1 million are connected). This will permit about 2 million premises to upgrade on demand to Fibre to the Premises (FTTP). The current estimate is that at least half of this investment will be outside the capital cities, thereby helping to deliver "city-like" quality in regional areas.

There is also a $300M co-investment fund for joint investments with states, territories and local governments to push fibre deeper into the NBN and, potentially, convert some accesses from Satellite or Fixed Wireless to a fixed-line option. In addition, there are business fibre zones, 85 of which are in regional areas, which will promote Gigabit-per-second speeds and symmetric services for businesses. Total investment is $700M, of which about $230M will be in regional areas. There is also an additional $50M co-investment fund to expand the business fibre zones or create new ones.

NBN Co spends about $200M each year on upgrades for Fixed Wireless or Satellite services, mainly for capacity expansion or optimization of Fixed Wireless. In the Fixed Wireless areas, there are 2,200 towers and about 19,000 cells. According to the latest monthly performance reports, only one cell is failing to deliver the performance threshold of 6 Mbps in the busy hour. In the Fixed Wireless network as a whole, the average daily download speed is above 60 Mbps, with a busy-hour average of 40 Mbps. In total, NBN Co plans to invest $2B over the next three years in regional areas.

Mr Williams described how NBN Co, by changing the frame structure of the wireless transmission, had created "Fixed Wireless Plus", which can deliver 75 Mbps downstream and 10 Mbps upstream. Looking to the future, NBN Co has secured spectrum in the 28 GHz band and has begun experimenting with mmWave transmission. In a proof-of-concept experiment near Mortlake, Victoria, 1 Gbps was delivered over 7.3 km, an apparent world record. Mr Williams noted that, of the 620,000 premises served by Fixed Wireless, 90% are within 7.3 km of a cell site. The full effect of 5G/mmWave will only become clear when there is cost-effective equipment available for all parts of the Fixed Wireless system.

Mr Williams outlined the continuing drive to lower the cost per bit for Fixed Wireless. Currently, the spectral efficiency achieved is 4 bits/Hz downstream and 1.6 bits/Hz upstream. This is at the upper levels of 4G/LTE performance and can be achieved because of the managed environment, including professional installation of antennas on end-user premises, operated by NBN Co. Further performance improvements are being pursued through carrier aggregation for load balancing and advanced antenna techniques (such as multibeam and massive MIMO).

http://doi.org/10.18080/jtde.v9n2.400

Returning to business fibre zones, 85 of which out of 240 are in regional areas, Mr Williams outlined the offer: enterprise-grade Ethernet service at up to 1 Gbps symmetrical; no build cost charged to the customer; and, for the first 3 years, no wholesale installation charge. In addition, wholesale prices are the same as in central business districts. This, Mr Williams believed, would be a "game changer" for business in regional areas, supporting advanced manufacturing and integrated supply chains.

For the Sky Muster satellite services, Mr Williams noted that the satellites were launched 5 years ago with a nominal life of 15 years, meaning that they have a residual life of 10 years, and perhaps a few years more with efficient conservation of fuel. Total available bandwidth from the two satellites is about 182 Gbps. The current access service is at 25 Mbps. The business satellite service can provide bursts of 50 Mbps down and 10 Mbps up. New equipment may enable services above 100 Mbps.

In closing, Mr Williams outlined a vision for the revitalization of regional life through the infrastructure provided by NBN Co. A survey, he noted, had found that 35% of Australians are considering relocating to their ideal location, which will be outside the main cities. The "new normal" will entail flexible working, with remote access to healthcare and other services. NBN Co, he contended, will continue to support the population and economy of regional areas.

Questions and Answers

Question: Are there opportunities to expand the fibre footprint in regional areas, for example, by demand aggregation or by expanding the fibre rollout around business areas?

Mr Williams noted that fibre access was already being installed in regional areas when new broadacre housing estates are developed and in business fibre zones. When fibre is pushed deeper into the network, it becomes incrementally cheaper to expand the fibre footprint into neighbouring areas. The $300M co-investment fund may be used for some of this expansion, depending on the priorities of local councils. Similarly, demand aggregation may be facilitated by local councils or state or territory governments, leading potentially to co-investment projects.

Question: The satellite service, with 120,000 connections out of the 400,000 planned, appears not to be popular. ACCAN has identified examples (Corbin, 2019, p. 14) where people are preferring to keep their DSL connections rather than switch to satellite service. Are there possibilities for expanding fixed services (or Fixed Wireless) in these areas to meet the perceived demand?

http://doi.org/10.18080/jtde.v9n2.400

Mr Williams answered that he would always support a consumer's informed decision to remain with an ADSL service instead of taking up a satellite solution. His and his team's direct experience, however, is that often those with less than favourable opinions about the satellite service have not used it.

He characterized the main negative feedback about satellite service as falling into two categories: reliability and data allowances. On reliability, he noted that there had been some teething problems with the core network, but they were now resolved. He conceded that the satellite service would be degraded during monsoonal conditions but would come back up, while, in contrast, he had heard of landlines being out for weeks after monsoons.

After feedback from stakeholders, NBN Co introduced Sky Muster Plus, which provides unmetered data for all but streaming video and VPN traffic. This makes the service comparable to the older ADSL unmetered services. Mr Williams' own experience during the Covid lockdown was that Sky Muster Plus worked well for working from home, supporting all the necessary information, communication and collaboration tools.

In addition, the co-investment fund could be used to support moving communities from Sky Muster to Fixed Wireless or fixed-line services.

Question: There appears to be a difference in perceived performance of Fixed Wireless Access between Australia and New Zealand. The quoted performance of the NBN Fixed Wireless seems to be comparable to that attained in New Zealand, where there is a satisfied base of customers. What is the reason for the difference in perception in Australia?

Mr Williams suggested that there can be long memories of service impacts. He conceded that the early Fixed Wireless installations were not up to standard, but a significant upgrade program has been undertaken and customer satisfaction, as surveyed, is now good.

Some upgrade activities that negatively affected services may also have been perceived as reliability issues. When the Covid lockdowns occurred and people were working from home, NBN Co was able to move most service-affecting upgrade activities to the period from midnight to 6 am, thereby avoiding disruption during business hours.

Question: The experiments with 5G and mmWave are very encouraging. In New Zealand, there is concern about foliage attenuation with mmWave. What has NBN Co considered about foliage attenuation?

Mr Williams answered that NBN Co's models do take account of terrain and foliage but there will need to be further extensions for mmWave. The professional installation approach for antennas on customers' premises does provide for optimizing the initial radio link but ongoing

http://doi.org/10.18080/jtde.v9n2.400

monitoring is necessary to identify links with low signal-to-noise ratios. The sophistication of the tools to identify individual services with problems is increasing.

Mr Williams also noted that the current spectrum holdings in the 2.3 and 3.4 MHz bands would remain. The mmWave spectrum could be used for premises close to a cell site, thereby freeing up radio resources at lower frequencies for use with premises that are further away.

Question: What can NBN Co do to support the expansion of mobile coverage in marginal, non-commercial areas?

Mr Williams firstly acknowledged the positive contribution of the questioner, Robin Eckermann, to thought leadership on regional and rural communications.

He then noted that NBN Co has a cell-site access product for co-location, but this has not been much taken up. In some cases, there has been co-investment in a tower site with mobile operators. NBN Co is considering the backhaul capabilities of the Sky Muster business service to support services to very remote communities.

The solution, he suggested, was to work cooperatively, as NBN Co has been doing, with other providers to support co-location and facility sharing.

Question: What will be the impact of Low Earth Orbit satellites (LEOs) on NBN Co's regional business?

Mr Williams considered that there was still much uncertainty about the commercial success of LEO-delivered broadband services. He noted that the vertically integrated operation being trialled by Starlink is a very different model from that delivered by NBN Co. He suggested that the LEO operators face three main challenges: a sufficient number of satellites; the regulatory rights to spectrum; and cost-effective flat-panel arrays.

Regarding NBN Co's stance, he reiterated that there are 10 years or more of operating life left in the Sky Muster satellites. NBN Co will evaluate alternative options closer to the end of life of the satellites, when the uncertainties may be less. He indicated that NBN Co is not committed to being an asset owner and could become a capacity buyer from other satellite operators.

Question: What commitment by government to regional economic development can be expected to follow the broadband expansion?

Mr Williams considered that economic and infrastructure developments were bedfellows and best advanced in an integrated manner. He noted that the $300 million co-development fund would be aligned with the priorities of local jurisdictions through local consultation.

http://doi.org/10.18080/jtde.v9n2.400

He described two recent developments. In New South Wales, which has designated "corridor towns" and "special activation precincts", the Bomen estate near Wagga has been converted from Fixed Wireless access to FTTP as a business fibre zone, to support other business development in the area. In Jabiru in the Northern Territory, NBN Co is building out fibre to support the developing industries in cultural tourism, as the region moves away from mining.

Question: In the Shoalhaven region of New South Wales, the council has reported difficulties with Fixed Wireless service in outlying rural areas. The service cannot support working from home or rural businesses in some cases. How can the council work with NBN Co on these issues?

Mr Williams noted that the NBN Co regional teams, including one in the Shoalhaven, are now better able to work with local communities to resolve problems with Fixed Wireless access. They are finding that, in some cases, the difficulties arise because of growing foliage or an antenna that has gone out of alignment. Tuning the Fixed Wireless service is also possible to improve performance.

Mr Williams reported that NBN Co is fully aware that it does not offer a business-grade Fixed Wireless service at present, only a business-grade Satellite service, and is reflecting on future developments of the service.

Question: The questioner was in Umuwa in the Anangu Pitjantjatjara Yankunytjatjara (APY) lands in South Australia. He considered that business opportunity was being stifled by the lack of suitable broadband access. What can NBN Co do to support business growth in these remote communities?

Mr Williams noted that Sky Muster service is available but VPNs would need to be tuned to take account of the unavoidable 500 ms delay in the satellite hops. He recognized the business opportunities in remote areas and indicated that it is a priority for NBN Co to connect First Nations communities.

[The questioner intervened to describe some of the business opportunities, including remote management of assets by pastoralists and mining companies. He described how Telstra had installed fibre to the administration building in Umuwa, enabling the change-over to full Cloud computing, which was not possible with the satellite service.]

Question: What kinds of use in regional and rural areas has been unexpected? Has NBN Co been able to support these unexpected uses?

Mr Williams pointed to a comment in the chat window that indicated that a power user in a regional area had used 600 GB on the Sky Muster Plus service and a neighbour had used 1 TB (1000 GB).

http://doi.org/10.18080/jtde.v9n2.400

He noted that opening up capability through Sky Muster Plus had revealed new demands such as Zoom conferences, access to city facilities from remote locations, and telehealth in remote areas ("GP in a box"). Distance, he said, creates innovations through necessity. He felt it was gratifying to be a part of this development.

In closing and thanking Gavin Williams, the chair noted that a future Broadband Futures Forum is planned on satellite services, particularly the possibilities from LEOs.

Conclusion

This was the sixth of a planned series of forums related to the future of the NBN and a broadband strategy for Australia. It was notable that a speaker from NBN Co had been available and willing to make a presentation.

Mr Gavin Williams, head of the relevant business unit within NBN Co, painted a picture of continuing development of broadband access in regional and rural areas. He was frank about deficiencies that had been identified in earlier services and described how further improvement had unlocked new possibilities for business in regional areas. He described how new funding initiatives, specifically the business fibre zones and the $300M co-investment fund, would lead to new developments, including the expansion of the FTTP footprint.

Mr Williams indicated that the creation of his business unit in 2019 had given renewed emphasis to developments in regional and rural areas. As well as better focussed monitoring and enhancement of services, the deployment of personnel in regional areas through NBN local had improved liaison with local authorities and local communities. This had helped to identify priorities and coordinate activities for economic and community development.

Mr Williams' presentation should instil some confidence that NBN Co will continue to improve broadband access in regional areas through technology developments and enhanced operations. No commitment to ubiquitous "city standards" has been made, but the availability of "city-like" services will continue to expand.

Fixed Wireless and Satellite will remain the main vehicles for delivery of broadband access in regional Australia for many years to come. It is in the interests of all Australians, if no-one is to be "left behind", that NBN Co continues to exploit technological and operational advances in these technologies to meet the evolving telecommunication needs of regional and rural businesses and communities.

http://doi.org/10.18080/jtde.v9n2.400

References

Campbell, L. H. (2019). The NBN Futures Forum: Realising the User Potential of the NBN, *Journal of Telecommunications and the Digital Economy*, *7*(4), 1–11. https://doi.org/10.18080/jtde.v7n4.228

Campbell, L. H. (2020a). The NBN Futures Forum: Learning from International Experience, *Journal of Telecommunications and the Digital Economy*, *8*(1), 49–57. https://doi.org/10.18080/jtde.v8n1.251

Campbell, L. H. (2020b). The NBN Futures Forum: Towards a National Broadband Strategy for Australia, 2020-2030, *Journal of Telecommunications and the Digital Economy*, *8*(4), 180–191. https://doi.org/10.18080/jtde.v8n4.372

Campbell, L. H., & Milner, M. (2019). The NBN Futures Forum: Discussing the future ownership of Australia's National Broadband Network, *Journal of Telecommunications and the Digital Economy*, *7*(3), 1–9. https://doi.org/10.18080/jtde.v7n3.202

Campbell, L. H., Smith, A. C., & Brooks, P. (2020). The NBN Futures Forum: Social and Economic Benefits of Broadband for Digital Inclusion and Telehealth, *Journal of Telecommunications and the Digital Economy*, *8*(3), 18–32. https://doi.org/10.18080/jtde.v8n3.346

Corbin, T. (2019). Promoting Digital Inclusion Through the NBN, *Journal of Telecommunications and the Digital Economy*, *7*(4), 12–16. https://doi.org/10.18080/jtde.v7n4.236

Holmes, J., Burke, J., Campbell, L. H., & Hamilton, A. (2020). Towards a National Broadband Strategy for Australia, 2020-2030, *Journal of Telecommunications and the Digital Economy*, *8*(4), 192–269. https://doi.org/10.18080/jtde.v8n4.371

Holmes, J., & Campbell, L. H. (2019). The NBN Futures Project, *Journal of Telecommunications and the Digital Economy*, *7*(4), 33–44. https://doi.org/10.18080/jtde.v7n4.238

RTIRC [Regional Telecommunications Independent Review Committee]. (2018). 2018 Regional Telecommunications Review: Getting it right out there. Australian Government. Available at https://www.communications.gov.au/publications/australian-government-response-2018-regional-telecommunications-independent-committee-report-2018 (accessed 31 March 2021).

Williams, G., & Altamore, M. (1992), Applications in an Intelligent Networking Environment, *Telecommunication Journal of Australia*, *42*(1), 32–38.

Regulating News and Disinformation on Digital Platforms:

Self-Regulation or Prevarication?

Derek Wilding
University of Technology Sydney

Abstract: In February 2021 two initiatives for regulating digital platforms in Australia were implemented. The News Media Bargaining Code ("News Code") attracted international attention as a legislative means of forcing platforms to pay for news content, while the Australian Voluntary Disinformation and Misinformation Code ("Disinformation Code") was modelled on an international initiative. Both were developed to meet Government policy formulated in response to Australia's Digital Platforms Inquiry. Whereas the Inquiry recommended the use of co-regulation, Government policy switched to voluntary codes for both, then to a legislative scheme for the News Code. This article examines the schemes and critiques the policy on which they are based. It applies a conceptual framework to assess the optimum conditions for the use of co-regulation and self-regulation. It finds that a self-regulatory scheme of voluntary codes was never a suitable approach for the News Code, and that the close involvement of the regulator on the Disinformation Code — without a suitable remit or enforcement powers — distorts the self-regulatory model. This can in part be explained by the failure to address well-recognised flaws in the co-regulatory framework for telecommunications and broadcasting, the consequences of which are now being seen in attempts to regulate digital platforms.

Keywords: Digital platforms, communications, media, co-regulation, self-regulation.

Introduction

For a short time in early 2021, global attention turned to Australia as our Parliament grappled with the challenge of regulating digital platforms. The heightened level of international interest was prompted mostly by the public drama surrounding Facebook's sudden decision to remove news (and, temporarily, a number of non-news information services) from its

http://doi.org/10.18080/jtde.v9n2.415

newsfeed. In an international context, as Lindsay (in print) has shown, Australia's initiative attracted attention for its use of competition law, rather than copyright law, to force platforms to pay publishers for news. While flawed, the scheme appears to have succeeded at least to some extent and for at least some publishers, with deals worth up to $250 million annually for news media businesses (Pash, 2021).

Despite its high profile, the News Media Bargaining Code (now Part IVBA, News Media and Digital Platforms Mandatory Bargaining Code, of the *Competition and Consumer Act 2010* (Cth)) (referred to below as "the News Code") is not the only attempt at regulation of digital platforms in Australia; instead, it can be seen as one of several initiatives aimed at bringing digital platforms within the regulatory framework. This article contrasts the approach taken in the News Code and in the new Australian Code of Practice on Disinformation and Misinformation ("the Disinformation Code"), both of which were developed in response to Government policy that aimed to

> deliver a regulatory framework that is fit for purpose and better protects and informs Australian consumers, addresses bargaining power imbalances between digital platforms and media companies, and ensures privacy settings remains [sic] appropriate in the digital age (Australian Government, 2019, p. 3).

The extent to which the regulatory framework can be described as "fit for purpose" is questionable. In particular, there is a level of uncertainty around the use of co-regulation in the communications sector, with previous policy reviews having shown some fundamental problems in the way it has been applied. As this article shows, the uncertainty surrounding *co-regulation* might in turn explain the inconsistency in how *self-regulation* has been applied to digital platforms.

Evolving government policy

Regarding the News Code and the Disinformation Code as two products of the same policy is important because it shows the variety of regulatory methods and tools currently being employed to tackle platforms. While they are both described as "codes", the first is an example of direct (or government) regulation, while the second constitutes industry self-regulation, albeit with a new level of government guidance. Neither can be described as "co-regulation" which, as explained below, combines industry-based rule-making with enforcement by a government regulator. The development of two new codes, neither of which is co-regulatory, is an interesting development in two respects. First, co-regulation has now been in place for almost 30 years in the communications sector, most notably in the form of codes such as the *Telecommunications Consumer Protections Code* ("the TCP Code") and the *Commercial Television Industry Code of Practice*. As Lee (2018, pp. 26-33) has explained, the regulatory

http://doi.org/10.18080/jtde.v9n2.415

framework in Part 6 of the *Telecommunications Act 1997* (Cth) – under which the TCP Code is registered – was designed both to facilitate market liberalisation in a technologically complex and fast-changing environment, while also addressing problems that had arisen in relation to consumer protection. Second, co-regulation was the approach the Australian Competition and Consumer Commission (ACCC) recommended for both news remuneration and disinformation in the Final Report of its Digital Platforms Inquiry (ACCC, 2019). The Government policy underlying both the News Code and the Disinformation Code (Australian Government, 2019; referred to below as "the Implementation Roadmap") was a direct response to the ACCC's recommendations. However, in declining to pursue a co-regulatory approach, the Government first opted for two voluntary or self-regulatory schemes, then changed course six months later and converted the News Code to legislation while keeping the Disinformation Code as self-regulation.

The Government's initial decision to use self-regulation for the two schemes was a curious move, especially in view of the increasingly common trend internationally away from platform self-regulation and towards government intervention (Gorwa, 2019, p. 2), albeit with lingering concerns for protection of freedom of speech and expression when addressing mis- and disinformation. In a broader sense, regulation of digital platforms needs to be seen in the context of the patchwork approach to regulation of the Internet that has been informed by: late 20th century enthusiasm for cyberspace as an "unregulated anarchy of open communication" (Riordan, 2016, pp. 4-5); early gains made by corporate first movers, including the emergence of s. 230 of the *Communications Decency Act of 1996* in the US and the *EU e-Commerce Directive*, limiting the liability of Internet intermediaries (Suzor, 2019, pp. 43-45); the gradual and pragmatic responses and incursions into regulation which now make the Internet "a curious, unprecedented hybrid of decentralised international organisational structures, informal voluntary contributions and governmental influence" (Oster, 2017, p. 214); and the more recent attempts to bring digital platforms within national legal frameworks, exposing what Gillespie (2018, p. 25) sees as "the myth of the neutral platform".

Evolving approaches to platform governance

Just as the *Communications Decency Act* is now being reconsidered in the US, the role of these intermediaries is being reconsidered here in Australia in spheres ranging from adult cyber abuse (in the Online Safety Bill 2020 (Cth)) to classification of content (Department of Communications and the Arts, 2020), data privacy (Attorney-General's Department, 2020), and defamation (Attorneys-General, 2021). The environment that gives rise to these policy challenges has been described by media and communications scholars as the "platformisation"

http://doi.org/10.18080/jtde.v9n2.415

of the Internet (see, for example: Flew, 2019; Van Dijck, 2018). In legal and regulatory terms, these issues are being approached in a relatively siloed manner: there is no unifying concept of "digital platform service", for example, to connect the matters dealt with under the Online Safety Bill with those covered by the Disinformation Code and the News Code. In this respect, the Australian regulatory approach runs counter to that being developed in scholarly work on digital platforms, in which the concept of "platform governance" (e.g., Gillespie, 2018; Gorwa, 2019; Helberger, Pierson & Poll, 2018; cf. Picard, 2020) is evolving to cover the range of different domains, actors and tools that will be called into operation by public policy.

The thinking involved in this scholarly work has informed, but is not the subject of, this article, which analyses two new schemes and considers how these contrasting attempts to regulate digital platforms conform with or depart from established regulatory practice. It begins by relating the origins of these schemes in the Digital Platforms Inquiry, followed by a description of the operation of each scheme. It then assesses the two schemes against a framework for determining when self- and co-regulation are appropriate regulatory approaches, finding that remuneration for news content was never a subject for self-regulation but that, on balance, a self-regulatory scheme was an appropriate approach for disinformation. The article concludes that these two attempts to regulate digital platforms can be seen as part of a haphazard approach to the use of self- and co-regulation in the communications sector in Australia. This in turn can be largely attributed to well-recognised flaws in the statutory frameworks for co-regulation. The effects of the failure to confront these problems is seen in the ill-fated attempt to use a voluntary code for news remuneration and the version of self-regulation used to address disinformation.

How the Digital Platforms Inquiry Shaped the Two Schemes

The Digital Platforms Inquiry (DPI) commenced in December 2017 with the issuing of terms of reference by the Government and ended in July 2019 with the publication of the ACCC's Final Report. As Flew & Wilding (2020, p. 52) have explained, it resulted from a commitment made by the Government to independent senators in return for agreement to media law changes in 2017, most significantly the repeal of the remaining cross-media ownership rules. These reforms were explained in terms of the profound effects on news media in Australia of digitisation and the arrival of foreign news services, but also the rise of digital platforms as key distributors of news and information. Accordingly, the ACCC was directed under s. 95H(1) of the *Competition and Consumer Act* to investigate various aspects of the role of digital platforms, including their impact on media advertising markets and the extent to which they exercise market power in commercial dealings with creators of journalistic content and advertisers. The ACCC's findings were substantial and varied, covering recommendations for

http://doi.org/10.18080/jtde.v9n2.415

changes to competition law, consumer law, privacy law, copyright law and media regulation. The critical outcomes that provided the basis for the new laws embodied in the News Code, the most significant outcome of the DPI to date, were the findings (ACCC, 2019, p. 58) that Google and Facebook have substantial market power in, respectively, the markets for Internet search and Internet search advertising and the markets for social media services and display advertising. Equivalent findings were not made in relation to the other products and services offered by these two platforms (for example, YouTube and Instagram) nor in relation to other digital platforms, with the ACCC preferring to monitor developments more generally. The ACCC also said that there was likely to be a market for news referral services, but did not go as far as making a finding to that effect; instead, it found that there was a substantial imbalance in negotiating power on the part of the platforms and news providers (ACCC, 2019, p. 99).

Focus on news remuneration and disinformation

In its Final Report, these findings on market power are the foundations for further inquiry by the ACCC into specific practices by digital platforms and their impact on other sectors of the Australian economy and on the community. In Chapter 5 of its report, the ACCC considered the commercial relationships between Australian news media businesses; in Chapter 6, it addressed the effects of platforms on the quality of choice of news and journalism available to Australians. It is these two chapters that led to recommendations for codes of conduct governing the commercial relationship between news providers and digital platforms (Recommendation 7, p. 257) and for a Digital Platforms Code to counter disinformation (Recommendation 15, p. 370), as well as for monitoring by the ACMA of platforms' voluntary initiatives at identifying to their users more reliable sources of news and other content, known as "credibility signalling" (Recommendation 14, p. 369). On the first of these, the ACCC concluded there was a significant bargaining imbalance between Australian news businesses on the one hand, and Google and Facebook on the other. It observed:

> The critical factor creating this imbalance is that for many media businesses, Google and Facebook are 'must have' platforms … media businesses cannot afford not to be on the Google and Facebook platforms and therefore, Google and Facebook have become unavoidable trading partners for many media businesses (ACCC 2019, p. 253).

A concept that underpinned this approach but which received more explicit expression in a subsequent ACCC paper (ACCC, 2020, p. 11) is the "indirect value" that platforms receive from consumers being attracted to use the platform on account of the news content.

On the second issue, the ACCC observed:

http://doi.org/10.18080/jtde.v9n2.415

> International examples and growing public concern about the presence of highly inaccurate and misleading content surfaced to Australian consumers present a compelling case for the Australian Government to address these issues (ACCC 2019, p. 369, footnoted omitted).

A review of the evidence and rationale underpinning these recommendations is beyond the scope of this article, but the recommendations themselves are explained further in the section below. A review of submissions made by industry participants, government actors and civil society is provided by Flew *et al.* (2021).

How the ACCC recommendations were reshaped in government policy

Although the ACCC gave more coverage to news remuneration than disinformation, both were subsequently incorporated into government policy. After consultation by Treasury and the Department of Communications and the Arts on the Final Report, the Government responded in late 2019 with its Implementation Roadmap, supporting in principle most of the ACCC's findings. These included Recommendations 7, 14 and 15, mentioned above. The Government said it would ask the ACCC to work with platforms to develop voluntary codes "to address bargaining power imbalances between digital platforms and news media businesses" (Australian Government, 2019, p. 15) and that the ACMA would oversee the development of "a voluntary code (or codes) of conduct for disinformation and news quality" (Australian Government, 2019, p. 16). The ACCC was to report on progress with the News Code by May 2020, with the codes to be finalised by November that year, while the ACMA was to report on the adequacy of the disinformation code by June 2021. While the ACCC's recommendations were the starting point for both initiatives, the Government said that work on the Disinformation Code should also be informed by "learnings of international examples, such as the European Union Code of Practice on Disinformation ['the EU Code']" (Australian Government, 2019, p. 7).

In addition, advertising arrangements – closely related to the news media bargaining issues – were to become the subject of a new Digital Platforms Branch of the ACCC charged with monitoring "ad tech" arrangements (Recommendation 5 in Chapter 3, p. 157).

The release of the Implementation Roadmap was followed by the ACCC issuing guidance to Google and Facebook in January 2020 on the development of voluntary codes of conduct. However, in April 2020 the Government announced that progress on the News Code was too slow, and that this Code would now be mandatory, not voluntary. In May 2020, the ACCC released a Concepts Paper (ACCC, 2020) on the design of a legislative scheme for the News Code. In July 2020, after receiving submissions on the Concepts Paper, the ACCC issued an

http://doi.org/10.18080/jtde.v9n2.415

Exposure Draft of proposed legislation, before a bill for the News Code was tabled in November: the Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2020.

In contrast to the formality in the development of this scheme, the development of the Disinformation Code was marked mainly by discussions between the ACMA and the industry association representing the platforms, DIGI, throughout 2020, and by the ACMA issuing a Position Paper (ACMA, 2020) in May of that year, ahead of DIGI releasing a draft code for consultation in October.

It will already be evident that between the point of the ACCC's recommendations and the enactment of the News Code and publication of the Disinformation Code – both in the week of 22 February 2021 – there were some major twists in the development of these two schemes. These variations, explained in the next section, reveal something of the difficulties of regulating dominant, global businesses, and something of the compromises made in doing so.

The News Media Bargaining Code

Despite its short life, the News Code has already been the subject of some critique (Caffarra & Crawford, 2020; Lindsay (in print); Leonard, 2021). Here, as the aim is to compare it to other communications regulation, a brief overview of the scheme will be followed by a closer examination of the *form* of regulation.

How the Code works

In principle, the News Code could be applied to any digital platform service that is designated in an act of the Treasurer (as the responsible Government Minister) under s. 52E of the *Competition and Consumer Act*. The scheme does not name any company or service, nor does it give a functional definition of "digital platform service"; instead, it relies on the designation of specific companies and the services they provide. By introducing (in s. 52A) the concept of "responsible digital platform corporation" as well as "designated digital platform corporation", it employs a mechanism for ensuring that the local Australian subsidiaries of Google and Facebook will be involved in responding to requirements imposed under the scheme, including the conduct of the negotiation, mediation and arbitration components.

Two further comments on its application to these companies are needed. First, the underpinning premise is that the prospect of the scheme coming into effect would be enough to force the platforms into separate agreements with news providers as, by doing so, they might escape formal designation under the Code (see the report of the Senate Economics Legislation Committee ["Senate Committee"], 2021, p. 27). This explains the negotiation of amendments to the Bill and the introduction of an explicit requirement (explained below) for

http://doi.org/10.18080/jtde.v9n2.415

the Treasurer to take these deals into account before designating a platform. Second, despite the fact that these side deals might mean that the scheme never actually comes into effect, some of the heat in the early 2021 negotiations between the Australian Government on the one hand and the two platforms on the other came from the proposition, set out in the Explanatory Memorandum to the Exposure Draft (p. 9), that it could apply to several of their services including Google Search and Facebook News Feed, both of which would have far-reaching impact for the platforms' business models, here and overseas. In the end, it appeared that the Code – if it is ever triggered – would more likely apply to Google's News Showcase service and Facebook's News service. The narrowing of its application was part of the compromise that saw both platforms retreat from earlier threats to leave the Australian market.

Returning to how the code works, the overall design of the scheme can perhaps be best explained by recognising that the starting point is bargaining and the end point is arbitration – but only if the bargaining does not work. The bargaining takes place between the local entities of Google and Facebook as the "responsible digital platform corporations" and any "registered news businesses". There are limits on what counts as a news business, but a business will qualify providing (s. 52G): it meets a revenue threshold (s. 52M); it operates predominantly in Australia for the dominant purpose of serving Australian audiences (s. 52O); and it can point to some professional standards (s. 52P). In addition (s. 52N), it must be able to assert that the primary purpose of the mastheads or other news sources it seeks to register is to produce democracy-enhancing, public interest journalism (known as "core news", s. 52A). The news business can then bargain for remuneration for the use of *all* its news content, including sports, entertainment and other news ("covered news", s. 52A). There is a legislated requirement to conduct the bargaining negotiations in good faith (s. 52ZH).

If the bargaining stage is unsuccessful, a mediation stage (s. 52ZIA) with a mediator appointed by the ACMA must precede the arbitration stage, which is initiated (s. 52ZL) via a notice from the news business to the ACCC and the formation of an arbitration panel by the ACMA. At this point the "final offer arbitration" system comes into effect (see Subdivision C of Division 7) which, apart from permitted information requests, involves only one submission and response from each of the parties and a submission on limited factual grounds from the ACCC. The panel must choose one of the submitted offers unless it considers each offer is not in the public interest, but, in that case, it is limited to an adjustment of one of the offers rather than reaching a new amount based on further inquiry (s. 52ZX). There is no review available for these determinations. Although the Act does not provide a formula or methodology for assessing remuneration, it says that the panel must take into account certain matters: the benefit of the content to the platform and the benefit to the news business of having the content made available by the platform; the reasonable costs of the news business in producing the content

http://doi.org/10.18080/jtde.v9n2.415

and the reasonable costs of the platform in making it available; whether there is an undue burden placed on the commercial interests of the platform; and the bargaining power imbalance between news businesses and platforms (s. 52ZZ).

In addition to the remuneration aspects, there is an important "non-differentiation" rule (s. 52ZC) that means platforms, in making available news content as well as in crawling (which, in this context, refers to web data extraction) and indexing it, cannot differentiate: between registered news businesses; between these businesses and those that are not registered; or between unregistered news businesses. The effect of this provision (subject to an exception noted in relation to "points of contention" below) is thought to be that the platform must either be prepared to remunerate all news businesses that qualify under the scheme or offer no news content on the services designated by the Treasurer. There are also some specific obligations (known as the "minimum standards", see Subdivision B of Division 4), the most significant of which is that the digital platform must give registered news media businesses 14 days' notice of a change to its algorithms where the change is likely to have "a significant effect" on referral traffic to the news business (s. 52S). Digital platforms can make standard offers and registered news businesses can bargain collectively (as might occur for groups of smaller publishers), and agreements between platforms and news businesses can result in the parties contracting out of the legislative requirements (see Division 9). Finally, there are enforcement powers given to both the ACMA and the ACCC, with the most significant being the penalties that can be sought by the ACCC under the *Competition and Consumer Act* in the event of a breach of the requirements for non-differentiation and good-faith bargaining and for failure to comply with an arbitral determination (Division 8). Consistent with existing penalties under this Act, they amount to the greater of $10 million, three times the value of the benefit obtained, or (if the value of the benefit cannot be obtained) 10% of annual turnover in the previous 12 months.

Points of contention

While there were several contentious aspects in the design and implementation of the scheme, the platforms strongly opposed the "final offer arbitration model" in the exposure draft, with the mediation provisions seen to be an amelioration of the original design under which platforms could be made to enter arbitration if initial bargaining was unsuccessful. Google described the final offer arbitration model as "completely unreasonable and unprecedented" (Google, 2020a, p. 43), with Facebook describing it as "highly unusual" and "an entirely untested experiment" (Facebook, 2020a, p. 12).

Another aspect they objected to was the criteria for arbitration presented in the version of the scheme presented in the ACCC's exposure draft (Google, 2020a, p. 46; Facebook, 2020a,

http://doi.org/10.18080/jtde.v9n2.415

p. 16). This required arbitrators to take account of the benefits news provides to platforms but not the benefits news businesses obtain from platform referrals. As is evident from the description of the scheme above, this was remedied so that the two-way value exchange must be taken into account, with amendments requiring recognition of the reasonable costs of producing news *and* of making it available on digital platforms, even though there is still no mechanism for ascertaining the value of news content. The principal remaining objections put by Google and Facebook after the Bill had been tabled and before amendments were made in the final weeks are recorded in the report of the Senate Committee (2021, pp. 22-24).

As noted above, the final version of the scheme also included a last-minute amendment to the designation provisions that encourages platforms to develop agreements with news media businesses as a means of avoiding the operation of the scheme altogether. Paragraph 52E(3)(b) now states that, in deciding whether to designate a company and its applicable services, the Treasurer must consider whether the company has made

> a significant contribution to the sustainability of the Australian news industry through agreements relating to news content of Australian news businesses (including agreements to remunerate those businesses for their news content).

Finally, changes to the non-differentiation rule now exclude the operation of that provision in situations including where "the differentiation arises solely from the amount of that remuneration" (s. 52ZC(4)). The combined operation of the new "significant contribution" test and the allowance in the non-differentiation rule for different ways of assessing payments to publishers was seen to address some of the most serious concerns expressed by the platforms with the original version of the legislation.

The Disinformation Code

Although the timeline for the development of the Disinformation Code was almost the same as that of the News Code – and although the two platforms that are the target of that scheme are also two of the eight signatories to the Disinformation Code – the schemes themselves are very different.

How the Code works

The Disinformation Code is published by Digital Industry Group Inc (DIGI), an incorporated association representing digital industry participants in Australia. DIGI's eight members comprise: the major "content platforms", Google, Facebook and Twitter; marketplace platforms, eBay and Redbubble; campaigning and fundraising platforms, Change.org and Gofundme; and Verizon Media, which provides businesses with services such as video

http://doi.org/10.18080/jtde.v9n2.415

streaming and cyber security. The eight Code signatories comprise four of the DIGI members (Google, Facebook, Twitter and Redbubble) along with Microsoft, TikTok, Adobe and Apple.

The Disinformation Code is designed to apply to digital platforms, but that term is not defined in the Code. Instead, the scope of the Code is prescribed in relation to two categories of services and products (see s. 4.1): "user-generated (including sponsored and shared) content" and "content that is returned and ranked by Search Engines in response to user queries" (with an additional definition of "search engine").

Instead of offering a series of specific rules, the Code is "outcomes based", presenting seven objectives and 10 outcomes arranged under the objectives, with more specific commitments presented under each outcome. An outcomes-based approach was advocated by the ACMA in its Position Paper of May 2021, where it set out a series of expectations for the code, in some detail:

> Outcomes-based regulatory frameworks are particularly well suited to complex, dynamic and fragmented markets, where more traditional rules-based regulation is less able to keep pace with the rate of technological change (ACMA, 2020, p. 23).

At the core of the Code is an opt-in mechanism that allows signatories to nominate one or more specified commitments (beyond a common commitment attached to Objective 1). Transparency Reports published by DIGI (2021) show that four of the signatories (Google, Facebook, Microsoft and TikTok) opted in to all obligations, while other signatories opted in to selected commitments. For example, Adobe did not opt in to the political advertising commitments, as they were not applicable to its products. As Twitter does not accept political advertising, it too elected not to opt in to these commitments.

The Code is designed to encourage actions that anticipate and respond directly to offending content and behaviour as well as strategies to promote the availability of reliable or authentic content. These actions and strategies are best explained by briefly describing the seven principal undertakings of the Code, set out in Objectives 1 to 7.

- Objective 1 ("provide safeguards against harms that might arise from Disinformation and Misinformation") includes a commitment to develop measures to reduce the propagation of disinformation and misinformation, for example through labelling and through demoting and removing certain content, as well as prioritising credible news content (s. 5.9). It also includes a commitment to implement procedures to enable users to report problematic behaviours and content (s. 5.11) and to publish aggregated reports on the removal of content (s. 5.13).

http://doi.org/10.18080/jtde.v9n2.415

- Objective 2 ("disrupt advertising and monetisation incentives for disinformation") includes commitments to implement policies that might include restricting the availability of advertising services and placements on sites that propagate disinformation as well as other measures such as providing brand safety and verification tools (s. 5.15).
- Objective 3 ("work to ensure the integrity and security of services and products delivered by digital platforms") involves measures to prohibit the use of fake accounts and bots that propagate disinformation (s. 5.17).
- Objective 4 ("empower consumers to make better informed choices of digital content") provides examples of commitments platforms could take, such as using technological means to signal the credibility of news sources, or prioritising or ranking content to enable users to "easily find diverse perspectives on matters of public interest", as well as promotion of digital literacy and support for fact-checking organisations (s. 5.20).
- Objective 5 ("improve public awareness of the source of political advertising carried on digital platforms") is aimed at providing greater transparency, even though political advertising is not regarded as "disinformation" or "misinformation" under the Code. The examples of measures that could be taken include requiring advertisers to verify and/or identify the source, and requiring political advertisements that appear in "a medium containing news or editorial content" to be presented in a way that makes them readily distinguishable as paid-for content (s. 5.22).
- Objective 6 ("strengthen public understanding of disinformation and misinformation through support of strategic research") involves commitments both to support research (s. 5.24) and to not prohibit or discourage "good faith research" (s. 5.26).
- Objective 7 ("strengthen public understanding of disinformation and misinformation through support of strategic research") includes a commitment to publish an annual report (s. 5.28), with a template for the first report provided in an appendix.

In addition to these objectives, s. 6 presents a list of matters that can be taken into account in ensuring the proportionality of measures adopted under the Code (e.g., s. 6.1G, "the proximity and severity of the harm that is reasonably likely to result from the propagation of the content"). Aspects of code administration, including the commitment to develop an escalated code complaint facility, are set out in s. 7.

http://doi.org/10.18080/jtde.v9n2.415

Points of contention

To date, while there has been some criticism (noted above) of the Code itself and the nature of the commitments made by signatories, there has also been criticism of the decision to adopt a self-regulatory model. Criticisms of the self-regulatory approach include: the use of the opt-in mechanism; the arrangements for reporting; and the arrangements for code administration. Several submitters were critical of the opt-in approach; for example, the Australian Muslim Advocacy Network (AMAN) (2002, p. 3) suggested there should be an *opt-out* mechanism where the code administrator scrutinises arguments for exclusion presented by platforms on grounds such as products and services offered.

While acknowledging these criticisms, it should be noted that the Australian code does go beyond its predecessor, the EU Code, in the following respects: extending the scope of the Code to include misinformation as well as disinformation; providing a general core commitment that applies to all signatories (i.e., a signatory cannot opt out of Objective 1); and its provisions on political advertising in Objective 5.

Variations in Regulatory Design

Having examined how the findings of the Digital Platforms Inquiry were encapsulated in Government policy and how both the News Code and the Disinformation Code operate, we can begin to see the challenge involved in making the regulatory framework "fit for purpose". Part of the challenge concerns the choice of regulatory method. The following analysis draws on a well-established typology of direct (government) regulation, co-regulation and self-regulation, adopting the approach of Lee & Wilding (2020, p. 2), itself an adaptation of the approach set out by the Department of Communications (2014, p. 6, p. 15). "Direct regulation" encompasses legislation, regulations and any regulatory instruments issued under delegation by government ministers or regulators. "Co-regulation" covers arrangements where industry participants, usually through their intermediary bodies, develop the rules set out in a code of practice or other instrument which is then registered with a regulator under a statutory power and enforced by the regulator. "Self-regulation" covers industry-based schemes where industry is responsible for rule-making as well as any enforcement (i.e., there is no formal role for a government regulator).

From co-regulation to voluntary codes and on to direct regulation

Unequivocally, the ACCC recommended a *co-regulatory* model overseen by the ACMA for both codes. The co-regulatory nature of the arrangements is evident from the ACCC's requirements that, although the platforms themselves would devise the codes, the ACMA would approve them and enforce them and, if acceptable codes were not submitted within nine

http://doi.org/10.18080/jtde.v9n2.415

months, develop its own mandatory standard (ACCC, 2019, p. 257). When the ACCC published its Final Report in July 2019, a self-regulatory approach was off the table, with the ACCC saying that, for the News Code, it "does not consider it likely that digital platforms and media businesses will resolve these issues in a timely fashion absent any form of intervention" (2019, p. 255).

The ACCC recommended a similar co-regulatory approach for disinformation, with "an independent regulator, such as the ACMA" registering and enforcing the code (ACCC, 2019, p. 370). And as with the News Code, the ACCC recommended that, if an acceptable code was not submitted within nine months, or if a code was developed but "the regulator believes the code is not operating efficiently", the regulator should develop a mandatory standard (ACCC, 2019, p. 372). In Recommendation 15, the ACCC stressed the need for the regulator to be able to "impose sufficiently large sanctions to act as an effective deterrent against code breaches". Importantly, though, it explicitly endorsed the use of co-regulation over direct regulation, citing a Government guide to the use of regulation (Council of Australian Governments, 2007, pp. 7-9):

> Co-regulation through an industry-drafted code is preferable in this case to direct government regulation, and is expected to better ensure stakeholder concerns and practical considerations such as cost of compliance are managed (ACCC, 2019, p. 372).

Despite the recommendations from the ACCC, the Government's policy decision to use voluntary codes, noted above, was not explained when the Implementation Roadmap was released in late 2019. Neither was there an explanation for what was meant by "voluntary" codes. For both schemes, however, the policy statement provided a fall-back in case these strategies did not work: if agreement on the voluntary news codes was not reached, the Government would "develop alternative options … and this may include the development of a mandatory code", while, if the platforms did "not sufficiently respond" with voluntary disinformation codes, the Government would "consider the need for further measures" (Australian Government, 2019, p. 15, p. 16).

The final version of the News Media Bargaining Code, however, was different from both its earlier conceptions. As noted above, the scheme is mandatory in the sense that it applies to those businesses designated by the Treasurer. Like the earlier voluntary version proposed by the Government, it is overseen by the ACCC. Unlike both its predecessors, it is a fully statutory solution.

The reasons for the second switch on the News Code have been documented in public comments from both the Treasurer and the Minister for Communications, as well as in the Explanatory Memorandum to the Bill and associated second reading speeches, and in a report

http://doi.org/10.18080/jtde.v9n2.415

of the Senate Committee (2021, p. 3). In short, there had been insufficient progress on the development of the voluntary codes of conduct that were proposed in the Implementation Roadmap. As the Treasurer (Frydenberg, 2020, p. 10) explained at the time:

> On the fundamental issue of payment for content, which the code was seeking to resolve, there was no meaningful progress and, in the words of the ACCC, 'no expectation of any even being made'.

While Google and Facebook may have been disappointed by the Government's decision to move from voluntary codes to mandatory codes, once this took place, criticism focussed on its provisions rather than the choice of direct regulation. Forty-three published submissions were made to the ACCC's Concepts Paper and 72 published submissions were made to its exposure draft of the proposed new Part IVBA of the *Competition and Consumer Act*. Some of the main points are noted by the Senate Committee in its report on the Bill, including the overwhelming support offered by Australia's major news organisations (Senate Committee, 2021, pp. 19-22). However, one consequence of the move to direct regulation was the prospect of enforcement actions, and in their submissions to the ACCC's initial Concepts Paper, both platforms suggested it was inappropriate to include pecuniary penalties as part of the enforcement mechanisms (Google, 2020b, pp. 55-56; Facebook, 2020b, pp. 54-56) or, as Facebook (p. 54) put it, "the imposition of monetary penalties as a means of governing commercial relationships".

In contrast, the main criticism levelled at the Disinformation Code was the decision to adopt a self-regulatory code rather than direct regulation. In some respects, this criticism is unfairly directed at the signatories and the code administrator, DIGI. The decision to shift from a co-regulatory approach recommended by the ACCC to a voluntary, self-regulatory approach was one made by Government (in the Implementation Roadmap). Nevertheless, comments from several of the community and academic (and some media company) submitters to the consultation draft released by DIGI in October 2020 reveal deep concern about this move, with the Centre for Responsible Technology (2020, p. 2) saying: "Self-regulation and self-reporting are not sufficient to ensure technology companies act on disinformation". Similarly, Reset Australia (2020, p. 9) said:

> We strongly believe that a self-regulatory code will be insufficient in addressing the harms that arise through disinformation …
>
> International precedent paints a bleak picture of the impact that an opt-in, buffet-style Code with no enforcement measures will have on driving the change necessary to serve Australians.

http://doi.org/10.18080/jtde.v9n2.415

Despite significant changes from the consultation draft to the final draft, Reset was even more forthright in its comments on the publication of the Disinformation Code (Reset Australia, 2021):

> It's ludicrous to have the peak body for Big Tech regulating itself … What we need is an independent public regulator, with the ability to issue fines, notices, and other civil penalties.

Perhaps not surprisingly, these criticisms of the use of self-regulation are not unlike those offered by a number (although not all) of Australian industry and civil society contributors to the DPI, as Flew *et al.* (2021, pp. 138-139) observe.

Assessment: Choice of Regulation

It is important to note that, in departing from the recommendations of the ACCC, the Government spoke of the use of voluntary codes, not of self-regulation; hence, the regulatory choice was presented as between a voluntary and a mandatory code, not between self-regulation and co-regulation. However, it was never clear whether the voluntary codes for news would be self-regulatory or statutory. Although voluntary codes would usually be self-regulatory, a voluntary code can be registered under Part IVB of the *Competition and Consumer Act* and enforced by the ACCC: it is "voluntary" in the sense that it only applies to the businesses that sign up to it. In contrast, as the ACMA does not have any powers to enforce voluntary codes of practice, it was apparent that the Disinformation Code would be self-regulatory.

In this way, it is possible that the approach to the News Code anticipated by the Government was not self-regulatory in the sense that the Disinformation Code was always to be developed by industry without being registered with, and enforced by, the ACMA. However, even a voluntary code enforced by the ACCC would allow participants to remain outside the regulatory framework, meaning the leverage built into the final News Code – where side deals are encouraged as a means of avoiding the application of the legislation – would not exist. Either approach seems at odds with the recommendations of the ACCC.

Further, the slippage in the concepts of "voluntary" and "self-regulatory" is perhaps hardly surprising given that the code-making process under Part 6 of the Telecommunications Act 1997 (Cth) is described as "self-regulation" and s. 106 of that Act says: "Compliance with an industry code is voluntary unless the ACMA directs a particular participant … to comply with the code". While it is true that not all service providers sign up to these codes as members of Communications Alliance (the body that develops them), the fact that they are enforceable

http://doi.org/10.18080/jtde.v9n2.415

against any participant in the industry makes it a stretch to describe them either as voluntary or self-regulatory.

This confusion over terminology – explored in more detail below – should be viewed alongside the different approaches within the same sector to the use of self-regulation, co-regulation and direct regulation. The approach to the News Code also stands in contrast to the approach in the Online Safety Bill, in which the Government has proposed a consolidated piece of legislation – bringing the online content regulation scheme into a single Act with protections against cyber-bullying, adult cyber abuse, image-based abuse and abhorrent violent material – that *does* embrace co-regulation and even sees an enhanced role for it. The discussion paper issued by the Department of Communications and the Arts (DOCA) in 2019 noted that "codes should be developed by a wider range of service providers than the current codes, reflecting the range of services that Australians now use to access online content" (DOCA, 2019, p. 40). In a departure from usual communications sector regulation, the current online content codes, as well as those anticipated under the reformed scheme, are voluntary (in the sense that they only apply to signatories) but then enforceable by the regulator (the eSafety Commissioner) once a service provider becomes a signatory.

As there appears to be some inconsistency here, it is useful to review the policy literature on self- and co-regulation in the communications sector in Australia.

When should self- and co-regulation be used?

One explanation for the reluctance to use co-regulation in the context of the News Code and the Disinformation Code might be found in the move away from co-regulation flagged (at least as a possibility, if not the preferred position) in the third stage of the telecommunications Consumer Safeguards Review being conducted by the Department of Infrastructure, Transport, Regional Development and Communications ("DITRDC").

"Sub-optimal": Self-regulation in telecommunications consumer protection

The consultation paper (DITRDC, 2020) issued by the Department for Part C of this review, "Choice and Fairness", echoed doubts about the efficacy of self-regulation – at least in the context of telecommunications consumer protection – that have emerged over recent years. (As explained above, the term "self-regulation" is used in the *Telecommunications Act 1997* (Cth) to describe what is generally understood in the communications sector and the regulatory literature as "co-regulation".) One of its proposals is for co-regulation to be "confined to second order safeguards or situations where Minister or regulator developed rules could usefully be supported by technical or process requirements" (DITRDC, 2020, p. 25). Its assessment of co-regulation is as follows:

http://doi.org/10.18080/jtde.v9n2.415

> The code development process has appeared to suit matters that require cooperation across industry (e.g., technical matters), rather than consumer issues that may create an impost on industry. There is an inherent tension in a process that requires industry to formulate its own consumer protection rules (DITRDC, 2020, p. 15).

This rather critical view of co-regulation has been brewing for the past decade. The Department had made a similar point in a 2014 report, *Regulating Harms in the Communications Sector* (DOC, 2014), but at that time attributed them to an earlier paper by the ACMA, *Optimal Conditions for Self- and Co-Regulation* (ACMA, 2011). As noted below, the Department reprised this sentiment in its *Final Report of the Review of the ACMA* (DOCA, 2016). However, the original ACMA report and the Review of the ACMA present these points in different ways.

The ACMA's comments in the 2011 version of *Optimal Conditions for Self- and Co-Regulation* (neither an earlier version in 2010 nor a later version in 2015 includes this analysis) were forthright. Using a case study based on its Reconnecting the Customer Inquiry, it concluded "few factors are present for effective co- and self-regulatory arrangements in the area of telecommunications customer care" (ACMA, 2011, p. 9). These observations about the telecommunications sector, while interesting, are not directly relevant to the current environment for digital platforms – for example, there is a large number of carriage service providers and a small number of digital platforms – but the ACMA did give some preliminary consideration to what, at the time, it called "video-sharing websites" such as YouTube. It took into account factors such as the rapid pace of change and the fact that existing company policies and guidelines for use of content suggested some willingness to address online content issues (p. 30). It concluded as follows:

> The preliminary analysis in this case study indicates that some of the conditions for effective self-regulation may be present for video-sharing websites. However, it also highlights the significant regulatory challenges posed by the online environment (ACMA, 2011, p. 31).

"Reinvigoration" of self-regulation: role of the ACMA

The potential problem with co-regulation was again considered by the Department in its Review of the ACMA; however, the rigour evident in the ACMA's own framework for assessing the use of co-regulation and self-regulation is absent. The Review noted the Department's earlier observations in *Regulating Harms in the Communications Sector* (DOC, 2014) but placed more emphasis on the movement towards self-regulation than on the need to bring some aspects of consumer protection back to direct regulation. It said the earlier work "suggests that a reform process should aim to reinvigorate the use of self-regulation" (DOCA,

http://doi.org/10.18080/jtde.v9n2.415

2016, p. 78). In addition, one of its five "regulatory design principles" for the ACMA was that "regulation should promote the greatest practical use of co-regulation and self-regulation" (p. 76), a position that does not indicate a retreat from co-regulation. Interestingly, though, it did suggest two areas where this might occur:

> … in areas where strong competition has emerged, or industry has sufficiently matured its practices over time, the regulator should assume the initiative to explore the conditions under which regulatory interventions could transition from rules-based regulation to co-regulation and from co-regulation to self-regulation. (DOCA, 2016, p. 97)

Specifically in relation to self-regulation, the review identified two factors that would be required for this to be effective (DOCA, 2016, p. 79):

- "a strong commitment from industry so that it will remain responsive to consumer needs and will support codes through high levels of voluntary compliance", and
- "effective compliance processes, with those processes being supported by the establishment of independent industry bodies to implement complaint handling procedures."

There is some similarity here with the policy articulated in *The Australian Government Guide to Regulatory Impact Analysis* (Australian Government, 2020), which recommends self-regulation as a good option where "industry participants understand and appreciate the need for self-regulation". But it also says it is appropriate where "the consequences of market failure are low", unlike situations where, for example, public concern might arise from a perceived conflict that threatens public safety. The guide describes self-regulation as "not a viable option" in such circumstances, providing the examples of food-handling, healthcare and aviation (p. 30).

While this aspect of when it might be practical to deploy self-regulation is not the same as the question of why self-regulation might be used, some of these elements have long been identified in the literature of regulatory theory as reasons for employing self-regulation: Gunningham & Rees (1997, p. 366), for example, identified "speed, flexibility, sensitivity to market circumstances and lower cost". Knowledge is also a factor here (see Coglianese & Mendelson, 2010, p. 153) and, in the case of disinformation, knowledge of developing practices and how best to address the problem clearly puts industry participants in a better position than regulators. However, the most developed approach evident in the Australian policy literature for assessing the use of self- and co-regulation in the communications sector is the framework provided by the ACMA in its *Optimal Conditions* reports.

http://doi.org/10.18080/jtde.v9n2.415

Identifying "optimal conditions": Applying the ACMA framework

In its 2011 report, the ACMA presented a framework for assessing the conditions which lead to effective – and not-so-effective – outcomes in the development, implementation and operation of co-regulatory and self-regulatory schemes. The framework incorporates seven aspects of environmental conditions (number of players in the market and coverage of the industry; whether it is a competitive market with few barriers to entry; homogeneity of products — whether they are essentially alike and comparable; common industry interest — whether there is a collective will or genuine industry incentive to address the problem or enhance existing provisions; incentives for industry to participate and comply; the degree of consumer detriment; and whether the environment is stable or rapidly changing). It also incorporates five aspects of the applicable regulatory scheme (whether the objectives are clearly defined by the government, legislation or the regulator; role of the regulator; the existence and operation of accountability and transparency mechanisms; consumer and other stakeholder participation in the development of the scheme; and whether the scheme is promoted to consumers). In applying this framework to telecommunications consumer protection, the ACMA identified five aspects of the environmental conditions and five features of the regulatory scheme that led to the conclusion that co-regulation was likely not suited to customer care in the telecommunications sector and that it was arguably necessary to augment these arrangements with direct regulation (ACMA, 2011, pp. 20-22).

A number of the ACMA's criteria are similar to, or the same as, criteria cited in cross-industry sources (see, for example, Freiberg, 2017, pp. 111-14), but the ACMA's guide has the advantage of criteria designed more specifically for a communications context. However, even the latest version of the framework used here (ACMA, 2015) predates the ACCC's work in the Digital Platforms Inquiry. As the analysis below shows, criteria suitable for application to telecommunications and broadcasting are not necessarily adaptable to digital platforms. (Although the 2011 analysis of telecommunications consumer protection is not included in the later version, the framework is largely the same.)

Usefulness of the ACMA framework

In applying the ACMA framework to the News Code and the Disinformation Code, it can be seen that two of the seven *environmental criteria* clearly support the use of self-regulation for news remuneration, while additional criteria likely support its use for disinformation. For news remuneration, these are "number of players in the market and coverage of the industry" and "whether the environment is stable or rapidly changing". In its explanation of the framework, the ACMA (2015, p. 12; p. 14) noted that "a small number of players with wide industry coverage will facilitate effective self-or co-regulatory arrangements", and that "self-

http://doi.org/10.18080/jtde.v9n2.415

regulation can be suited to fast-changing environments that may be hindered by static systems of direct regulation". The small number of content-based digital platforms and the fast pace of change therefore suggest that self-regulation is suited to this environment. In addition, for disinformation, "common industry interest" is likely to apply because the industry association, DIGI, was prepared to take the lead and open its forum to participation from non-members, and because platforms' own interests might be served by being a signatory to a disinformation code that could offer value in attempts to build trust among users.

The framework is also useful in indicating environmental factors that are likely to work against the success of a self-regulatory model: lack of competition in the market and the great variation in products and services offered by platforms – within their own businesses, as well as across different providers – were documented at length by the ACCC in the Digital Platforms Inquiry.

In addition, application of the ACMA's five *features of the regulatory scheme* results in clear indications of the problems that could be encountered when using self-regulation for news remuneration. In part, this is because the regulatory objectives and the role of the regulator were uncertain, as the Government adapted the ACCC recommendations and then switched from voluntary codes to a legislative scheme. It is also because of the resistance presented by the platforms to recognition of the value news provides them and their unwillingness to consider a formalised remuneration scheme. In contrast, the industry association managing the development of the Disinformation Code was prepared to design a program for consultation through round tables and written submissions, along with indirect input through academic advisors, and there would be opportunities for promotion of the code through internal platform policies as well as the association. In terms of clarity in the policy objectives for disinformation, Government policy did at least note the precedent of the EU Code, although its suitability was later questioned in the ACMA Position Paper.

Limitations of the framework

While the analysis above shows that the ACMA framework can provide some useful guidance in deciding on regulatory strategies for digital platforms, the analysis also reveals some aspects of the framework that are difficult to apply to digital platforms.

In relation to the *environment criteria*, the category of "amount of consumer detriment" is difficult to assess for either scheme. For news remuneration, there may be significant detriment to news businesses and possibly, in the longer term, to citizens and society, but there is less direct consumer detriment and it does not concern aspects such as public health and safety, which is the example provided by ACMA (2015, p. 13) for where direct regulation may be more appropriate. For disinformation, there could conceivably be a serious impact in terms

http://doi.org/10.18080/jtde.v9n2.415

of public health and safety (e.g., from vaccine conspiracies) or harm to democratic institutions, but actual harm of this kind has not been seen in Australia so far.

In relation to *features of the regulatory scheme*, accountability and transparency are hard to judge for disinformation. Experience with the EU Code might have suggested that a lack of specific commitments and uniform reporting obligations, if replicated in Australia, may make it difficult to assess compliance; in the end, the reporting framework and complaints handling facility were still being developed at the time the code was finalised. Even more difficult to apply for news remuneration are the categories of "consumer and other stakeholder participation in the development of the scheme" and "whether the scheme is promoted to consumers", since the scheme is one that involves news businesses and digital platforms, without involvement of consumers.

Beyond these specific aspects relating to the two schemes, there are some more general difficulties in applying the framework to digital platforms. In relation to disinformation, for example, the variety of products and services offered by the relatively small number of signatories to the code makes the assessment of incentives to comply difficult to assess. In addition, some criteria such as the rapidly changing environment might need to be given more weight than other criteria when the framework is applied in the digital platform environment, compared to the broadcasting environment. It can also be difficult simply comparing one form of digital platform regulation to another (for example, the importance of consumer detriment resulting from disinformation versus harm to news businesses in the case of news remuneration). This is not helped by a lack of clear delineation in the ACMA framework for the use of self-regulation and co-regulation: the framework seems to apply more generally to self-regulation, with additional commentary on co-regulation where applicable.

While some of the aspects noted above might be new to the digital platform environment, some of the challenges are not unlike the situation described by the Australian Law Reform Commission (ALRC) when it considered the use of self-regulation for classification of media content. The ALRC (2012, p. 196) observed:

> While in some areas there may be market incentives for content providers to classify—for example, because distributors and consumers of some products want and expect advice about content—these incentives do not exist in other areas.

Nevertheless, some meaningful conclusions can be drawn from the application of the ACMA framework.

http://doi.org/10.18080/jtde.v9n2.415

What the framework reveals about the digital platform schemes

The News Media Bargaining Code

The first overall finding from applying the ACMA framework is that direct regulation was more suitable than self-regulation for news remuneration. This means that the change from co-regulation to voluntary codes and then to direct regulation was likely to have confused the line of policy development. It allowed less time for development and consultation on the legislative model and, at the point of switching to direct regulation, provoked a foreseeable backlash from industry. Admittedly, the recommendation for co-regulation was not part of Government policy, and while the ACMA framework would benefit from some additional commentary to differentiate the application of self-regulation from co-regulation, it is likely that – had it been applied – it would have highlighted the benefits of accounting for the changing environment while also providing some reassurance in terms of enforcement. As Lee & Wilding (2021, p. 7) have observed, flaws in the current arrangements for developing telecommunications and broadcasting co-regulatory codes do not, in themselves, present an irrefutable argument for abandoning co-regulation; instead, there could be an argument for reforming key aspects of co-regulation in order to retain the benefits of industry knowledge in rule-making while injecting enhanced consumer consultation and regulatory oversight (Lee & Wilding, 2021, p. 11).

The Disinformation Code

It is still more productive to apply the ACMA framework to the Disinformation Code, as this scheme remained a self-regulatory model from the announcement of Government policy in late 2019 to implementation of the Code in early 2021. The decision to use self-regulation for this initiative is, on balance, in the author's opinion, supported by the application of the framework, and also fits with the ACMA's initial assessment back in 2011 that there was some potential for video-sharing websites to be subject to effective self-regulatory arrangements.

However, there are reasons for caution raised by the application of the framework. In the environmental conditions, these include: the lack of a competitive market where consumer choices are likely to act as a brake on unreasonable practices; the great variety in products and services, which makes them hard to compare; and the potential for consumer detriment in contexts such as health disinformation and electoral disinformation. While these are significant issues, it is possible that they are outweighed by the other environmental elements, such as the small number of players and the changing aspects of technology, products and consumer practice. Of more interest to the present analysis are the relevant features of the regulatory schemes, as these are more within the control of policy-makers and regulators. These relate to items 8, 9 and 10 in the ACMA framework: the clear definition of objectives;

http://doi.org/10.18080/jtde.v9n2.415

the role of the regulator; and the existence and operation of accountability and transparency mechanisms.

In relation to the clear definition of objectives, the Government policy guidance issued in late 2019 was scant and provided for great variation in approach and content. Most importantly, it anticipated one or more codes that would deal with "disinformation and news quality" and that would "address concerns regarding disinformation and credibility signalling" (Australian Government, 2019, p. 16, p. 7). It also referred specifically to the precedent of the EU Code.

There are two points worth noting about this guidance. First, while the policy statement clearly targeted "disinformation", it soon became apparent that the ACMA, which was charged with overseeing the process, required that it deal with both disinformation and misinformation. As this was not apparent from the policy statement and differed from the precedent of the EU Code – to which several of the industry participants were already signatories – it caused confusion and delay and a level of complexity in the Code itself which could have been avoided. Second, while news quality was ultimately addressed in the code, there was uncertainty over how it should be addressed and the extent to which it was appropriate for platforms to engage in credibility signalling. Furthermore, there was an overlap here with the News Code. Despite the ACCC stating clearly in its Concepts Paper in May 2020 that "flagging quality journalism" was a matter for the Disinformation Code not the News Code (ACCC, 2020, p. 27), Part IVBA of the *Competition and Consumer Act* now includes a requirement in s. 52X (related to, but not part of, the "minimum standards") which requires responsible digital platform corporations to ensure that "a proposal is developed for the designated digital platform service to recognise original covered news content when it makes available and distributes that content".

In relation to the role of the regulator, the policy decision for the ACMA to "have oversight of the codes and report to Government on the adequacy of the platforms' measures and the broader impacts of disinformation" (Australian Government, 2019, p. 7) always sat oddly with the explicit warning that: "Should the actions and responses of the platforms be found to not sufficiently respond to the concerns identified by the ACCC, the Government will consider the need for future measures" (p. 16). This is because the ACMA has no remit to regulate digital platforms under the *Australian Communications and Media Authority Act 2005* (Cth) ("ACMA Act") and no powers under the *Broadcasting Services Act 1992* (Cth) ("BSA") to make rules concerning disinformation. Amendments to both Acts could address these shortcomings, and in the meantime the ACMA's reporting function would appear to be covered by s. 10(1)(q) of the ACMA Act: "to report to, and advise, the Minister in relation to the broadcasting industry, internet industry and datacasting industry". However, in the event of code failure, there is no immediate solution. Legislative change would be required to give the ACMA powers

http://doi.org/10.18080/jtde.v9n2.415

to create its own standards or service provider rules to address the problem. Given the rapidly-changing environment and the possibility that harm could arise at short notice (for example, at election time), it would be preferable for the ACMA's reserve powers to be in place now.

In relation to accountability and transparency mechanisms, there are two concerns. The first is the lack of specificity in many of the commitments under the code, with only four of them (5.11, 5.26, 5.27, 5.28) being obligations to take specific action (e.g., 5.11 is a commitment to implement a facility for users to report certain behaviours). The more usual approach is for a commitment to be met by implementing policies designed to achieve an end (e.g., 5.14: "Signatories will implement policies and processes that aim to disrupt advertising and/or monetisation incentives for Disinformation"), followed by a list of examples of such policies that could be pursued (e.g., "restricting the availability of advertising services and paid placements on accounts and websites that propagate Disinformation"). This can be seen, at least in part, as a result of the outcomes-based approach to the design of the code which was proposed by the ACMA (ACMA, 2020, p. 24). As noted above, there were reasons for taking this approach, including the difficulty of prescribing rules in a fast-changing environment. However, Freiberg (2017, p. 491) has cautioned that, while this kind of approach gives the regulated companies flexibility in finding the most appropriate, and sometimes the lowest cost, means of addressing complying with the code, "there may be uncertainty about what constitutes acceptable compliance".

A second problem concerns the reporting arrangements. Most if not all submitters to the public consultation on the code were critical of the reporting arrangements set out in the draft Code. For example, Jacob Wallis (2020, p. 2) from the International Cyber Policy Centre at the Australian Strategic Policy Institute noted the absence of relevant key performance indicators (KPIs), while the Australian Communications Consumers Action Network (ACCAN) (2020, p. 3) suggested more specificity in articulating annual reporting commitments and that reporting ought to be standardised. Similar comments were made by Reset Australia (2020, p. 8) and AMAN (2020, p. 6). The Law Society of New South Wales Young Lawyers ("NSW Young Lawyers") (2020, p. 5) recommended:

> that a format be adopted for the substantive components of the annual reports provided by signatory Digital Platforms, that would allow for analysis of the efficacy of the measures taken, and to allow for future benchmarking.

Some of these observations draw on similar criticism of the EU Code and the resulting recommendations in a report for the European Commission (Plasilova *et al.*, 2020, pp. 89-95) for two classes of KPIs: "service level indicators" and "structural indicators". Administration of the EU Code has been complicated as a result of the signatories reporting on Code

http://doi.org/10.18080/jtde.v9n2.415

commitments in different ways without any common baseline, such as through the use of raw numbers of actions compared to, say, a proportion of overall actions. (See, for example, the independent assessment of the EU Code conducted by the European Regulators Group for Audio-visual Media Services, 2020). In a briefing note for the European Commission, James Pamment (2020, p. 2) said there was a lack of detail of data in the signatories' reports and success metrics for their efforts, and an inconsistency of approaches. Lack of uniformity in reporting was also noted in the EC's own staff assessment of reporting obligations in 2020, with a report noting, for example, that data on manipulative techniques was provided at an aggregated and global level (European Commission, 2020, p. 9).

The problems for transparency and accountability of a lack of specificity in both the commitments and the reporting requirements can be seen as connected to the failure to specify objectives. Freiberg has noted the need for precision in spelling out the objectives or requirements, and that the risks of information asymmetry between the regulator and the regulatee can leave the regulator compromised (Freiberg, 2017, p. 124). At the time of writing, the signatories to the Australian Disinformation Code had just published their initial three-month reports on implementation of the Code. These will be important sources for the ACMA's assessment of "the adequacy of the platforms' measures" (Australian Government, 2019, p. 7).

The international dimension

Finally, for both the News Code and the Disinformation Code, the international dimension of regulating digital platforms adds a level of complication not experienced when considering the use of self- or co-regulation for Australian telecommunications and broadcasting services. Feick & Werle (2011, p. 524) note that differences across jurisdictions in attitudes to free speech as well as to the criminality that should attach to some activities can make it difficult to forge international legal solutions, but that "international agreements among firms and associations are not necessarily easier to achieve than intergovernmental treaties". While, as noted above, the ACMA's framework would suggest that the small number of players in the digital platform environment provides support for the use of self-regulation, the need for local Australian subsidiaries to take advice, if not direction, from parent companies in other jurisdictions can, at the very least, affect timeliness of rule development and response, and, at worst, create adverse outcomes.

Conclusions

The shifting ground on the form of regulation considered appropriate for digital platforms – self-regulation, co-regulation, direct regulation – indicates the difficulties of finding solutions for a sector characterised by rapidly developing technologies and business and consumer practices (an argument for using self- or co-regulation) when also dealing with very powerful

http://doi.org/10.18080/jtde.v9n2.415

international players. These international firms, while prepared to introduce measures to deal with growing state and community concern over the spread of disinformation, did not have a great incentive to share revenue with local industry participants – and even less to create an international precedent by doing so. It is perhaps this quandary that leads to the irony in the outcome: a fiercely contested statutory scheme may be averted by the striking of private agreements that are not even the subject of a formal industry-based self-regulatory code.

In regulatory terms, this article has shown that a rigorous analysis of the best forms of regulation for these two issues was missing from the policy development phase. This is despite almost three decades of experimentation with co- and self-regulation; several policy reviews and reports over the last decade that can assist in the task; and the availability of a conceptual framework developed by the communications regulator for applying these forms of regulation. While that framework gives only a partial result when applied to the two schemes, it does show that self-regulation was never an appropriate tool for regulating news remuneration, but that it is at least a viable option for disinformation. Accordingly, it is difficult to see why the Government moved the News Code from the ACCC's recommendation of co-regulation to voluntary codes instead of straight to direct regulation, where it ended up.

This rather haphazard approach bears out the call by Lee & Wilding (2021, pp. 10-11) for a more holistic review of the regulation of telecommunications, broadcasting and online services in a way that might facilitate the incorporation of digital platforms. They point to flaws in the arrangements for developing broadcasting codes that remain unaddressed almost 30 years after they were introduced (2021, p. 12). Similarly, Flew & Wilding (2020, p. 61) referred to "the 'unfinished business' of reforming media regulation", with the current policy questions seeing a re-run of attempts in the early part of the last decade (through the Convergence Review) to find a new framework for the regulation of convergent communications – this time through the concept of "harmonisation" of laws applying to media and to digital platforms.

This is not to say, however, that the Australian Government is somehow recalcitrant by international standards, or that it has not faced some difficult conceptual as well as practical difficulties. Writing over a decade ago on the regulation of cyberspace, Feick & Werle (2010, p. 524) predicted that "Internet regulation will remain a patchwork of different regulatory approaches in continuous flux, no model being superior to any other". And while the ACMA's framework may give an incomplete picture on when to use self- and co-regulation for digital platforms, it does offer useful guidance, informed by extensive experience in other forms of communications regulation. It also allows for the preliminary comparative analysis presented above, prompting reflection on the need to rethink the role of co-regulation and its relationship to self-regulation, and the role of the regulator in both.

http://doi.org/10.18080/jtde.v9n2.415

The avoidance of co-regulation

Under the Disinformation Code regime, the ACMA looms over DIGI, setting out its expectations in code development and positioning itself (at the direction of government) as monitor of progress in implementation, auditor of annual reports, and checkpoint for the continued operation of self-regulation. This approaches the form of "meta-regulation" characterised by Coglianese & Mendelson (2010, pp. 156-157) where governments guide and oversee self-regulation, for example in requirements to develop detailed pollution prevention plans. In applying this to Australia, Freiberg (2017, pp. 120-25) noted the presence of such arrangements as early as the late 19th century and referred to various recent arrangements in Victoria, including in relation to drug and poison safety. Similarly, Tambini, Leonardi & Marsden (2008, p. 43), in sketching out forms of self- and co-regulation used in media content, noted what Schulz & Held (2001) (in relation to Germany) described as "regulated self-regulation", one form of which was "audited self-regulation".

Accordingly, there is nothing new or ground-breaking in the way the ACMA shadows DIGI, although it is not the norm for self-regulation in the communications sector. It also needs to be seen in the context of the well-established idea in regulatory theory about the need for an independent third party – usually governmental in some capacity, even in the background – to maintain pressure on participants. It should be recognised, however, that these ideas about the shadowy role of the state are usually articulated in relation to enforcement, which Gunningham & Rees (1997, p. 389) pinpointed as the main weakness of self-regulation. Similarly, it was on the aspect of enforcement that Ayres & Braithwaite (1992, p. 19) saw the state operating in the background of self-regulation as a "benign big gun". In the case of the Disinformation Code, however, it is reasonable to ask: how benign is the ACMA and how big is its gun? The Government has actively inserted the ACMA into the self-regulatory rule-making stage and given it some monitoring and assessment functions without an explicit remit, any formal compliance role, or any enforcement powers. Although the ACMA's "optimal conditions" framework suggests there is at least an arguable case for self-regulation, the approach evident in addressing disinformation may in fact be closer to co-regulation, while lacking the elements that would make a co-regulatory model effective.

Given these departures from established practices in communications regulation – specifically, the enhanced role of the state in self-regulation of disinformation and the development of a legislative scheme for news remuneration that was designed never to apply – and that the regulated entities are the same, and that, further, both schemes relate to information of one kind or another, how can we understand the place of these two schemes in our regulatory framework? Are these new forms of regulation?

http://doi.org/10.18080/jtde.v9n2.415

Making sense of the two schemes

Lee & Wilding (2020, p. 11) have described the involvement of ACMA in the Disinformation Code as "guided self-regulation", but it can also be characterised in the terms used by Bartle & Vass (2005) over 15 years ago. In reviewing the use of and potential for self-regulation and co-regulation – and in the process, noting the more advanced adoption of these forms of regulation in the Australian communications sector – the authors noted the importance of recognising the place of self-regulation within the modern regulatory state:

> The context of self-regulation today is therefore one of 'enclosure' by the regulatory state. Where self-regulation operates, it operates with the sanction, or support or threat of the regulatory state (Bartle & Vass, 2005, p. 44).

They depicted the relationship in the following figure (Bartle & Vass, 2005, p. 45):

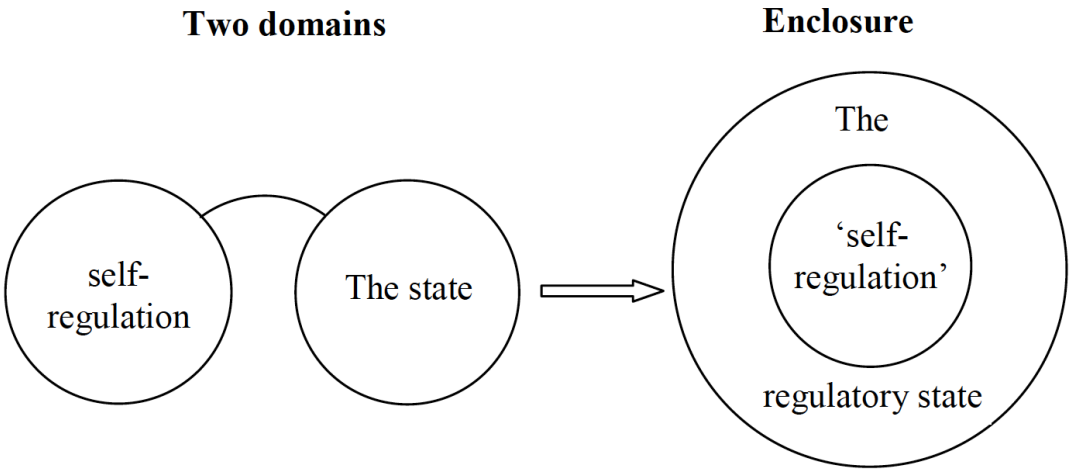


Figure 1. Bartle & Vass [2005, Figure 10], 'Two Worlds Become Enclosed'

Interestingly – and as a result of the unusual outcome where Google and Facebook have avoided the application of Part IVBA of the *Competition and Consumer Act* through the development of side agreements with publishers – this figure can perhaps be seen to apply to *both* the Disinformation Code (actual self-regulation) and the News Code (direct regulation that is not triggered).

A more recent and perhaps more developed way of viewing it is set out by Robert Gorwa (2019), who argues that a conception of the "platform governance triangle" – drawing on the idea of a "governance triangle" proposed by Abbott & Snidel (2009) as a means of representing corporate governance – that features firms, state actors and NGOs – can be applied to, among other things, the EU Code of Practice on Disinformation. Drawing on the observation that there can be difficulties in ensuring acceptable levels of governance among industry participants based in different jurisdictions, Gorwa (2019, p. 4) notes the development of

http://doi.org/10.18080/jtde.v9n2.415

international agreements, collaborations and standards setting bodies ("transnational governance initiatives") that attempt to overcome the obstacles facing black letter law solutions. He identifies various permutations of the three categories of actors applicable in the Internet environment (firms, NGOs and governments) and provides the EU Code as an example of a State-Firm initiative, under which: "The state role, when compared with traditional command-and-control legislation, is relatively limited to more of an informal oversight and steering role" (Gorwa, 2019, p. 10).

Interestingly, Flew *et al.* (2021, pp. 140-41) take issue with this analysis, citing the approach to news remuneration demonstrated in the Digital Platforms Inquiry and the News Code. Just as the analysis of the ACMA framework above noted the need to better account for interactions between different companies rather than between companies and consumers, Flew *et al.* point out that the chief actors in the Inquiry and the News Code were the technology firms and the news businesses (led by News Corp), although they also observe the activism of the ACCC, and in particular its Chair, Rod Sims. They say that this degree of "regulatory activism" on a domestic level was accompanied by "a new era of transnational cooperation among regulatory authorities" (p. 141) as these jurisdictions face similar attempts to grapple with platform regulation. Flew *et al.* in fact use the language of "co-regulation" to describe the relationship:

> [the Code], which will be overseen by the Australian Communications and Media Authority (ACMA) in a co-regulatory framework …, would sit between the state and the firm, as the state would be involved in brokering relations between competing corporate interests. (Flew *et al.*, 2021, pp. 134-135)

There is a certain logic here, and the authors were writing before the final version of the legislation was settled, but in some ways the News Code is distinctively *not* co-regulation, at least in the conventional Australian form described above. In the absence of agreement on remuneration, the scheme involves an independent party deciding the amount of remuneration, with other "minimum standards" also applying. And if the scheme is not triggered because the Treasurer believes there is sufficient contribution towards the news industry, in a sense there is no regulation.

This uncertainty surrounding *co-regulation* might help explain the inconsistency in how we approach *self-regulation*. Co-regulation is firmly established in the communications sector in Australia, but as the Consumer Safeguards Review and other preceding policy work have shown, there are fundamental problems with the way in which it has been applied. This seems to have affected its potential application in the sphere of digital platforms. There may be good reasons for not using co-regulation, but there may also be ways of fixing the problems experienced in telecommunications and broadcasting. This might help avoid the misplaced

http://doi.org/10.18080/jtde.v9n2.415

deployment of voluntary codes in contexts such as news remuneration, as well as the form of maladapted self-regulation devised to address disinformation.

In the meantime, perhaps the concept of "enclosure" used by Bartle & Vass (2005) is the most suitable way of depicting the anticipated outcome from Australia's recent attempts to regulate digital platforms. In the wake of Parliament passing the News Code legislation, there was much speculation as to who "won". The Government? Facebook and Google? News businesses? It is not yet entirely clear. And in relation to disinformation, self-regulation still needs to prove it can overcome some major flaws. With the development of both Codes, existing principles of regulatory design have taken quite a beating and may themselves need some reconsideration to cope with the emerging, international environment. A new version of the ACMA framework, capable of more nuanced application to the digital platform environment and offering more specificity on the distinctions between self- and co-regulation, would be a useful resource. Meanwhile, the digital platforms have, at least temporarily, been corralled. But it would be overstating the outcome to say they have been enclosed.

Declaration

The author was part of a team commissioned by the Australian Competition and Consumer Commission to conduct research for the Preliminary Report of the Digital Platforms Inquiry. He was also part of a team commissioned by DIGI to provide research and to assist in the development of the Disinformation Code. He made policy submissions on the development of the News Media Bargaining Code and the Consumer Safeguards Review.

References

Abbott, K., & Snidal, D. (2009). The governance triangle: Regulatory standards institutions and the shadow of the state. In W. Mattli & N. Woods (Eds.). *The politics of global regulation* (pp. 44–88). Princeton University Press.

Attorney-General's Department. (2020). *Privacy Act review: Issues paper*. https://www.ag.gov.au/integrity/publications/review-privacy-act-1988-cth-issues-paper

Attorneys-General (Defamation Working Party). (2021). *Review of Model Defamation Provisions – Stage 2: Discussion paper*. https://www.justice.nsw.gov.au/justicepolicy/Pages/lpclrd/lpclrd_consultation/review-model-defamation-provisions.aspx

Australian Communications and Media Authority (ACMA). (2020). *Misinformation and news quality on digital platforms in Australia: A position paper to guide code development*. https://www.acma.gov.au/australian-voluntary-codes-practice-online-disinformation

Australian Communications and Media Authority (ACMA). (2015). *Optimal conditions for effective self- and co-regulatory arrangements*: *Occasional paper*.

http://doi.org/10.18080/jtde.v9n2.415

https://www.acma.gov.au/publications/2015-06/report/optimal-conditions-effective-self-and-co-regulatory-arrangements-2015-edition

Australian Communications and Media Authority (ACMA). (2011). *Optimal conditions for effective self- and co-regulatory arrangements. Occasional paper*. https://www.acma.gov.au/publications/2015-06/report/optimal-conditions-effective-self-and-co-regulatory-arrangements-2015-edition

Australian Communications and Media Authority Act 2005 (Cth)

Australian Communications Consumers Action Network (ACCAN). (2020). *Submission to Digital Industry Group Inc: Australian Code of Practice on Disinformation*. https://digi.org.au/submissions/

Australian Competition and Consumer Commission (ACCC). (2020). *Mandatory News Media Bargaining Code: Concepts paper*. https://www.accc.gov.au/focus-areas/digital-platforms/news-media-bargaining-code/concepts-paper

Australian Competition and Consumer Commission (ACCC). (2019). *Digital Platforms Inquiry: Final report*. https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report

Australian Government. (2020). *Australian Government guide to regulatory impact analysis*. (2nd ed.). https://pmc.gov.au/resource-centre/regulation/australian-government-guide-regulatory-impact-analysis

Australian Government. (2019). *Regulating in the digital age: Government response and implementation roadmap for the Digital Platforms Inquiry*. https://treasury.gov.au/publication/p2019-41708

Australian Law Reform Commission (ALRC). (2012). *Classification—content regulation and convergent media: Final report*. (ALRC report 118). https://www.alrc.gov.au/publication/classification-content-regulation-and-convergent-media-alrc-report-118/

Australian Muslim Advocacy Network (AMAN). (2020). *Policy submission to DIGI on the Australian Code of Practice on Disinformation*. https://digi.org.au/submissions/

Ayres, I., & Braithwaite, J. (1992). *Responsive regulation: Transcending the deregulation debate*. Oxford University Press

Bartle, I., & Vass, P. (2005). *Self-regulation and the regulatory state: A survey of policy and practice*. (Centre for the Study of Regulated Industries research report 17). https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.553.3190&rep=rep1&type=pdf

Broadcasting Services Act 1992 (Cth)

Caffarra, C., & Crawford, G. (2020, September 25). The ACCC's News Media Bargaining Code: Experimenting with "decentralized regulation" of dominant digital platforms. *ProMarket*. https://promarket.org/2020/09/25/the-acccs-news-media-bargaining-code-experimenting-with-decentralized-regulation-of-dominant-digital-platforms/

Centre for Responsible Technology. (2020). *Ensuring a strong and meaningful code on disinformation: Submission to the Australian Code of Practice on Disinformation*. https://digi.org.au/submissions/

Coglianese, C., & Mendelson, E. (2010). Meta-regulation and self-regulation. In R. Baldwin, M. Cave, & M. Lodge (Eds.). *The Oxford handbook of regulation* (pp. 146-168). Oxford University Press.

Communications Alliance. (2019). *Telecommunications Consumer Protections Code*. Industry Code C628:2019. https://www.commsalliance.com.au/Documents/all/codes/c628

Communications Decency Act of 1996 47 USC §§ 230

Competition and Consumer Act 2010 (Cth)

Council of Australian Governments. (2007). *Best practice regulation: A guide for ministerial councils and national standard setting bodies*. https://pmc.gov.au/sites/default/files/publications/COAG_best_practice_guide_2007.pdf

Department of Communications (DOC). (2014). *Regulating harms in the Australian communications sector: Observations on current arrangements*. (Policy background paper no. 2). https://www.communications.gov.au/publications/regulating-harms-australian-communications-sector-policy-background-paper-no2

Department of Communications and the Arts (DOCA). (2020). *Review of Australian classification regulation*. https://www.communications.gov.au/have-your-say/review-australian-classification-regulation

Department of Communications and the Arts (DOCA). (2019). *Online safety legislation reform: Discussion paper*. https://www.communications.gov.au/have-your-say/consultation-online-safety-reforms

Department of Communications and the Arts (DOCA). (2016, October). *Review of the Australian Communications and Media Authority: Final report*. https://www.communications.gov.au/documents/review-australian-communications-and-media-authority-final-report

Department of Infrastructure, Transport, Regional Development and Communications (DITRDC). (2020). *Consumer Safeguards Review—part C—choice and fairness: Consultation paper*. https://www.communications.gov.au/have-your-say/consumer-safeguards-review-consultation-part-c-choice-and-fairness

Digital Industry Group Inc. (DIGI). (2021). *Australian Code of Practice on Disinformation and Misinformation 2021*. Available at https://digi.org.au/wp-content/uploads/2021/02/Australian-Code-of-Practice-on-Disinformation-and-Misinformation-FINAL-PDF-Feb-22-2021.pdf

Digital Industry Group Inc. (2020, May). Disinformation Code. https://digi.org.au/disinformation-code/

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (e-Commerce Directive) (entered into force 8 June 2000)

European Commission. (2018). *EU Code of Practice on Disinformation*

European Commission. (2020). *Commission staff working document: Assessment of the code of practice on disinformation - achievements and areas for further improvement*.

http://doi.org/10.18080/jtde.v9n2.415

https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement

European Regulators Group for Audiovisual Media Services (ERGA). (2019). *ERGA report on disinformation: Assessment of the implementation of the Code of Practice*. https://erga-online.eu/wp-content/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf

Explanatory Materials to the Exposure Draft Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2020. https://www.accc.gov.au/focus-areas/digital-platforms/news-media-bargaining-code/draft-legislation

Exposure Draft Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2020 (Cth). https://www.accc.gov.au/focus-areas/digital-platforms/news-media-bargaining-code/draft-legislation

Facebook. (2020a). *Facebook response to the Australian Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2020*. https://www.accc.gov.au/focus-areas/digital-platforms/news-media-bargaining-code/submissions-to-exposure-draft

Facebook. (2020b). *Response to the Australian Mandatory News Media Bargaining Code concepts paper*. https://www.accc.gov.au/focus-areas/digital-platforms/news-media-bargaining-code/submissions-to-concepts-paper

Feick, J., & Werle, R. (2010). Regulation of cyberspace. In R. Baldwin, M. Cave, & M. Lodge (Eds.). *The Oxford handbook of regulation* (pp. 523-547). Oxford University Press.

Flew, T. (2019). The platformized Internet: Issues for Internet law and policy. *Journal of Internet Law*, *22*(11), 3-16.

Flew, T. & Wilding, D. (2021). The turn to regulation in digital communication: the ACCC's Digital Platforms Inquiry and Australian media policy. *Media, Culture & Society*, *43*(1), 48-65. https://doi.org/10.1177/F0163443720926044

Flew, T., Gillet, R., Martin, M., & Sunman, L. (2021). *Return of the regulatory state: A stakeholder analysis of Australia's Digital Platforms Inquiry and online news policy*. *The Information Society*, *37*(2), 128-145. https://doi.org/10.1080/01972243.2020.1870597

Free TV Australia. (2015). *Commercial Television Industry Code of Practice*. https://www.freetv.com.au/resources/code-of-practice/

Freiberg, A. (2017). *Regulation in Australia*. The Federation Press.

Frydenberg, J. (2020). Here's news: We'll hold digital giants to account. *The Australian*, 20 April 2020, p. 10.

Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Harvard University Press.

Google. (2020a). *Draft News Media and Digital Platforms Mandatory Bargaining Code: Submissions in response*. https://www.accc.gov.au/focus-areas/digital-platforms/news-media-bargaining-code/submissions-to-exposure-draft

Google. (2020b). *Mandatory News Media Bargaining Code: Response to the ACCC's concepts paper*. https://www.accc.gov.au/focus-areas/digital-platforms/news-media-bargaining-code/submissions-to-concepts-paper

Gorwa, R. (2019). The platform governance triangle: Conceptualising the informal regulation of online content. *Internet Policy Review*, *8*(2), 1-22.

Gunningham, N., & Reese, J. (1997). Industry self-regulation: An institutional perspective. *Law and Policy*, *19*(4), 363-414.

Helberger, N., Pierson, J. & Poll, T. (2018). Governing online platforms: From contested to cooperative responsibility. *The Information Society*, *34*(1), 1-14. https://doi.org/10.1080/01972243.2017.1391913

Law Society of New South Wales Young Lawyers, The. (2020). *Submission on the Digital Industry Group Inc's Draft Australian Code of Practice on Disinformation*. https://digi.org.au/submissions/

Lee, K. (2018). *The legitimacy and responsiveness of industry rule-making*. Hart Publishing.

Lee, K., & Wilding, D. (2021). The case for reviewing broadcasting co-regulation. *Media International Australia*. https://doi.org/10.1177%2F1329878X211005524

Leonard, P. (2021, March 12). The battles between Google, Facebook, and news media proprietors over fair value exchange for news content. *Competition Policy International*. https://www.competitionpolicyinternational.com/the-battles-between-google-facebook-and-news-media-proprietors-over-fair-value-exchange-for-news-content/

Lindsay, D. (in press). Australia and EU policy responses to algorithmic news distribution: A comparative analysis. In J. Meese and S. Bannerman (Eds). *The algorithmic distribution of news*. Palgrave Macmillan.

Online Safety Bill 2020 (Cth)

Oster, J. (2016). *European and international media law*. Cambridge University Press.

Pamment, J. (2020). *EU Code of Practice on Disinformation: Briefing note for the new European Commission*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2020/03/03/eu-code-of-practice-on-disinformation-briefing-note-for-new-european-commission-pub-81187

Pash, C. (2021, May 6). How much are Google and Facebook paying for news in Australia? *AdNews*. https://www.adnews.com.au/news/exclusive-how-much-are-google-and-facebook-paying-for-news-in-australia

Picard, R. (2020). *Media and communications policy making: Processes, dynamics and international variations*. Palgrave Macmillan.

Plasilova, I., Hill, J., Carlberg, M., Goubet, M., & Procee, R. (2020). *Study for the "Assessment of the implementation of the Code of Practice on Disinformation": Final report*. European Commission. https://digital-strategy.ec.europa.eu/en/library/study-assessment-implementation-code-practice-disinformation

Reset Australia. (2020). *Submission on the Australian Code of Practice on Disinformation*. https://digi.org.au/submissions/

Riordan, J. (2016). *The liability of Internet intermediaries*. Oxford University Press.

Senate Economics Legislation Committee. (2021). *Report on Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2020 [Provisions]*. https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/TLABNewsMedia

Shultz, W. & Held, T. (2001). *Regulated self-regulation as a form of modern government*. Verlag Hans Bredow Institut.

Suzor, N. (2019). *Lawless: The secret rules that govern our digital lives*. Cambridge University Press.

Tambini, D., Leonardi, D., & Marsden, C. (2008). *Codifying cyberspace: Communications self-regulation in the age of Internet convergence*. Routledge.

Telecommunications Act 1997 (Cth)

Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2020 (Cth)

Van Dijck, J., Poell, T., & De Wall, M. (2018). The platform society: Public values in a connective world. Oxford University Press.

Wallis, J. (2020). *Submission to the UTS Centre for Media Transition's consultation process on the DIGI Group's Australian Code of Practice on Disinformation*. https://digi.org.au/submissions/

http://doi.org/10.18080/jtde.v9n2.415

Dude, Where's My Data? The Effectiveness of Laws Governing Data Breaches in Australia

Jack Hile
Macquarie University

Abstract: The increasing prevalence of large-scale data breaches prompted Australia to strengthen the Privacy Act by enacting the Privacy Amendment (Notifiable Data Breaches) Act to regulate the behaviour of entities entrusted with personal data. However, this paper argues that these legislative instruments are ineffective when dealing with data breaches and their associated problems. In supporting this conclusion, this paper first develops a criterion for effective data breach law, and then evaluates the Australian framework against this criterion to determine its operational effectiveness. In addition, this paper analyses practical developments in the area of data-breach law to garner insights as to how the Australian framework can be made more effective. Ultimately, this paper concludes that the Australian framework is ineffective when dealing with large-scale data breaches, and recommends future legislative amendment as a means of bolstering its effectiveness.

Introduction

The growing reliance on the Internet as a means of processing and storing personal data has presented a slew of issues for society as a whole, the most prominent being the unauthorised access to personal data by third parties, and the associated consequences arising from its misuse. As personal data rapidly becomes the 'life-blood of retail' (Aguirre *et al.*, 2015, p. 34), it has become increasingly common for online vendors to acquire personal data from customers under the assumption that this data will be securely stored (Morey *et al.*, 2015). However, in recent times, the threat of unauthorised access to personal data and the malicious consequences that may follow have increased as the frequency of large-scale data breaches has grown (Winder 2019).

This paper will employ the meaning of 'data breach' espoused by Geistfeld (2017, pp. 386-387), who defined a data breach as the theft or unauthorised access to one's confidential information that has been entrusted to another in a business transaction. The prominence of such breaches can be seen through recent examples such as the Microsoft Exchange

http://doi.org/10.18080/jtde.v9n2.381

vulnerability which affected tens of thousands of servers globally (Palmer 2021), and other megalithic examples, such as Sony, which had the financial records of 77 million user accounts compromised (Quinn & Arthur 2011), or Equifax, who were subject to a data breach that exposed the personal data of over 140 million customers (Swinhoe 2020). Australian entities have also been subject to major data breaches, with ServiceNSW, a provider of government services, being subject to a data breach in 2020 that exposed the personal data of 186,000 customers (Bungard 2020).

As an attempt to better regulate the conduct of parties who are entrusted with personal data, the *Privacy Amendment* (*Notifiable Data Breaches Act) 2017 (Cth)* ('**NDB Scheme**') was introduced to impose notification and reporting obligations on specified bodies to notify affected individuals in the event of an eligible data breach. However, while reporting obligations are imposed and a complaints system has been created, the NDB Scheme has two main faults. Specifically, individuals are unable to commence legal action on their own volition, and there is no scheme in place that prescribes compensation or damages for affected individuals (Smith & Bloch 2018).

Aim of research

The central aim of this study is to evaluate the effectiveness of the Australian legal and regulatory framework and analyse potential reforms in the event it is deemed ineffective. To achieve this central objective, the paper will: (1) develop a theoretical framework for determining what constitutes effective data breach law; (2) increase understanding of the effectiveness of Australian law regarding its ability to recognise and compensate data breaches**;** (3) consider academic, legislative, and judicial materials to create a roadmap for future domestic reform; and (4) develop options to guide future legislative reform in Australia.

The existing literature

There is a distinct lack of scholarly literature on the provision of compensation following a data breach in the Australian context. However, there have been some contextual studies into the operation of the Australian legislation regarding data breaches generally. Alazab, Hong & Ng (2021) maintain that the NDB Scheme gives entities responsible for data protection significant leeway while imposing responsibilities on data subjects who must shoulder the consequences of a data breach (2021, p. 28). Further, Daly (2018, p. 489) has noted that under the current framework, individuals are denied an equal access to the courts, while Selvadurai, Kisswani & Khalaileh (2017, p. 13) have opined that there is room for further initiatives in Australia. However, there is currently no academic discourse regarding the role of

http://doi.org/10.18080/jtde.v9n2.381

compensation in Australian data-breach law, and this paper will therefore fill a void in the Australian jurisprudential landscape.

While no literature expressly considers the Australian context, various theoretical frameworks with the potential to provide legal redress to individuals following a data breach have been developed. Most notably, Bergelson (2003, pp. 436-443) recommends the attachment of a bundle of rights and therefore a quantifiable monetary value to personal data, while Samuelson (2000, p. 1129) has maintained that copyright protection should be extended to personal data as a method of protection. Additionally, Lim (1999, p. 90) has proposed a contractual model for the regulation of breaches in data security. However, the abovementioned proposals all focus on the determination of liability in the event of a breach and do not consider the inherent difficulties that arise when providing compensation if liability is found. This paper, by focusing on the availability of compensation for individuals, will consider data-breach law from a novel theoretical standpoint and will provide new recommendations in a historically shunned area of discussion.

Finally, this paper will draw insights from the wider international context, most notably in the European Union ('**EU**') under the *General Data Protection Regulation* ('**GDPR**'). It is prudent to note, in line with Lynskey (2017, p. 285), that the EU data protection governance structure has not attracted much doctrinal attention. However, a distinct focus will be placed on the work of Chamberlain & Reichel (2019, pp. 8-9), who note that the compensation provisions of the GDPR are unclear and grant national courts significant flexibility. Further, this paper will assess the work of O'Dell (2017, p. 113), who maintains that the broad discretion placed on national courts undermines the consistent application of the GDPR, and Lynskey (2017, p. 261), who reiterates that the reliance on the discretion of national courts and supervisory authorities erodes the effectiveness of data protection rules generally.

Theoretical Framework for Determining What Constitutes Effective Data-Breach Law

Before the effectiveness of the Australian legislative framework can be critiqued it is prudent to first outline the criteria for effective data-breach law. This paper will consider effectiveness under three main categories, namely: the proper attribution of liability following a data breach, a direct right of action for individuals, and the existence of a consistent compensation mechanism (together '**the criteria for effective data-breach law**'). Each of the abovementioned categories will be considered separately.

http://doi.org/10.18080/jtde.v9n2.381

Attributing liability in data breach matters

The benefits of a defined liability model are espoused by Mitrakas (2011, p. 129), who notes that attributing liability in the information security context is a useful means of reducing social costs, and that the ability to apportion liability between information owners and information security service providers is desirable, as it contributes to a reduction in transaction costs.

However, while legal effectiveness is in many ways defined by the ability to identify which party is legally at fault, care must be taken when creating a mechanism to attribute liability. Specifically, the level of care demanded by legislation must be carefully weighed against the practicality of feasible protection measures available to businesses. In this sense Raz (2010, p. 6), while discussing liability rules generally, correctly notes that, if the level of care demanded by the law is inappropriately high, it may invalidate the claim that the liability resulting from a data breach is legitimately tied to an act of negligence. As such, it is evident that a liability model must be balanced to accurately apportion blame, which has led Mitrakas to conclude that assessing the liability of a service provider is a complex task (Mitrakas, 2011, p. 131). However, despite this complexity, this paper accepts that the ability to attribute fault is an essential part of an effective legal system, and must exist in some form to guarantee the success of a data-breach law.

Academic discourse has supported a slew of workable frameworks that are capable of attributing liability in data breach matters, most notably the least cost avoider model ('**LCA**'), the law of contract, and the legislative model that regulates conduct through statute. These frameworks will be individually assessed to determine which is the most appropriate for data-breach matters.

The Least Cost Avoider Model

The LCA model operates on the premise that, when an accident could have been avoided if a party took care, the obvious approach is to place liability on the party who could have prevented the accident at the lowest cost (Dari-Mattiacci & Garoupa, 2007, p. 235). This approach assists in identifying who should be deemed liable for an incident, and has a positive external effect on the risk landscape as a whole. As parties understand their liabilities in the event care is not taken, entities generally exercise higher levels of care, which contributes to an overall increase in safe practice, and contributes to a decrease in the magnitude and frequency of risk-based activities overall (Carbonara *et al.*, 2016, pp. 173-175). Examples of this approach include, but are not limited to, cars slowing down to avoid a collision, manufacturers exercising a higher level of care to avoid faulty goods being provided to consumers (Dari-Mattiacci & Garoupa, 2007, p. 236), or data controllers investing more heavily in data security to avoid a data breach occurring.

http://doi.org/10.18080/jtde.v9n2.381

However, while the LCA model assists in mitigating the occurrence of accidents generally, the model has three main deficiencies. First, when attributing liability, the LCA model relies on information that, while available at the time of adjudication, may not have been available to the parties when they decided whether or not to exercise higher levels of care (Dari-Mattiacci & Garoupa, 2007, p. 237-238). As a result, parties may be deemed liable for a failure to take preventative action in circumstances where they were unaware they had an obligation to do so (Raz, 2010, p. 16). This approach to liability has been criticised by Meglio (2020, pp. 1225-1226) who, while discussing data breach law generally, warns against the imposition of unclear compliance obligations in circumstances where the risks to data subjects are poorly understood.

Secondly, the LCA model requires that liability be attributed entirely to the party with the lowest costs of care (Dari-Mattiacci & Garoupa, 2007, p. 245). As such, parties may forego taking preventative measures if they are confident that they are not the party with the lowest cost of care, thereby shouldering the burden to take preventative measures on a singular party. Thirdly, under the LCA model, parties will likely have an understanding of what fines will be issued if they are found to be liable for a data breach. Further, parties will understand the cost of implementing more stringent security measures. As such, parties may decide not to comply with the requirement to implement protective measures if they know the costs of care are higher than the fine that will be issued if they are found to be liable for a data breach (Dari-Mattiacci & Garoupa, 2007, p. 246). This allows parties to purposely breach their legal obligations on the understanding that compliance with the law costs more than non-compliance. As such, parties are able to selectively comply with their obligations, which undermines the effectiveness of the LCA model.

Contract law

One solution to the issue of liability in data-breach matters would be to allow parties to decide who is liable through the use of contractual provisions (Lim, 1999, p. 90). Kecsmar (2003, p. 280-283) correctly maintains that contractual clauses can establish clear rights and responsibilities that introduce legal certainty into the area of data-breach law. In addition, Massey (2010, p. 89) validly asserts that through contract parties can opt to circumvent the need for arbitration which may make the determination of cases more expedient. Further, Lim (1999, p. 90) affirms that contract law is already a widely accepted means of regulation that is international in scope and adaptable to changing social circumstances. Finally, Lindqvist (2017, pp. 59-60) has noted that the use of contracts is beneficial as it allows stakeholders to include broader forms of damage that can be specifically tailored to the data that is the subject of the contract. This allows individuals to determine what constitutes adequate damages in the event of a breach of contract, which facilitates a more balanced distribution of liability

http://doi.org/10.18080/jtde.v9n2.381

between data controllers and data subjects (Lindqvist, 2017, pp. 59-60). However, as will be discussed below, the effectiveness of contract law is limited by two key deficiencies that render it inoperable when dealing with data breaches and their associated consequences.

First, while contracts allow parties to establish their own liability and compensation provisions, an imbalance in bargaining power may allow data controllers to limit their own legal liability or restrict the rights of data subjects. As Lindqvist (2017, p. 62) notes, it is usually the data controller that decides the terms of a contract. Further, standard-form contracts are often written in a 'take it or leave it' form where, if an individual does not agree to the terms of the contract, they are precluded from using a product or service (Lindqvist, 2017, p. 62). This situation has led Prins (2006, p. 292) to conclude that, as a result of an imbalance in bargaining power, individuals faced with a standardised contract are likely to accept any contractual terms that data controllers offer them. The use of 'take it or leave it' terms under the threat of exclusion of use therefore allows data controllers to coerce individuals into contracts that they may ordinarily be reluctant to agree to (Prins, 2006, p. 292).

Secondly, the feasibility of contract law as a means of attributing liability is hindered by its lack of adaptability. The subject of a contract is fixed at the time it is drafted and can often only be altered through express agreement by the contracting parties. Personal data, however, when digitised, can rapidly change form and location, which makes it difficult to draft contracts involving personal data with precision. For example, the holder of personal data may transfer the data to a server in a different country or convert data into a different file type. In both of the above examples a contract would likely need to be amended each time the form of personal data changed, which has led Lindqvist to conclude that contracts relating to personal data are often difficult to draft, lead to confusion among stakeholders, and will likely cause problems in the future (Lindqvist, 2017, p. 62). As such, the inability of contracts to adapt to a fast-paced technological landscape limits their ability to consistently attribute liability in data breach matters.

Legislation

While the LCA model and contract law have merit, commentators have noted that in general legislation can provide better incentives for compliance than ordinary liability rules (Dari-Mattiacci & Garoupa, 2007, p. 236). Further, research to date suggests that data-breach notification laws may have an overall positive effect on encouraging better data security practices (Daly, 2018, p. 480), which reduces the risk of a data breach generally. Additionally, Solove maintains that there must be a centralised system by which individuals can exercise their rights, which he states can be achieved through information regulation that prescribes a set of actions that must be followed (Solove, 2006, p. 370). This paper agrees with the above findings, and accepts that an enforceable legislative scheme is the most favourable model by

http://doi.org/10.18080/jtde.v9n2.381

which liability can be attributed effectively in data-breach matters. This is due to the fact that a codified negligence standard creates an environment where parties clearly understand their obligations when dealing with personal data (Dari-Mattiacci & Garoupa, 2007, p. 239).

This paper acknowledges the argument that legislation may disproportionately affect small and young firms by creating an anti-competitive market landscape (Campbell *et al.*, 2015, p. 67). That said, Solove (2006, p. 384) correctly notes that modern society is already heavily regulated, and the inclusion of a negligence standard in a domestic legal framework will not impede economic development in any significant manner. As such, this paper considers that legislation can effectively establish a liability standard capable of consistent application, thereby making it the most appropriate liability model for the purposes of the following discussion.

Conclusions on liability

While the LCA model and contract law both present a feasible method of attributing liability in the event of a data breach, this paper aligns with the view of Garoupa in maintaining that regulation generally provides better incentives than ordinary liability models (Dari-Mattiacci & Garoupa, 2007, p. 236). As such, the scope of the following discussion, when discussing liability, will be limited to statutory provisions that regulate the conduct of parties following a data breach.

A direct right of action for individuals

The second criterion of effective data breach law is the ability of individuals to directly enforce the law in court. As will be discussed below, this paper agrees that meaningful access to the courts is an essential feature of a functional legislative scheme, which Abel maintains can only be secured if a litigant can identify the central issues in a case and present evidence and arguments in a court regarding those issues (Abel, 2012, p. 808). This is of particular importance in respect of data-breach laws, as modern technology has created a range of new legal issues that warrant judicial determination (Dolbow, 2017, p. 1935).

That said, it is important to recognise that there are several reasons why a direct right of action may not be feasible, most notably the fact that it might strain judicial resources. For example, Jamison (2019, p. 35) has warned that a direct right of action may give rise to an increase in the number of nuisance suits, while Nieuwesteeg & Faure (2018, p. 1238) have argued that deferring jurisdiction away from supervisory bodies will detrimentally affect the efficiency of the courts. However, the risk of frivolous suits can be overcome with sufficient safeguards, and the introduction of a direct right of action will ensure that individuals are able to effectively assert their rights (Jamison, 2019, p. 35). As such, the increased workload placed on the courts is an unfortunate collateral impact that is required to ensure all affected individuals enjoy

http://doi.org/10.18080/jtde.v9n2.381

unequivocal access to justice in the event of a data breach. Ultimately, while a direct right of action will adversely affect judicial efficiency, it is arguable that this right would tailor the law specifically to the needs of data breach victims (Alazab *et al.*, 2021, p. 27). As a result, this paper accepts that a direct right of action is a necessary component of effective data breach law.

A consistent compensation mechanism

The final criterion of effective data-breach law is the ability of individuals to receive compensation in the event of a data breach. Timmel (2012, p. 48) has noted that the costs of data security incidents to data subjects are real and material, which supports the notion that individuals should be entitled to some form of compensation to remedy the consequences that flow from a data breach.

That said, the provision of compensation is challenging due to the fact that the damage suffered as a result of a data breach is often fluid and difficult to quantify. For example, if an individual's social media account is lost or stolen as a result of a data breach, it is likely that the individual will wish to be compensated for the loss of the account. However, studies have shown that the value of data (and by extension the damage suffered as a result of its loss) can fluctuate significantly (Glikman & Glady, 2015), which makes it difficult to determine whether compensation is appropriate and, if so, what damages would be adequate to compensate for the loss. As such, it is likely that a court, when attempting to compensate a plaintiff for the loss of personal data by a defendant, would have difficulties determining adequate compensation. This is especially so given that traditional valuation methods have been ineffective in data breach matters (Sidgman & Crompton, 2016, p. 172).

This paper recognises that compensating a plaintiff for loss suffered as a result of a data breach is a difficult task (Stewart, 2005, p. 21). However, this paper does not accept that this difficulty by itself justifies a legislative approach where courts are unable to compensate individuals. As will be discussed later in this paper, it is unimportant whether the compensation provided is in the form of material or non-material damages, it is only necessary that a legislative framework is able to compensate individuals in the event of a data breach.

The practical operation of the criteria

The aforementioned criteria for effective data-breach law operate in tandem to create a legislative model in which legal wrongdoing and its consequences are recognised and adequately compensated. The framework for attributing liability, a direct right of action to a court, and a consistent and clear compensation model all contribute to a well-rounded and

http://doi.org/10.18080/jtde.v9n2.381

effective legal model that is capable of adapting to emerging technological issues in the area of data-breach law.

The Effectiveness of the Present Australian Legal Framework

To assess the effectiveness of Australian law it is prudent to consider its operation in line with the criteria for effective data-breach law. However, this paper will first outline the provisions of the *Privacy Act 1988* (‘**PA**’) and the NDB Scheme that regulate the storage and use of personal data in Australia. It is noted that the PA and NDB scheme refer to ‘personal information’. However, for the purposes of consistency in terminology throughout this paper, the term ‘personal data’ will be used instead.

Australia’s legislative framework

The Privacy Act

The handling and use of personal data in the Australian context are governed by the PA. The PA contains the Australian Privacy Principles (‘**APPs**’), which impose obligations on Commonwealth agencies, private companies with an annual turnover of more than $3 million, and private health providers irrespective of their size (‘**APP Entities**’) (PA, 1988, s. 6). While the PA provides for thirteen APPs that govern the use and disclosure of data, for the purposes of this paper only Principles six and eleven are relevant, and the following discussion will be restricted as such. APP 6 maintains that, if an APP entity holds data about an individual that was collected for a specific purpose, the APP Entity must not use or disclose the data for another purpose unless the individual has consented to the secondary purpose (PA, 1988, sch. 1 pt 3 cl. 6.1-6.2(a)). APP 11, in complementing APP 6, states that, if an APP Entity holds personal data, the entity must take reasonable steps to protect the data from misuse, interference and loss (PA, 1988, sch. 1 pt 4 cl. 11.1(a)), as well as from unauthorised access, modification or disclosure (PA, 1988, sch. 1 pt 4 cl. 11.1(b)). In other words, APP 11 provides that APP Entities must take reasonable precautions to prevent data breaches in any circumstance, whether inadvertent, deliberate, or on account of external malicious sources. In the event of non-compliance, an individual must first make a complaint to the organisation that has allegedly breached an APP and, if the organisation does not respond satisfactorily, the individual may then make a complaint to the federal Privacy Commissioner (PA, 1988, s. 36). The abovementioned provisions set a baseline standard for personal data protection in Australia and create a complaints mechanism for individuals in the event their personal data is improperly disclosed by an APP Entity.

http://doi.org/10.18080/jtde.v9n2.381

The Privacy Amendment (Notifiable Data Breaches) Act

In addition to the PA, the NDB Scheme was enacted to strengthen data protection legislation and better protect the rights of individuals as society progresses to a predominantly online realm (Australian Law Reform Commission, 2008, p. 61). The NBD Scheme is located under Part IIIC of the PA, and imposes an obligation on APP Entities to notify both the federal Privacy Commissioner and any affected individuals in the event an eligible data breach occurs (PA, 1988, ss 26WK(2), 26WL(2)). An eligible data breach is defined to be any unauthorised access to, or unauthorised disclosure of, personal data, where a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the data relates (PA, 1988, s. 26WE(2)(a)). In determining whether serious harm is likely to be suffered, regard is to be had to the kind and sensitivity of the data (PA, 1988, s. 26WG(c)-(d)), the persons who have obtained the data (PA, 1988, s. 26WG(g)), whether the data is protected (PA, 1988, s. 26WG(e)-(f)), the nature of the harm (PA, 1988, s. 26WG(i)), and any other relevant matters (PA, 1988, s. 26WG(J)).

The effectiveness of the Australian legal framework

This paper recognises that the Australian legal framework is successful in attributing liability in the event of a data breach. The PA expressly states which entities will be subject to its provisions (PA, 1988, s. 6), and what circumstances must be met for a data breach to be considered 'eligible' for notification (PA, 1988, s. 26WE(2)). In addition, the framework accounts for situations where multiple APP Entities jointly hold personal data that is subject to a data breach. For example, an eligible data breach of one entity will also be considered an eligible data breach of all entities that hold the same data (OAIC, 2019), and all entities are generally responsible for complying with the NDB scheme in relation to the affected data. As such, the Australian legal framework is capable of attributing liability to either a singular party or multiple parties in the event of a data breach.

Despite the ability of the Australian framework to attribute liability, this paper recognises that the framework has two main faults. First, the framework fails to provide individuals with a right of direct access to the courts. Secondly, there is no compensation model that can be relied on by individuals in the event of a data breach. For clarity, these issues will be discussed separately.

A direct right of action for individuals

Given the High Court has failed to recognise a general right to privacy or any corresponding tortious action for a breach of privacy (ABC v Lenah Game Meats, 2001; Smethurst v Commissioner of Police, 2020, para 48), individual complaints regarding a data breach must be directed through the Office of the Australian Information Commissioner ('**OAIC**'). The

http://doi.org/10.18080/jtde.v9n2.381

OAIC is entitled to investigate complaints, make determinations, and issue fines in circumstances where non-compliance is found (PA, 1988, ss 36A, 40, 52). However, there are concerns regarding the capacity of the OAIC to respond in data-breach matters. In this sense, Coyne (2015) has noted that insufficient funding has impacted the OAIC's ability to adequately carry out its investigative functions, while Daly (2018, p. 489) has maintained that the OAIC lacks the capacity to properly investigate each claim. These limitations are of particular importance when considering large-scale data breaches in which hundreds of thousands or even millions of individuals are affected (Quinn & Arthur, 2011), as the OAIC is unable to carry out its investigative function to an adequate standard when dealing with claims of this magnitude. Whilst representative complaints are possible under the PA (PA, 1988, s. 38), Timmel has noted that the absence of a clear statutory cause of action creates a significant hurdle for plaintiffs in privacy class actions (Timmel, 2012, p. 48). This hurdle limits the success of representative claims in Australia, and forces individuals to rely on the investigative power of the OAIC to seek legal redress. However, on account of its limited capacity, the OAIC is often unable to effectively pursue individual complaints (Daly, 2018, p. 489).

This reliance on the OAIC to investigate infractions has prompted Daly (2018, p. 492) to note that more stringent data-breach laws are necessary to facilitate the proper application of the NDB Scheme. Additionally, commentators have recently affirmed the need for individuals to have a proper avenue of redress where a notifiable data breach has occurred (Alazab *et al.*, 2021, p. 27). As such, the recommendation to include a direct right of action for individuals following a data breach is frequently proffered, most notably by the Australian Competition and Consumer Commission ('**ACCC**') in its Digital Platforms Inquiry. In its final report, the ACCC recommended granting individuals a direct right to bring actions against APP entities to seek compensation for an interference with their privacy (ACCC, 2019, p. 35). This recommendation garnered approval from the OAIC, which supported the implementation of a direct right of action for individuals (OAIC, 2019), and the Australian Government, who in principle endorsed the introduction of a direct right of action in Australian data-breach law (Australian Government, 2019, p. 18). Further, the Australian Law Reform Commission has previously advocated for the inclusion of a direct right of action (2014, p. 53), while academic discourse has criticised the Australian framework for failing to provide individuals with an avenue to sue for a breach of the APPs (Goggin *et al.*, 2019, p. 6).

However, it is arguable that allowing public access to the courts in data-breach matters will facilitate an increase in nuisance claims (Jamison, 2019, p. 35). Currently, investigative powers are centralised under the authority of the OAIC, which has jurisdiction to investigate a matter following a complaint (PA, 1988, s. 40(1)), or on its own initiative (PA, 1988, s. 40(2)). However, once a complaint has been received, the OAIC is under no obligation to undertake

http://doi.org/10.18080/jtde.v9n2.381

an investigation, and may decide not to investigate if it is satisfied that the act complained of is not an interference with the privacy of the individual (PA, 1988, s. 41(1)(a), or that the complaint is vexatious, misconceived, lacking in substance, or not made in good faith (PA, 1988, s. 41(1)(d)). Section 41 of the PA is effectively a screening mechanism that allows the OIAC to restrict its investigative resources to those claims with substantial merit, while culling those complaints that, in the Commissioner's opinion, have no reasonable chance of success. If a direct right of action were introduced, and complaints from individuals could be instigated directly, the courts would likely be forced to service an increased number of vexatious or misconceived claims, as there would be no authoritative body screening the matters beforehand. That said, the risk of frivolous suits can be overcome with sufficient safeguards (Jamison, 2019, p. 35), and as such an increased workload placed on the courts is not, by itself, a sufficient justification to exclude a direct right of action in data breach matters.

Ultimately, while the inclusion of a direct right of action for individuals may adversely impact the efficiency of the courts, this paper accepts that the effectiveness of the Australian legal framework would be bolstered should a direct right of action be introduced, as doing so would ensure that the merit of each claim would be properly assessed by a competent judicial body.

Individual compensation in the event of a data breach

The PA and NDB Scheme both fail to provide compensation to individuals whose data has been compromised in a data breach. This paper recognises that assessing the value of harm to intangible property such as personal data is difficult (Brooks, 1998, p. 384). Further, Stewart (2005, p. 21) is correct to maintain that calculating economic damages following a data breach is no simple task. Nevertheless, it is unacceptable for a legislative scheme to find a party liable for a data breach yet offer no compensatory damages to those individuals who have been affected by the conduct.

Ultimately, the implementation of a compensation mechanism into the PA would bolster its effectiveness by allowing courts to compensate individuals following a data breach. That said, this paper does not recommend the creation of an arbitrary compensation model for data breaches. Instead, as will be discussed later, this paper recommends granting courts the ability to award non-material damages in data-breach cases on broad grounds such as breach of privacy or distress. This approach has already garnered approval under the GDPR, with Tâbušca, Garais & Enâceanu (2018, p. 78) noting that damages of this type have created an effective policy framework that is capable of consistently compensating individuals following a data breach.

http://doi.org/10.18080/jtde.v9n2.381

Conclusions on the effectiveness of the Australian legal framework

The above discussion highlights that the Australian data breach regime has several flaws. First, Daly (2018, p. 489) accurately asserts that concentrating the power to initiate legal proceedings on the OAIC deprives individuals of the ability to seek legal redress on their own accord. Secondly, Dolbow (2017, p. 1935) and Abel (2017, p. 808) correctly maintain that precluding individual access to the courts denies claimants a meaningful access to justice. Finally, the NDB Scheme fails to provide victims of a data breach with a right to compensation. Ultimately, these deficiencies support the conclusion of Daly (2018, p. 492) that the current data-breach notification laws are merely a weak, retroactive response to corporate non-compliance. However, this paper echoes the views of Selvadurai, Kisswani & Khalaileh (2017, p. 13) in maintaining that these fundamental flaws have the potential to be remedied through further initiatives, the potential success of which will be evaluated below.

Insights from the European Union

The success of the GDPR will be assessed in line with the criteria for effective data-breach law. However, this paper will first outline the provisions of the GDPR that regulate the storage and use of personal data. The regulations of the EU have general application, are binding in their entirety, and are directly applicable in all member states of the EU (TFEU. 2012, art. 288). As a result, the following discussion will be confined to an analysis of the GDPR itself and will not consider any domestic legislation that has been enacted in response by member states.

The legislative framework of the GDPR

The GDPR imposes two broad obligations on data controllers (those entities that determine the purposes and means of processing data (GDPR, 2016, art. 4(7)), and third parties that process data on behalf of another entity (GDPR, 2016, art. 4(8))). First, in the case of a personal data breach, the data controller must notify the supervisory authority that a breach has occurred within 72 hours unless the breach is unlikely to result in any risk to the rights and freedoms of those affected (GDPR, 2016, art. 33(1)). Secondly, when a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the data controller must communicate the personal data breach to the data subject without undue delay (GDPR, 2016, art. 34(1)). These notification obligations are analogous to the requirements of the NDB Scheme; however, the GDPR is divergent in the way it establishes a direct right of action and a scheme of compensation for individuals who are affected by a data breach. Article 82 of the GDPR is relevant in this respect, which provides that a data controller can be held liable to pay compensation for any damage (either material or non-material) caused by an infringement of the GDPR (GDPR, 2016, art. 82(1)). The Article also provides that affected

http://doi.org/10.18080/jtde.v9n2.381

individuals are entitled to bring such claims for compensation before their national court or the courts of the member state where the data controller has an establishment (GDPR, 2016, art. 82(6)). Article 82 therefore establishes a direct right of action in the event of a data breach, as well as a model of compensation that is able to compensate individuals for both material and non-material damage.

In addition to Article 82, Recital 146 is of relevance when considering an individual's entitlement to damages. The Recital maintains that a data controller should compensate any damage suffered as a result of an act that infringes the GDPR (2016, recital 146). The Recital maintains that damage is to be interpreted broadly, and that affected individuals should receive full and effective compensation for the damage they have suffered (GDPR, 2016, recital 146). In addition, in instances where multiple data controllers are involved in the same negligent processing, they will be held jointly liable for the entire damage (GDPR, 2016, recital 146). This approach effectively regulates multi-party data breaches, bypasses the complex task of apportioning liability between various data controllers, and gives the framework a character of transparency (Chamberlain & Reichel, 2019, p. 7).

The effectiveness of the GDPR in regulating data breaches

This paper will now assess the effectiveness of the GDPR against the criteria for effective data-breach law. Specifically, the GDPR will be considered exclusively in relation to the deficiencies of the Australian legal framework. If the GDPR is effective where the Australian framework is deficient, it is reasonable to assert that it would be beneficial to incorporate those successful aspects of the GDPR into Australian law to bolster its effectiveness.

A direct right of action for individuals

The effective results of the GDPR can be seen most prominently through the implementation of a direct right of action in data breach matters. Szydło (2017, pp. 370-376) notes that, prior to the enactment of the GDPR, complaints for data-breach violations were administered independently by the national supervisory authority of each member state. These bodies possessed a wide range of powers, with Lynskey (2017, p. 255) noting their role as negotiators, law enforcers, and policy advisors among a slew of other responsibilities. In addition, Lynskey (2017, p. 261) reiterates that these bodies, as the sole investigator of data breach violations, were permitted a broad level of discretion in determining what violations to pursue and what remedies to award to affected individuals. Supervisory authorities were therefore able to use their discretionary power to reject individual and small-group complaints on the grounds of pragmatism to pursue more strategic issues (Lynskey, 2017, p. 262). This situation is analogous to Australia, where the OAIC holds dominion over the instigation of judicial proceedings for data-breach violations. This framework denies complainants an effective

http://doi.org/10.18080/jtde.v9n2.381

avenue to seek legal redress, and ultimately inhibits an individual's access to justice in the event of a data breach.

The GDPR has remedied the issue facing the Australian legal framework by granting individuals access to national courts for data-breach violations. This both remedies the complaints of Szydło (2017, pp. 370-376) and Lynskey (2017, p. 261) by effectively curtailing the discretionary power of investigative bodies, while simultaneously alleviating the workload of historically resource-starved institutions that Daly (2018, p. 489) and Coyne (2015) have noted are not capable of operating at an adequate standard when tasked with investigating large-scale data breaches. Also, without the consistent stream of individual complaints, these investigative bodies can devote more time to larger investigations and the development of better preventative practices to mitigate the occurrence of data breaches in the future.

Individual compensation in the event of a data breach

Tâbušca, Garais & Enâceanu (2018, p. 78) have noted that the GDPR, through Article 82 and Recital 146, has created an effective statutory framework that regulates the processing of personal data and damages in the event of a data breach. However, the framework is not without its faults, with O'Dell (2017, p. 111) noting that the provision of damages is not qualified by any method of calculation, and at present there has been no guidance provided as to the proper interpretation of Article 82 or Recital 146. In this sense, when courts are required to determine what damages are appropriate, the only assistance provided by the GDPR is that a person who has suffered damage is entitled to compensation (GDPR, 2016, art. 82), which should be full and effective (GDPR, 2016, recital 146). The drafting of these provisions, as Chamberlain and Reichel (2019, pp. 8-9) have concluded, has created a somewhat vague legal framework in which member states are granted significant discretion to determine what is compensable damage and effective compensation on a case-by-case basis. This framework has promoted the emergence of conflicting determinations on what non-material damage is worthy of compensation, which has led Lynskey to note that the best way to remedy violations under the GDPR remains contested (Lynskey, 2017, p. 261).

The inconsistent application of the GDPR's compensation provisions can be seen through conflicting determinations on what degree of harm is required to justify the provision of non-material damage. For example, in a matter involving the improper disclosure of personal data to an unauthorised third party, the Darmstadt Regional Court held that the violation of the protection of personal data, by itself, poses a sufficient risk to justify the provision of non-material damages (Darmstadt Regional Court, 2020, paragraph 70). While not considering data breaches per se, the Düsseldorf Labor Court made a similar decision regarding the threshold for damages under Article 82 by determining that a data controller, by failing to respond to a request for information made by a data subject, had committed an offence that

http://doi.org/10.18080/jtde.v9n2.381

entitled the data subject to non-material damage under Article 82 (Labor Court of Düsseldorf, 2020, Section I, paragraph 4(dd)). The Court in this matter noted that the severity of immaterial damage is irrelevant for the establishment of liability, and that the concept of damage is to be interpreted broadly (Labor Court of Düsseldorf, 2020, Section I, paragraph 4(dd)). These matters highlight that the threshold test for the provision of non-material damage under the GDPR is low, and that the mere occurrence of a data breach will be sufficient to entitle a data subject to compensation.

Conversely, the District Court of Frankfurt found differently in a matter involving a data breach. In this instance, the customer data of a hotel had been made available to third parties in error, which the plaintiff discovered through a media release relating to the incident (District Court of Frankfurt, 2020, paragraph 3-5). The Court in this matter found that serious impairment is required for a claim for non-material damage under Article 82, and that in the event of a data breach mere discomfort or a minor violation of a data subject's rights is not sufficient to justify a claim for damages (District Court of Frankfurt, 2020, paragraph 2). Ultimately, the court found that causal damage in the form of pain and suffering is required to create objectively understandable and detectable damage, and that individually perceived discomfort without serious impairment to an individual's self-image or reputation is insufficient to create an injury worthy of non-material damage (District Court of Frankfurt, 2020, paragraph 27-30).

This paper recognises that the above matters are somewhat distinct. That said, in light of the above it is evident that the discretion provided to courts has created a legal landscape in which conflicting threshold tests are being applied regarding what constitutes compensable damage under Article 82 of the GDPR. On one hand, the Courts of Darmstadt and Düsseldorf accept that the severity of the immaterial damage is irrelevant when considering whether compensation is available, and that the mere violation of personal data held by a data controller is sufficient to create a harm worthy of compensation. However, the stance employed by the District Court of Frankfurt is at odds with the approach of other EU courts, and severely restricts the circumstances in which a court is able to compensate individuals in the event of a data breach. As a result, O'Dell (2017, p. 113) is correct to assert that the application of the GDPR is contingent on further discretionary steps by the national courts of member states which, as Chamberlain and Reichel (2019, pp. 8-9) have noted, leaves member states grappling with the question of how far national flexibility is expected to stretch in the data protection area. The effectiveness of Article 82 and Recital 146 is therefore limited by the lack of clarity on the circumstances in which non-material damage can be provided in the event of a data breach.

http://doi.org/10.18080/jtde.v9n2.381

That said, Article 82 and Recital 146 allow courts to compensate individuals who have been impacted by a data breach. As such, it is likely that imputing a similar provision to Article 82 or Recital 146 into Australian law would bolster its ability to provide redress to individuals. However, it is not disputed that these provisions would need to be amended before being implemented into Australian law. Specifically, it would be necessary to include a threshold test of damage that must be met before non-material damage could be awarded, as this would curb judicial discretion and ensure consistency in the outcomes of data-breach matters. In doing so, the Australian landscape would be able to effectively compensate individuals in a diverse range of data-breach matters, and would satisfy the criteria for effective data-breach law.

Conclusions on the effectiveness of the GDPR

Ultimately, the GDPR, despite its shortcomings, has successfully remedied several issues that continue to plague the Australian scheme. First, in line with the findings of Szydło (2017, pp. 370-376) and Lynskey (2017, p. 261), the empowerment of individuals to instigate their own complaint has curtailed the unchecked discretion of independent investigative bodies, thereby promoting a more meaningful access to justice. Secondly, irrespective of the findings of Chamberlain and Reichel (2019, pp. 8-9), the provision of a scheme of damages has been successful in providing redress to affected individuals following a data breach. Finally, while this paper accepted the finding of O'Dell (2017, pp. 111-112) that the GDPR fails to consistently compensate plaintiffs in data-breach matters, this flaw in and of itself is not sufficient to detract from the success of the GDPR in providing non-material damage to individuals. Ultimately, the GDPR satisfies the criteria for effective data-breach law, and provides a feasible remedy to the issues faced by the Australian legal framework. As such, it would be sensible to introduce similar measures into the Australian jurisdiction, albeit with a number of modifications.

Conclusions

This paper argued that the Australian legal framework fails to provide an avenue for individuals to instigate a claim or receive compensation following a data breach. Further, this paper accepted that the NDB Scheme, while attempting to respond to the pressing need for privacy protection, has provided APP Entities with significant leeway while imposing the responsibility to deal with the consequences of a data breach on affected individuals (Alazab *et al.*, 2021, p 28). As such, it is evident that the PA and NDB Scheme are unable to satisfy the criteria for effective data-breach law, and are therefore in need of legislative amendment.

Secondly, this paper evaluated the success and limitations of the GDPR. This paper, whilst identifying issues regarding the clarity of the GDPR's compensation provisions, did not

http://doi.org/10.18080/jtde.v9n2.381

consider that the shortfalls identified by O'Dell (2017, p. 113) are sufficient to entirely diminish the effectiveness of the GDPR. Ultimately, the GDPR satisfied the criteria for effective data-breach law, and showcased its potential in being able to remedy the deficiencies suffered by the Australian jurisdiction. Consequently, this paper recommends that, in the case of future domestic reform, the Australian legislature consider the successful aspects of the GDPR and its capacity to bolster the effectiveness of Australian law. Specifically, this paper recommends that Australia take steps to implement a right to non-material damage for a breach of the NDB Scheme similar to Article 82 and Recital 146 of the GDPR. Doing so would recognise a cause of action following a data breach, facilitate a direct right of action for privacy matters, and allow courts to grant compensation on broad grounds such as breach of privacy or distress.

Acknowledgements

I would firstly like to thank Niloufer Selvadurai, without whom this paper would not have been possible. Further, I would like to thank my sister, Ellen, my brother-in-law, Sean, and my parents, Maree and Gregory, who have spent longer than they should have reading countless drafts of this work. In addition, I would like to thank my partner, Amelia, whose consistent moral support helped me make the final push to get this paper over the line. Finally, I would like to thank the many friends who gave their time to read this paper: your constructive criticism and encouragement meant more than you'll ever know.

References

Abel, L. (2012). Turner v Rogers and the Right of Meaningful Access to the Courts. *Denver University Law Review*, *89*(4), 805-823.

Aguirre, E., Mahr, D., Grewal, D., De Ruyter, K., & Wetzels, M. (2015). Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness. *Journal of Retailing*, *91*(1), 34-49. http://dx.doi.org/10.1016/j.jretai.2014.09.005

Alazab, M., Hong, S., & Ng, J. (2021). Louder bark with no bite: Privacy protection through the regulation of mandatory data breach notification in Australia. *Future Generation Computer Systems*, *116*, 22-29. https://doi.org/10.1016/j.future.2020.10.017

Australian Broadcasting Corporation v Lenah Game Meats (2001) 208 CLR 199.

Australian Competition and Consumer Commission. (2019). *Digital platforms inquiry - final report*. Canberra: Commonwealth of Australia. Available at https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf

Australian Government. (2019). *Regulating in the digital age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry*. Available at https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf

Australian Law Reform Commission. (2008). *For your information: Australian privacy law and practice* (108). Available at https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/

Australian Law Reform Commission. (2014). *Serious invasions of privacy in the digital era* (123). Available at https://www.alrc.gov.au/wp-content/uploads/2019/08/final_report_123_whole_report.pdf

Bergelson, V. (2003). It's Personal But Is It Mine? Toward Property Rights in Personal Information. *University of California Davis Law Review*, *37*(2), 379-452.

Brooks, R. (1998). Deterring the Spread of Viruses Online: Can Tort Law Tighten the Net. *Review of Litigation*, *17*(2), 343-392.

Bungard, M. (2020, September 7). Service NSW cyber attack: Data of 186,000 customers leaked. *The Sydney Morning Herald*. Available at https://www.smh.com.au/national/nsw/data-of-186-000-customers-leaked-in-service-nsw-cyber-attack-20200907-p55t7g.html

Campbell, J., Goldfarb, A., & Tucker, C. (2015). Privacy Regulation and Market Structure. *Journal Of Economics & Management Strategy*, *24*(1), 47-73. https://doi.org/10.1111/jems.12079

Carbonara, E., Guerra, A., & Parisi, F. (2016). Sharing Residual Liability: The Cheapest Cost Avoider Revisited. *The Journal Of Legal Studies*, *45*(1), 173-201. https://doi.org/10.1086/685498

Christiani, T. A. (2016). Normative and empirical research methods: Their usefulness and relevance in the study of law as an object. *Procedia - Social and Behavioural Sciences*, *219*, 201-207. https://doi.org/10.1016/j.sbspro.2016.05.006

Coyne, A. (2015, July 17). Starved of funding, resources, OAIC is left to shrivel. *IT News*. Available at https://www.itnews.com.au/blogentry/starved-of-funding-resources-oaic-is-left-to-shrivel-405273

Daly, A. (2018). The introduction of data breach notification legislation in Australia: A comparative view. *Computer Law & Security Review*, *34*(3), 477-495. https://doi.org/10.1016/j.clsr.2018.01.005

Dari-Mattiacci, G., & Garoupa, N. (2007). Least-Cost Avoidance: The Tragedy of Common Safety. *Journal Of Law, Economics, And Organization*, *25*(1), 235-261. https://doi.org/10.1093/jleo/ewm052

Darmstadt Regional Court, 13 O 244/19, 26 May 2020

Dolbow, L. (2017). Introduction: The Power of New Data and Technology. *Vanderbilt Law Review*, *70*(6), 1935-1938.

Düsseldorf Labor Court, 9 Ca 6557/18, 5 March 2020.

Frankfurt District Court, 385 C 155/19, 10 July 2020.

Geistfeld, M. (2017). Protecting Confidential Information Entrusted to Others in Business Transactions: Data Breaches, Identity Theft, and Tort Liability. *Depaul Law Review*, *66*(2), 385-412. https://via.library.depaul.edu/law-review/vol66/iss2/4

Glickman, P., Glady, N. (2015, October 14). What's the value of your data? *TechCrunch*. Available at https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/

Goggin, G., Vromen, A., Weatherall, K., Martin, F., & Sunman, L. (2019). Data and digital rights: recent Australian developments. *Internet Policy Review*, *8*(1). https://doi.org/10.14763/2019.1.1390

Jamison, S. (2019). Creating a National Data Privacy Law for the United States. *Cybaris, An Intellectual Property Law Review*, *10*(2), 1-40. https://open.mitchellhamline.edu/cybaris/vol10/iss1/2.

Kecsmar, K. (2003). Contractual Solutions to the Transfer of Personal Data from Europe to Third Countries Without Providing an Adequate Level of Protection: Inventory. *International Business Law Journal*, *3*, 269-284.

Kugler, L. (2018). The war over the value of personal data. *Communications of the Association of Computing Machinery*, *61*(2), 17-19. https://doi.org/10.1145/3171580

Lim, L. (1999). Approaches to Liability for Breaches in Data Security. *Macarthur Law Review*, *3*, 81-97. http://www.austlii.edu.au/au/journals/MacarthurLawRw/1999/8.html

Lindqvist, J. (2017). New challenges to personal data processing agreements: Is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of things?. *International Journal of Law and Information Technology*, *26*(1), 45-63. https://doi.org/10.1093/ijlit/eax024

Lynskey, O. (2017). The 'Europeanisation' of Data Protection Law. *Cambridge Yearbook of European Legal Studies*, *19*, 252-286. https://doi.org/10.1017/cel.2016.15

Massey, R. (2010). Outsourcing – New Standard Contractual Clauses for the Transfer of Personal Data Outside the EU. *Computer and Telecommunications Law Journal*, *16*(4), 88-89.

Meglio, M. (2020). Embracing Insecurity: Harm Reduction Through a No-Fault Approach to Consumer Data Breach Litigation. *Boston College Law Review*, 61(3), 1223-1269. Available at https://lawdigitalcommons.bc.edu/bclr/vol61/iss3/9

Mitrakas, A. (2011). Assessing liability arising from information security breaches in data privacy. *International Data Privacy Law*, *1*(2), 129-136. https://doi.org/10.1093/idpl/ipr001

Morey, T., Forbath, T., & Schoop, A. (2015, May). Customer data: Designing for transparency and trust. *Harvard Business Review*. Available at https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust

Naldi, M., Flamini, M., & D'Acquisto, G. (2013). Liability for data breaches: A proposal for a revenue-based sanctioning approach. *Network and System Security*, 264-277. https://doi.org/10.1007/978-3-642-38631-2_20

Nieuwesteeg, B., & Faure, M. (2018). An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law and Security Review*, *34*(6), 1232-1246. https://doi.org/10.1016/j.clsr.2018.05.026

Office of the Australian Information Commissioner. (2019, July 13). Part 4: Notifiable Data Breach (NBD) Scheme. *OAIC*. Available at https://www.oaic.gov.au/privacy

/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/

Office of the Australian Information Commissioner. (2019, September 23). Digital Platforms Inquiry final report — submission to the Australian Government. *OAIC*. Available at https://www.oaic.gov.au/engage-with-us/submissions/digital-platforms-inquiry-final-report-submission-to-the-australian-government/

O'Dell, E. (2017). Compensation for breach of the General Data Protection Regulation. *Dublin University Law Journal*, *40*(1), 97-164. https://doi.org/10.2139/ssrn.2992351

Palmer, D. (2021, March 22). Microsoft Exchange Server attacks: 'They're being hacked faster than we can count', says security company. *ZDNet*. https://www.zdnet.com/article/microsoft-exchange-server-attacks-theyre-being-hacked-faster-than-we-can-count-says-security-company/

Prins, C. (2006). When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?. *SCRIPT-ed*, *3*(4), 270-303. https://doi.org/10.2966/scrip.030406.270

Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth).

Purtova, N. (2010). Private law solutions in European data protection: Relationship to privacy, and waiver of data protection rights. *Netherlands Quarterly of Human Rights*, *28*(2), 179-198. https://doi.org/10.1177/016934411002800203

Quinn, B., & Arthur, C. (2011, April 27). PlayStation network hackers access data of 77 million users. *The Guardian*. https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data

Raz, J. (2010). Responsibility and the negligence standard. *Oxford Journal of Legal Studies*, *30*(1), 1-18. https://doi.org/10.1093/ojls/gqq002

Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) [2016] OJ L 119/1.

Reichel, J., & Chamberlain, J. (2019). The relationship between damages and administrative fines in the EU General Data Protection Regulation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3447854

Ritter, J., & Mayer, A. (2018). Regulating data as property: A new construct for moving forward. *Duke Law and Technology Review*, *16*(1), 220-277. Available at https://scholarship.law.duke.edu/dltr/vol16/iss1/7

Samuelson, P. (2000). Privacy as intellectual property?. *Stanford Law Review*, *52*(5), 1125-1173. https://doi.org/10.2307/1229511

Selvadurai, N., Kisswani, N., & Khalaileh, Y. (2017). Strengthening data privacy: The obligation of organisations to notify affected individuals of data breaches. *International Review of Law, Computers & Technology*, *33*(3), 271-284. https://doi.org/10.1080/13600869.2017.1379368

Sidgman, J., & Crompton, M. (2016). Valuing personal data to foster privacy: A thought experiment and opportunities for research. *Journal of Information Systems*, *30*(2), 169-181. https://doi.org/10.2308/isys-51429

Smith, G., & Bloch, V. (2018, October 17). Where are all the data breach class actions in Australia? *Allens Linklaters*. Available at https://www.allens.com.au/insights-news/insights/2018/10/pulse-where-are-all-the-data-breach-class-actions-in/

Smethurst v Commissioner of Police [2020] HCA 14.

Smyth, S. (2013). Does Australia really need mandatory data breach notification laws – And if so, what kind. *Journal of Law Information and Science*, *22*(2), 159-182. Available at http://www.austlii.edu.au/au/journals/JlLawInfoSci/2013/8.html

Solove, D., & Hoofnagle, C. (2006). A Model Regime of Privacy Protection. *University of Illinois Law Review*, *2*, 357-404. Available at https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2080&context=faculty_publications

Spiekermann, S., & Korunovska, J. (2017). Towards a value theory for personal data. *Journal of Information Technology*, *32*(1), 62-84. https://doi.org/10.1057/jit.2016.4

Steppe, R. (2017). Online price discrimination and personal data: A General Data Protection Regulation perspective. *Computer Law & Security Review*, *33*(6), 768-785. https://doi.org/10.1016/j.clsr.2017.05.008

Stewart, A. (2001). Damages for mental distress following breaches of confidence: Preventing or compensating tears. *European Intellectual Property Review*, *23*(6), 302-304.

Stewart, M. (2005). Calculating economic damages in intellectual property disputes: The role of market definition. *The Computer and Internet Lawyer*, *22*(8), 21-28.

Swinhoe, D. (2020, April 17). The 15 biggest data breaches of the 21st century. *CSO Online*. Available at https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Szydło, M. (2017). The independence of data protection authorities in EU law: Between the safeguarding of fundamental rights and ensuring the integrity of the internal market. *European Law Review*, *42*(3), 369-387.

Tâbušca, A., Tâbušca, S. M., Garais, G. E., & Enâceanu, A. E. (2018). Mobile apps and GDPR issues. *Journal of Information Systems and Operations Management*, *12*(1), 77-88.

The Privacy Act 1988 (Cth).

Timmel, S. (2012). Privacy liability and new world risks. *Franchising World*, *44*(12), 47-50.

Treaty on the Functioning of the European Union, opened for signature 7 February 1992, [2012] OJ C 326/47 (entered into force 1 November 1993).

Winder, D. (2019, August 20). Data breaches expose 4.1 billion records in first six months of 2019. *Forbes*. Available at https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/?sh=42806975bd54

Witzleb, N. (2009). Justifying gain-based remedies for invasions of privacy. *Oxford Journal of Legal Studies*, *29*(2), 325-363. https://doi.org/10.1093/ojls/gqp005

Revisiting the Nexus between Digital Economy and Economic Prosperity: Evidence from a Comparative Analysis

Nidhal Mgadmi
Faculty of Economic Sciences and Management of Mahdia

Wajdi Moussa
Higher Institute of Management of Tunis

Azza Béjaoui
Higher Institute of Management of Tunis

Tarek Sadraoui
Faculty of Economic Sciences and Management of Mahdia

Guachaoui Afef
Faculty of Economic Sciences and Management of Sousse

Abstract: In this paper, we try to investigate the contribution of digitalization on economic growth in both developed and developing countries over the period 1990-2020. For this end, different econometric tools are applied on a panel dataset. Overall, we show that the digital technologies seem to significantly and positively affect economic growth in both groups of countries. The digitalization impact level tends to differ across countries. Our empirical results also display that the short- and long-term relationship between information and communication technologies and economic growth is well documented. Such results can be useful for policymakers to enhance the digital economy and provide novel channels to develop adequate policies and promote new institutions. So, benefits from digitalization can lead to realize substantial economic growth.

Keywords: Digitalization, Economic growth, Impact, Generalized moments method, Economic Prosperity.

Introduction

By and large, overwhelmingly, the momentous evolution of the Internet has led to the emergence of the digital economy, which has increasingly changed the practices of production,

http://doi.org/10.18080/jtde.v9n2.384

distribution and consumption. The digital economy can be defined as a set of economic activities which employ digitized information and knowledge as crucial factors of production, new information networks as key activity space, and communication technologies to boost productivity growth (according to the World Economic Forum and the Group of Twenty). Indeed, individuals tend to frequently use mobile communication and social media to communicate, share information and even provide knowledge and services. Not only people rely on the transformational power of digital technologies, but also political authorities and entrepreneurs rush to use digital technologies for disclosing important information, providing services, and so on. Ben Youssef *et al.* (2020) report that digital technologies, including the Internet, smartphones and other applications, enable one to gather, store, treat and share information. They also reveal that such technologies play a transformational role in the worldwide economy. In this regard, the Information and Communication Technologies have enormously facilitated the creation of new entrepreneurship processes, jobs, products, market channels and marketing strategies. For instance, mobile banking helps individuals access to financial services (Myovella, Karacuka & Haucap, 2019). Digital technologies have also led to business transformations in the value chain of all sectors (Manyika & Roxburgh, 2011).

Most notably, the digital economy has increasingly contributed to boost economic growth (Brynjolfsson & Collis, 2019; Curran, 2018; Gomber *et al.* , 2018) by satisfying the demand for digital products, such as communication materials (Habibi & Zabardast, 2020), and enhancing productivity and investment in different economic sectors (Hofman, Aravena & Aliaga, 2016). In this respect, many researchers have investigated the relationship between the digital economy and economic development and have shown that the growing use of different digital technologies fosters economic growth (Bjorkroth, 2003; Roller & Waverman, 2001; Canning, 1999; Madden, 1998). For instance, Bukht & Heeks (2017) report that digitalization plays a crucial role in fostering economic prosperity. Nonetheless, there is a well-documented persistent digital divide between developed and developing countries even though digital technologies have been used around the world (Castells & Cardoso, 2006). Ward & Zheng (2016) report the nexus between the digital economy and economic growth can depend on the country's development level. Dewan & Kraemer (2000) argue that the improvement in digital infrastructure leads to more economic benefits to developed countries than to developing countries. However, Thompson & Garbacz (2011) show that the increasing development of broadband infrastructure tends to influence lower income countries more than higher income countries. The extent of such impact thus remains inconclusive even though digitalization is considered as a leading driver of economic growth.

Based on this crux, this paper attempts to examine the dynamic short- and long-term relationship between the digital economy and economic growth for different countries. More

http://doi.org/10.18080/jtde.v9n2.384

precisely, we analyze the contribution of digitalization to economic growth for developing and developed countries in the long and short term. The use of both groups of countries aims at gaining insight into whether such a nexus depends on the levels of development of the country. Herein, a panel dataset is used, consisting of 30 years from 1990 to 2020, for 28 developed and 27 developing countries. From a methodological standpoint, we perform cointegration analysis and use the generalized moments method to estimate the digital economy-economic prosperity nexus. Such econometric techniques allow us to overcome potential endogeneity issues and better explore the dynamic relationship between economic growth and infrastructure investment.

This paper is organized as follows. The following section presents a synopsis of empirical studies. The subsequent section reports methodology, data, descriptive statistics and empirical results. The final section is a conclusion.

Related Literature on the Digital Economy–Economic Development Nexus

Many researchers have investigated the relationship between digitalization and economic growth for different countries. For instance, Qiang & Rossotto (2009) analyze the impact of the digital revolution on economic growth for 120 developed and developing countries over the period 1980–2006. They clearly show that a rise of 10% in the adoption rate of digital innovation leads to an increase of 0.81% in economic growth for low- and middle-income countries. Using 42 developed and developing countries, Yousefi (2011) examines the relationship between digital economy and economic growth over the period 1993-2001. The empirical results indicate that the investment in digital technologies only improves economic growth in developed countries.

Thompson & Garbacz (2011) clearly show that the growing evolution of broadband infrastructure increasingly influences the economic growth for low-income countries compared to high-income countries. Sassi & Mohamed (2013) show a positive and significant effect of digital diffusion measured by mobile phone, fixed-line telephone, and Internet use on economic growth over the period 1960-2009 for 17 MENA countries. Niebel (2014) analyzes the effect of information and communication technologies (ICT) on economic growth for developing, emerging and developed countries. It clearly demonstrates that developing, emerging and developed countries do not show significant differences in the output elasticity of ICT between countries.

Pradhan, Arvin & Norman (2015) examine the relationship between digital innovation, financial development and economic growth for 21 Asian countries over the period 2001-2012.

http://doi.org/10.18080/jtde.v9n2.384

They report that digital innovation and financial development contribute to boost the long-run economic growth of Asian countries. Using panel data from India, Ghosh (2016) show the positive and significant effect of mobile phone penetration on economic growth and financial inclusion.

Aghaei & Rezagholizadeh (2017) explore the influence of information and communication technology on economic growth for Organization of Islamic Cooperation (OIC) countries from 1990 to 2014. They report that digitalization significantly influences economic growth for these countries. Pradhan, Mallik & Bagchi (2018) explore the extent and direction of the relationship between both broadband and Internet users and economic growth for G-20 countries over the period 2001-2012. They report a significant and positive relationship between digitalization and economic growth. Myovella, Karacuka & Haucap (2019) analyze the relationship between economic growth and digital technologies over the period 2006-2016 using a panel dataset of 41 Sub-Saharan African and 33 OECD countries. They report that digital innovations have a positive effect on economic growth in developed and developing countries. The effect of broadband Internet seems to be higher for OCDE countries than Sub-Saharan African countries, where it is minimal, and the impact of mobile telecommunications is lower for Sub-Saharan African countries than OECD countries. Bahrini & Qaffas (2019) examine the effect of information and communication technology on economic growth for the Middle East and North Africa (MENA) over the period of 2007–2016. They indicate that information and communication technology (e.g., mobile phones, Internet usage, and broadband adoption) seems to be a key driver of economic growth. In this respect, they clearly show that mobile phones have the most significant positive effect on economic growth; and Internet usage and broadband adoption are among the crucial factors that contribute to the economic growth of developing countries. Habibi & Zabardast (2020) examine the contribution of the education and digital technologies to economic growth for 10 Middle East and 24 OCDE countries. They use Internet users, broadband subscriptions and mobile phones to measure the digital economy. They show that better access to education is crucial for the Internet to create economic benefits, whereas it appears to be inadequate for mobile phone usage. Fernández-Portillo *et al.* (2019) investigate the effect of the digital economy on economic growth for the European Economic Community. They clearly show that digitalization is a key factor to boost economic growth. Solomon & van Klyton (2020) examine the effect of using digital technology on economic growth for 39 African countries from 2012 to 2016. The empirical results indicate that the difference between the effect of individual, business and government ICT usage on economic growth is well documented. As well, they indicate that only individual usage has a positive effect.

http://doi.org/10.18080/jtde.v9n2.384

Other researchers, rather, focus on explaining the impact of the digital divide on economic growth for different groups of countries. For example, Acemoglu & Zilibotti (2001) report that the potential for productivity benefits from using digital innovations relies mainly on the skills of the workforce in a developed/developing country. Indeed, developed countries possess skilled workers and thus are in a greater position to collect gains from digital technologies. Niebel (2014) indicates that the contribution of digitalization to economic growth in developing countries is different from developed countries because of the lack of absorptive capacity (e.g., an appropriate level of human capital) and additional factors (e.g., in research and development capacities). Samimi, Ledary & Samimi (2015) show that the impact of digitalization on economic growth in low-income countries can take more time, given that there is a lack of competitive environment and the importance of government control, compared to high income countries.

Empirical Validation

This section reports a battery of tests, econometric modelling and estimation methods used to investigate the contribution of the digital economy to sustainable economic development. As well, we report a panel of data employed to analyze such a relationship.

Data description and descriptive statistics

As aforementioned, we attempt to analyze the effect of the digital economy on sustainable economic development. To this end, we gather data from the World Bank and the International World Fund related to 55 (28 developed and 27 developing) countries over the period 1990-2020 on annual frequencies. Using panel data help us to have more flexibility in modelling differences and variability among two groups of countries in terms of digitalization infrastructure. That is why we attempt to use the criteria of intra-group homogeneity and inter-group heterogeneity in technology. We also prefer to exclude the United States and China, given that they are more digitized than others and adopt digital technologies in different economic fields. So, we avoid more variability in group in order to produce insightful findings. The developed countries are: Austria, Belgium, Canada, Chile, Cyprus, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Israel, Italy, Japan, Hungary, Luxembourg, New Zealand, Norway, Romania, South Korea, Panama, Poland, Portugal, Spain, Switzerland and United Arab Emirates. The developing countries are: Argentina, Bolivia, Brazil, Colombia, Ecuador, Egypt, El Salvador, Georgia, India, Indonesia, Jamaica, Jordan, Kazakhstan, Malaysia, Morocco, Mexico, Moldova, Paraguay, Philippines, Peru, Sri Lanka, Senegal, Thailand, Tunisia, Turkey, Vietnam and Zimbabwe.

The gross domestic product per capita (GDPH) is used to measure the sustainable development. In this paper, the sustainable economic development refers to the continuity

http://doi.org/10.18080/jtde.v9n2.384

without a great fluctuation in the economic growth rate: i.e., the development has been persistent during a longer time period. In this regard, Armeanu, Vintilă & Gherghina (2018) report that sustainable economic development includes three different facets: economic, social, and environmental growth. They also profess that sustainable economic development can be boosted when income is improved, with higher income being captured in gross domestic product, which consequently transmits into per capita income. So, Gross Domestic Product can be considered as a proxy for sustainable economic development. As well, the gross domestic product per capita has been largely employed as an indicator of sustainable economic development (e.g., Arias, 2006; Fernández-Portillo *et al.*, 2019; Vasylieva *et al.*, 2019).

The degree of economic openness is measured by the ratio of the sum of exports and imports to the Gross Domestic Product for each country (Ouvcom). The people's growth rate (Pop) tends to approximate the evolution of population for each country. The Gross fixed capital formation[i] (GFCF) is used as tangible investment and includes land improvements, as well as machinery and road building. The public consumption is approximated by the governments' current spending for the purchases of goods and services (Conpub). Three indicators are used to highlight the global digital economy:[ii] the mobile subscription corresponds to the cellular mobile phone subscriptions (per 100 people) (AbMobile); individuals using the Internet (% of population) (Utint); and the fixed broadband subscriptions (per 100 people) (AboLb). Finally, we use the inflation rate based on the Consumer Price Index (CPI) and the control of corruption (CONCOR).

The descriptive statistics of data used in this study are reported in Table 1. Descriptive statistics comprise the mean, median, standard deviation, minimum, maximum, skewness and kurtosis, and Jarque-Bera for normality test. The first part of Table 1 reports the statistical indicators for developed countries; the second part for developing countries.

Table 1. Descriptive Statistics of Different Variables

Part 1. *Statistical Indicators for Developed Countries*						
	Mean	St. Dev	Variance	Skewness	Kurtosis	Jarque-Bera
LGDPH	10.2223	0.8410	0.7073	-1.2117	1.8345	334.1109
LOUVCOM	4.3267	0.5038	0.2538	0.3972	1.2267	77.2499
POP	-0.4876	1.3698	1.8763	3.0392	1.3602	60.7245
LGFCF	3.1201	0.2089	0.0436	0.3837	2.7416	293.14118
LCONPUB	2.8966	0.7502	0.5629	24.5269	0.7884	168.2865
LABMOBILE	3.4292	2.1376	4.5695	-1.9231	3.8449	169.6758
LUTINT	2.6052	2.6363	6.9502	-1.7442	2.8468	733.2403
LABOLB	0.5078	3.4180	11.6825	-0.9151	-0.2116	122.7742
LCPI	4.1546	0.3413	0.1165	-0.4011	2.2006	198.4154
LCONCOR	4.4527	1.2079	1.4589	15.8104	2.2602	120.254

http://doi.org/10.18080/jtde.v9n2.384

Part 2. *Statistical Indicators for Developing Countries*						
	Mean	St. Dev	Variance	Skewness	Kurtosis	Jarque-Bera
LGDPH	8.1033	0.7315	0.5351	-0.1181	-0.5984	14.4347
LOUVCOM	4.1648	0.5174	0.2677	-0.2449	0.0665	8.5243
POP	0.2644	0.6127	0.3754	-2.4145	16.3156	9361.1402
LGFCF	3.0619	0.3152	0.099375	-2.6404	15.4071	9251.1550
LCONPUB	2.5439	0.3263	0.106447	-0.6499	2.1410	218.7820
LABMOBILE	2.0628	3.3570	11.26942	-1.2514	0.7441	237.7587
LUTINT	0.6967	3.8035	14.46646	-1.0221	0.4271	152.0946
LABOLB	-2.2664	4.1572	17.28263	-0.5573	-0.7998	65.6383
LCPI	3.4946	0.2751	0.075691	-0.5385	0.4903	48.8435
LCONCOR	3.4839	1.0467	1.095689	5.3193	113.301	451643.434

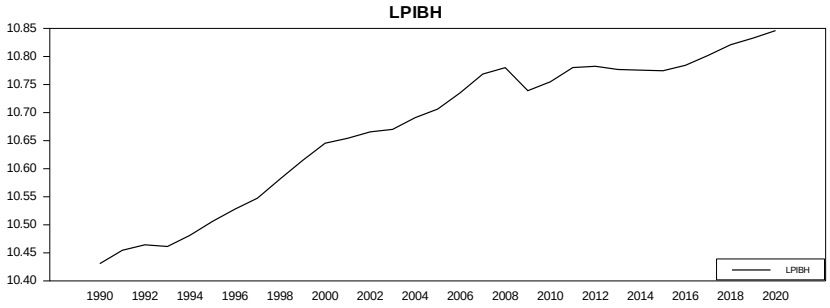
Note: L refers to the natural logarithm

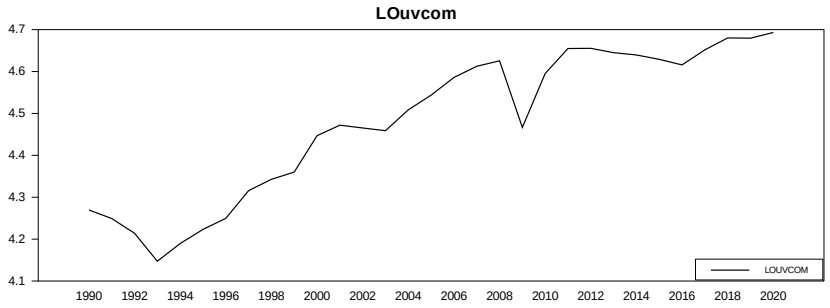
From the first part of Table 1, all the variables seem to have positive mean values, which range from 0.5078 and 10.2223, expect for the people's growth rate. The standard deviation seems to be very small for each variable. Some asymmetries between different variables in terms of skewness and kurtosis seem to be well documented. For instance, the values of skewness are less than zero for the gross domestic product per capita, the cellular mobile phone subscriptions (per 100 people), individuals using the Internet (% of population), the fixed broadband subscriptions (per 100 people), and the inflation rate. Hence, these variables are asymmetrical on the left. However, the other variables (LOUVCOM, POP, LGFCF, LCONPUB and LCONCOR) are characterized by a positive skewness. All the variables seem not to follow the normal distribution, given that the Jarque-Bera statistics are higher than the critical chi-squared value.

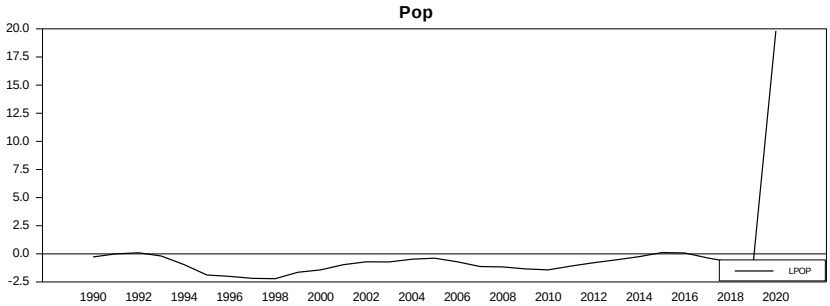
From the second part of Table 1, all the variables are characterized by positive mean values, which range from 0.6967 to 8.1033, except for the fixed broadband subscriptions (per 100 people). For the developing countries as well, there exists a very low standard deviation for each variable. The values of skewness are less than zero for all variables, except for the control of corruption. All of the variables do not follow the normal distribution: the Jarque-Bera statistics are higher than the critical chi-squared value.

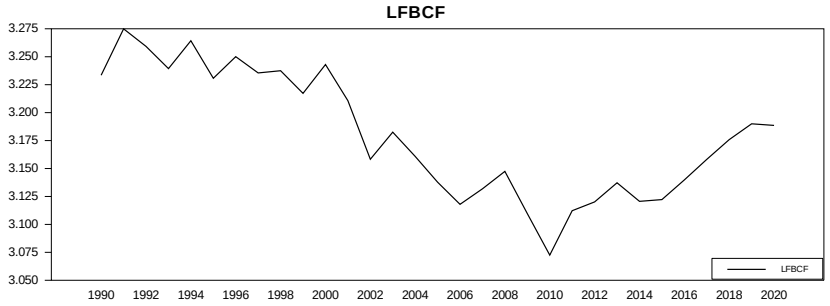
Figures 1 and 2 illustrate the evolution of different variables for both groups of countries during the period 1990-2020. As we can see in Figures 1 and 2, time series plots evolve differently, although all plots show cyclical swings. As well, the issue of the non-stationarity and volatility clustering behaviour are well documented.

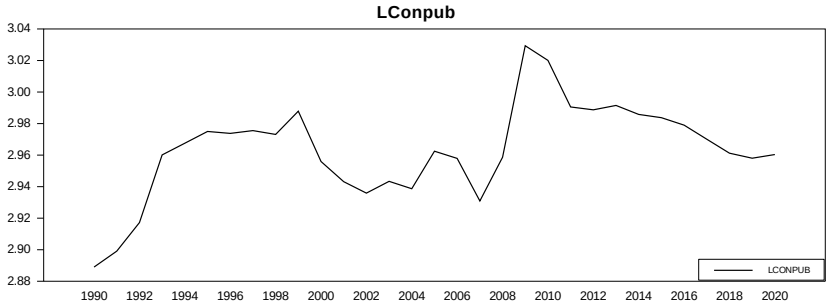
http://doi.org/10.18080/jtde.v9n2.384











http://doi.org/10.18080/jtde.v9n2.384

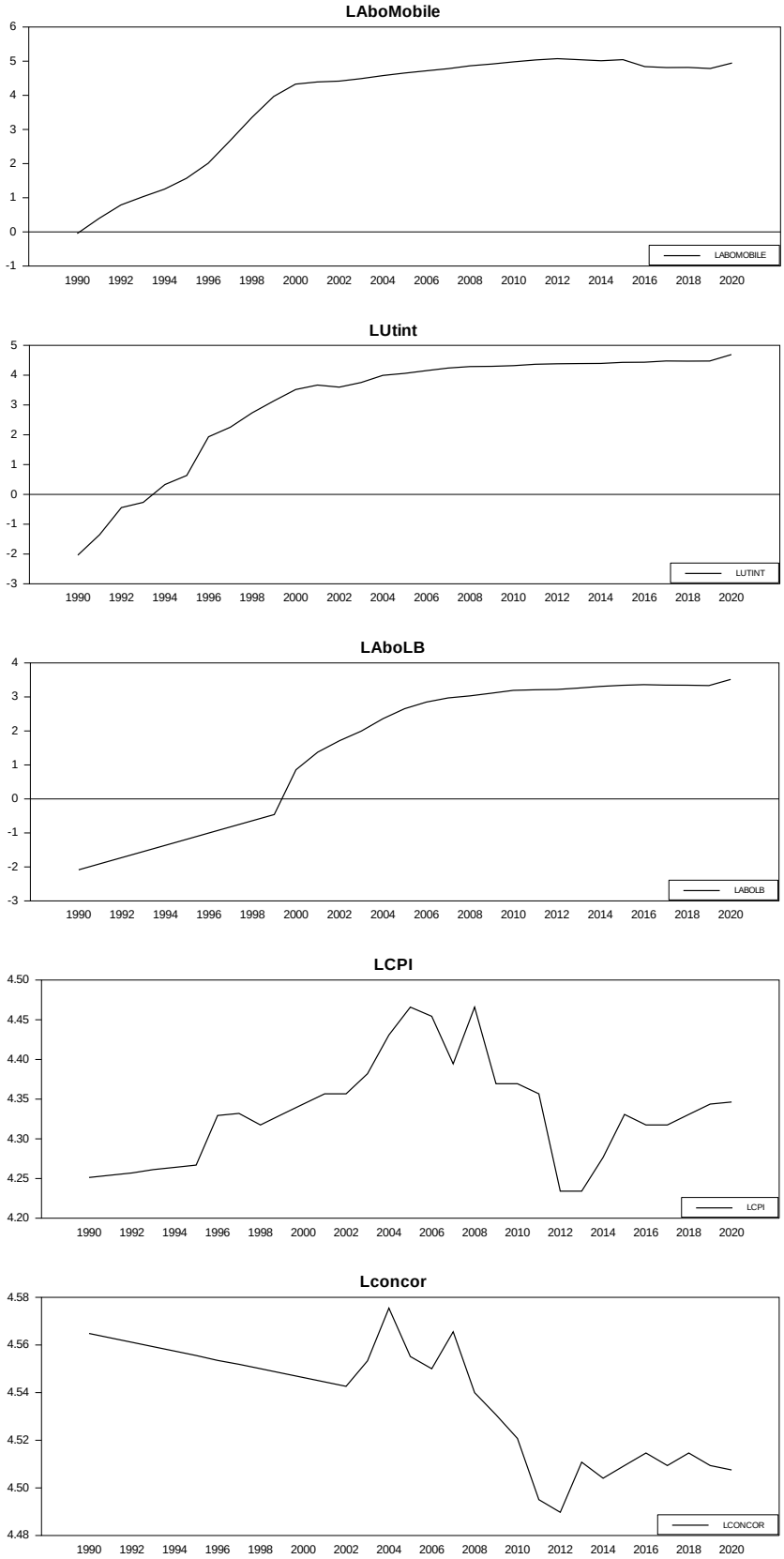
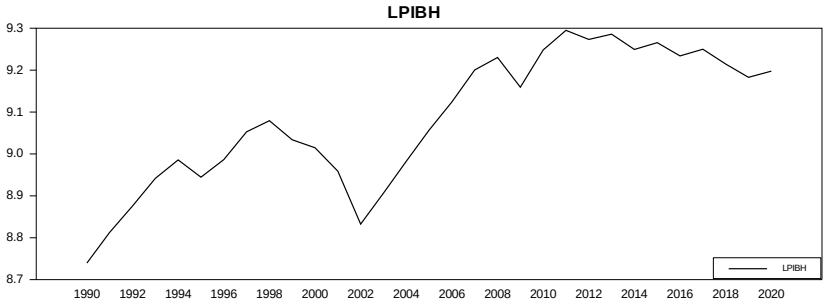
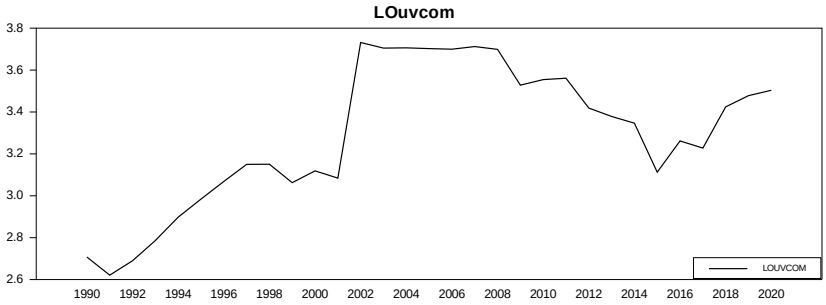
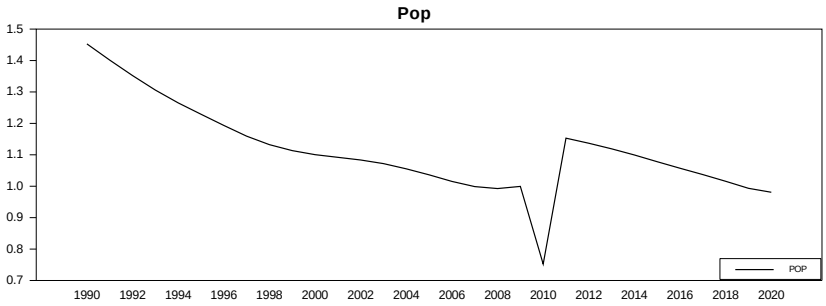


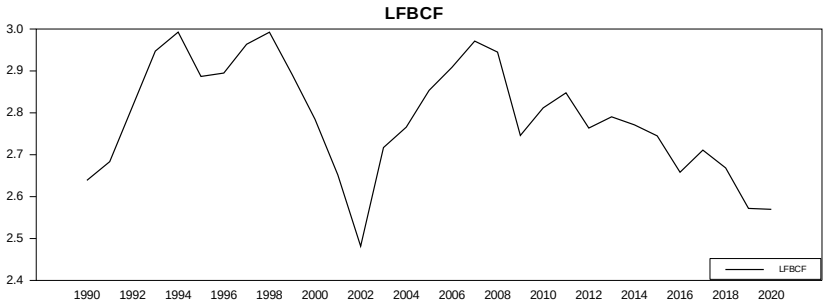
Figure 1. The Behaviour of Different Variables for Developed Countries

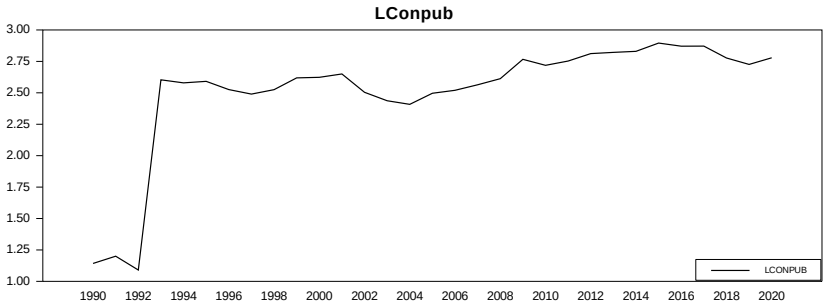
http://doi.org/10.18080/jtde.v9n2.384











http://doi.org/10.18080/jtde.v9n2.384

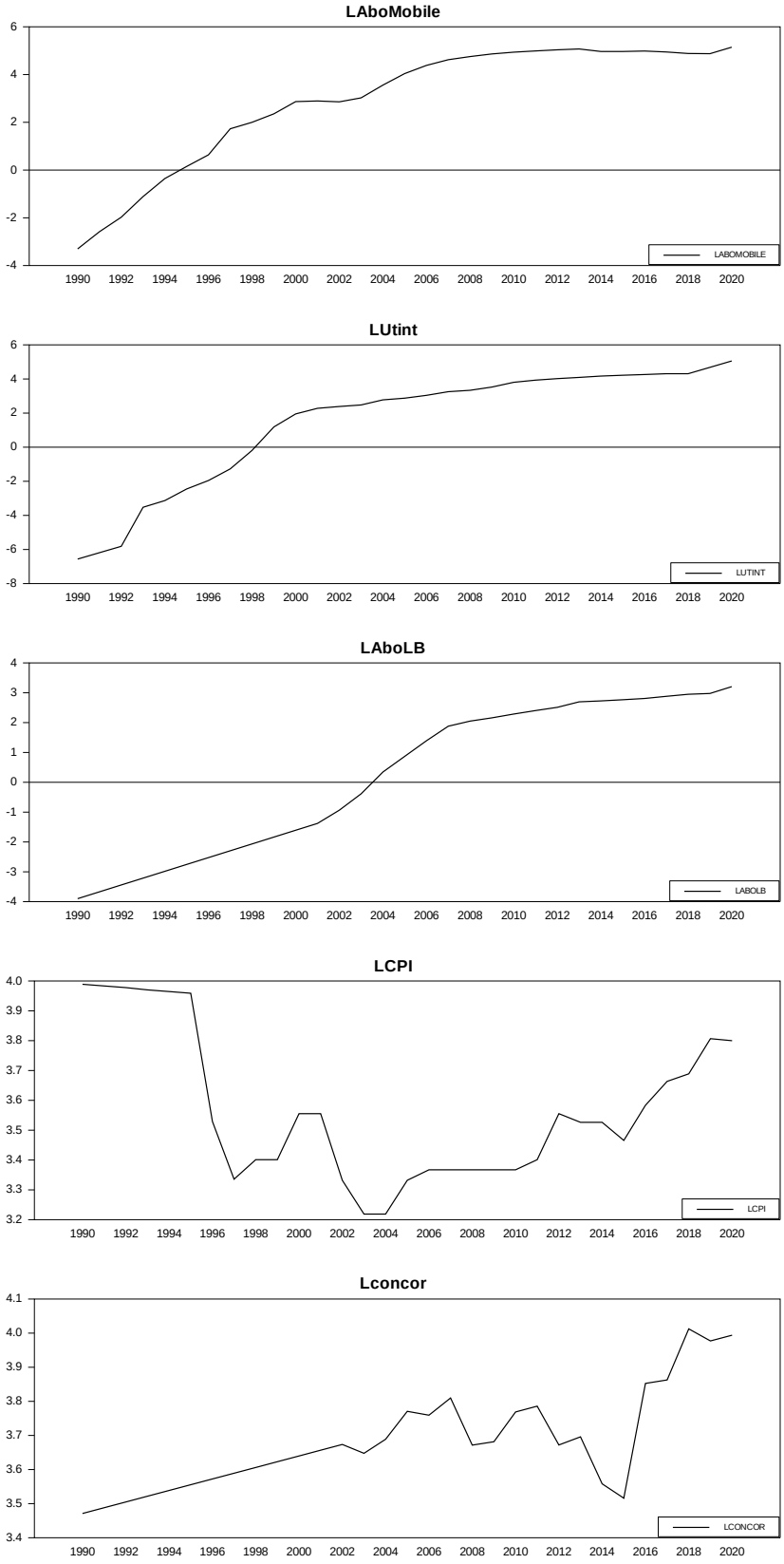


Figure 2. The Behaviour of Different Variables for Developing Countries

http://doi.org/10.18080/jtde.v9n2.384

We afterwards study the relationships between different variables for the developed and developing countries over the period 1990-2020. The variance-covariance matrices for the developing (Part 1) and developed (Part 2) countries are reported in Table 2.

Table 2. Variance-Covariance Matrix for Different Variables

Part 1. *Variance-Covariance Matrix for Developed Countries*										
	LGDPH	LOUVCOM	POP	LGFCF	LCONPUB	LABOMO	LUTINT	LABOLB	LCPI	LCONCOR
LGDPH	**0.7160**	0.1433	0.0843	-0.0466	0.0616	0.7970	1.0081	1.1694	0.2083	0.1635
LOUVCOM	0.1433	**0.2461**	0.1668	-0.0203	-0.0096	0.3218	0.4000	0.6107	0.0372	0.0006
POP	0.0843	0.1668	**1.8740**	0.0347	-0.0842	0.0008	-0.1007	-0.0161	0.0371	0.0731
LGFCF	-0.0466	-0.0203	0.0347	**0.0450**	-0.0177	-0.0046	-0.0253	-0.0568	-0.0145	-0.0158
LCONPUB	0.0616	-0.0096	-0.0842	-0.0177	**0.0656**	0.0827	0.1266	0.2031	0.0304	0.0273
LABOMO	0.7970	0.3218	0.0008	-0.0046	0.0827	**4.6252**	5.4492	6.3535	0.1990	-0.0893
LUTINT	1.0081	0.4000	-0.1007	-0.0253	0.1266	5.4492	**7.0316**	8.0078	0.2985	-0.0901
LABOLB	1.1694	0.6107	-0.016	-0.0568	0.2031	6.3535	8.0078	**11.9143**	0.3203	-0.1636
LCPI	0.2083	0.0372	0.0371	-0.0145	0.0304	0.1990	0.2985	0.3203	**0.1187**	0.0777
LCONCOR	0.1635	0.0006	0.0731	-0.0158	0.0273	-0.0893	-0.0901	-0.1636	0.0777	**1.5379**
Part 2. *Variance-Covariance Matrix for Developing Countries*										
	LGDPH	LOUVCOM	POP	LGFCF	LCONPUB	LABOMO	LUTINT	LABOLB	LCPI	LCONCOR
LGDPH	**0.5553**	-0.0523	-0.0669	0.0175	0.04409	0.9724	1.1991	1.3422	0.0545	0.1493
LOUVCOM	-0.0523	**0.2694**	-0.0361	0.0323	-0.0055	0.25104	0.2297	0.1176	0.0102	-0.0490
POP	-0.0669	-0.0361	**0.3749**	0.0153	-0.0114	-0.44512	-0.5529	-0.63053	-0.0055	0.0083
LGFCF	0.01749	0.0323	0.0153	**0.0946**	-0.0060	0.0417	-0.0498	-0.0635	0.0192	0.0888
LCONPUB	0.0441	-0.0055	-0.0114	-0.0060	**0.1058**	0.0707	0.1726	0.1656	0.0305	0.0588
LABOMO	0.9724	0.2510	-0.4451	0.0417	0.0707	**10.6307**	11.2562	11.5047	0.1304	0.3835
LUTINT	1.1991	0.2297	-0.5529	-0.0498	0.1726	11.2562	**14.3724**	13.6584	0.1702	0.341
LABOLB	1.3422	0.1176	-0.6305	-0.0634	0.1656	11.5048	13.6584	**17.0611**	0.1963	0.4187
LCPI	0.0546	0.0102	-0.0055	0.0192	0.0305	0.1304	0.1702	0.1963	**0.0727**	0.1497
LCONCOR	0.1493	-0.0490	0.0083	0.0888	0.0588	0.3835	0.3406	0.4187	0.1497	**1.0460**

The elements on the diagonal refer to the variances of variables, whereas the off-diagonal elements refer to the covariances between different variables for developed (Part 1) and developing (Part 2) countries. Overall, negative and positive relationships between different variables are well documented among developed and developing countries.

We thereafter analyze the issue of stationarity (in level and first difference) of all the variables for the developed and developing countries over the period 1990-2020. To this end, we use the homogeneous unit root test on panel data proposed by Levin, Lin & Chu (2002). Table 3 reports the results obtained from such test.

http://doi.org/10.18080/jtde.v9n2.384

Table 3. Results from Unit Root Tests for Panel Data

Results from Levin, Lin & Chu (2002) Test												
	Developed Countries						Developing Countries					
	In Level			In First Difference			In Level			In First Difference		
	Levin-Lin rho-stat	Levin-Lin t-rho-stat	Levin-Lin ADF-stat	Levin-Lin rho-stat	Levin-Lin t-rho-stat	Levin-Lin ADF-stat	Levin-Lin rho-stat	Levin-Lin t-rho-stat	Levin-Lin ADF-stat	Levin-Lin rho-stat	Levin-Lin t-rho-stat	Levin-Lin ADF-stat
LGDPH	2.2511	2.1749	2.6333	-41.965	2.9690	2.4493	3.2839	4.1455	4.2579	-36.4270	2.9923	2.2591
LOUVCOM	0.7794	1.4298	1.6563	-42.7387	2.5667	1.9626	-1.0911	0.3004	0.5002	-47.0663	-0.35124	-0.6848
POP	-3.5822	-0.2737	-0.9137	-45.5018	0.9908	1.5987	0.5008	0.3594	1.1232	-39.4665	0.3630	0.9365
LGFCF	-4.3869	-1.6664	-1.5613	-46.2473	2.1341	2.3705	-4.3614	-1.055	-0.7250	-40.8615	0.7053	0.1647
LCONPUB	-2.7733	0.2804	0.5835	-44.0065	2.3121	2.1391	-2.6405	-0.7469	-0.4735	-41.9551	0.7885	0.1262
LABOMO	-1.2126	-5.6712	-0.3977	-19.8439	3.0714	2.5144	0.2259	-3.0217	0.5697	-19.9522	-2.2687	-2.1619
LUTINT	-1.6992	-6.4585	-1.8438	-22.8651	1.1416	1.3937	0.4621	-2.0316	-0.0032	-32.0896	-8.1799	-6.2408
LABOLB	1.7013	0.4660	1.7558	-26.876	-0.2126	-0.2907	2.5222	1.8560	3.4887	-25.3695	-3.2694	-3.9821
LCPI	-1.9771	-0.1128	-0.0166	-44.6396	2.3457	1.8955	-1.0881	0.6763	0.6630	-48.782	0.3744	0.4151
LCONCOR	-1.1349	0.4549	0.5484	-52.9870	-0.8429	0.3832	-0.6677	0.3442	0.6224	-49.3861	-1.3276	-1.5572

Results from IPS Test				
	Developed Countries		Developing Countries	
	In Level	In First Difference	In Level	In First Difference
LGDPH	2.8411	-3.3117	4.2891	-3.0062
LOUVCOM	0.5405	-2.6820	-1.185	-2.7914
POP	1.1721	-2.7591	-1.4965	-2.5740
LGFCF	4.4714	-3.2482	2.8397	-2.2556
LCONPUB	2.6165	-2.4791	2.7818	-2.0380
LABOMO	-0.4376	-3.1734	1.0212	-2.8366
LUTINT	2.2600	-1.7479	-1.0144	-8.8033
LABOLB	2.0408	-2.2416	4.3471	-5.5041
LCPI	-0.1231	-2.4555	-1.1260	-2.7340
LCONCOR	1.2923	-2.4221	0.7886	-7.0527

From Table 3, we clearly show that all variables for developed and developing countries seem to be non-stationary in level using the homogeneous unit root test on panel data proposed by Levin, Lin & Chu (2002). After a first difference, such variables become stationary, given that the calculated values of the test statistics are less than the critical value of -1.64. Hence, the variables for the developed and developing countries are integrated of order one. Table 3 also reports the results from the IPS (Im, Pesaran & Shin, 2003) test for different variables in terms of level and first difference related to the developed and developing countries over the period 1990-2020.

As shown in Table 3, the exogenous and endogenous variables seem to have unitary roots in levels for both developed and developing countries given that the values of IPS statistics are greater than the critical value of -1.64. After a first difference, all variables become stationary since the values of IPS statistics are less than the critical of value of -1.64. Hence, the different

http://doi.org/10.18080/jtde.v9n2.384

variables are integrated of order one. Such findings thus confirm those of the homogeneous unit root test on panel data proposed by Levin, Lin & Chu (2002).

Statistics estimation results and interpretation

From the foregoing, we apply the cointegration analysis approach on panel data in order to analyze the long-term relationship between sustainable development and other variables over the period 1990-2020. In this regard, the error correction model (ECM) is considered as a useful framework for examining the short- and long-term linkages between different variables under study, for both developed and developing countries. Formally, the model is given as follows:

$$Log(GDPH_{it}) = c + \alpha Log(Ouvcom_{it}) + \beta POP_{it} + \chi Log(GFCF_{it}) + \delta Log(CONPUB_{it}) + \varphi Log(ABMobile_{it}) + \phi Log(UTINT_{it}) + \eta Log(ABOLB_{it}) + \lambda Log(CPI_{it}) + \mu Log(CONCOR_{it}) + \varepsilon_{it}$$

where:

- $GDPH_{it}$ is the gross domestic product per capita for the country i at year t;
- $Ouvcom_{it}$ is the degree of economic openness for the country i at year t;
- POP_{it} is the people's growth rate for the country i at year t;
- $GFCF_{it}$ is the gross fixed capital formation for the country i at year t;
- $CONPUB_{it}$ is the public consumption for the country i at year t;
- $ABMobile_{it}$ is the mobile subscription for the country i at year t;
- $UTINT_{it}$ corresponds to individuals using the Internet in percentage of population for the country i at year t;
- $ABOLB_{it}$ is the fixed broadband subscriptions (per 100 people) for the country i at year t;
- CPI_{it} is the consumer price index for the country i at year t;
- $CONCOR_{it}$ is the control of corruption for the country i at year t.

But before estimating the model, we analyze the stationarity of the residuals in the long-term relationship based on seven tests of Pedroni (1995, 1997). The results of these tests are reported in Table 4. Needless to say, Pedroni's seven tests include four tests based on within-dimension and three tests based on between-dimension. Both types[iii] of tests are based on the null hypothesis of no cointegration.[iv] Overall, the results indicate that the residuals of the long-term relationship are stationary in level, given that the seven statistics of Pedroni (1995, 1997) are lower than the critical value of -1.64.

http://doi.org/10.18080/jtde.v9n2.384

Table 4. Results of Pedroni (1995, 1997) Tests

	Rho-stat	v-stat	pp-stat	Adf-stat	Rho-stat*	pp-stat*	Adf-stat*
Residuals for developed countries	-3.1764	-2.453	-3.1334	-3.0976	-2.12543	-1.8976	-1.9988
Residuals for developing countries	-2.7853	-2.432	-3.4521	-4.4031	-1.9842	-1.9932	-2.0986

Note: * refers to tests based on 'between' dimension

Based on the aforementioned results, we estimate the long-term relationship between the natural logarithm of gross domestic product per capita and other variables (macroeconomic variables, indicators of the digital economy, and institutional variables) for both developed and developing countries over the period 1990-2020. To this end, we apply the Fully-Modified procedure on annual panel data described in Hansen (1995). The empirical results are reported in Table 5.

Table 5. Estimation Results for Long-Term Relationship based on Fully-Modified Procedure

	Developed Countries		Developing Countries	
	Coefficients	Signification	Coefficients	Signification
LOUVCOM	0.09	8.33	-0.05	-3.73
POP	-0.03	-3.22	-0.10	-1.80
LGFCF	0.26	22.14	0.16	13.64
LCONPUB	-0.01	-4.07	-0.03	-1.78
LABOMO	0.05	3.93	-0.01	-0.12
LUTINT	0.12	3.07	0.01	2.45
LABOLB	0.53	24.16	0.04	18.53
LCPI	-0.11	-3.86	0.09	5.23
LCONCOR	-0.17	-3.34	-0.03	-3.36

From Table 5, the estimation of the long-term relationship based on the Fully-Modified technique provides significant results for most explanatory variables for developed countries. The ratio of the sum of exports and imports to the Gross Domestic Product for each country (Ouvcom) has a significant and positive effect on the Gross Domestic Product per capita. However, the people's growth rate (Pop) seems to negatively and significantly affect sustainable economic development. The Gross Capital Formation (GFCF) has a positive and significant effect on sustainable development. Nevertheless, the three indicators related to the global digital economy —mobile phone subscriptions (per 100 people) (AbMobile); individuals using the Internet (% of population) (Utint); and the fixed broadband subscriptions (per 100 people) (AboLb) — tend to positively and significantly affect sustainable economic development, indicating the relevance of the digital economy in boosting economic development by creating more jobs and enhancing people's wellbeing. The negative effects of

http://doi.org/10.18080/jtde.v9n2.384

the inflation rate and the control of corruption on the Gross Domestic Product per capita seem to be well documented.

The estimation results seem to be quite different for developing countries. Indeed, the estimation of the long-term relationship based on the Fully-Modified technique gives significant results for explanatory variables, expect for the Gross Capital Formation (GFCF). Unlike the developed countries, the ratio of the sum of exports and imports to the Gross Domestic Product for each country (Ouvcom) significantly and negatively influences sustainable development. But, like the developed countries, the people's growth rate (Pop) has a negative and significant impact on sustainable development. The indicators related to the digital economy have a slight effect on economic development. Therefore, the digital economy sector has no participation in the economic development for developing countries. As well, the control of corruption and the consumer price index slightly influence economic development.

We thereafter analyze the linear fit of the long-term relationship between variables within the error correction model (ECM) based on the Fully-Modified technique. The estimation results from the ECM are presented in Table 6.

$$\Delta Log(GDPH_{it}) = \alpha + \beta_1 \Delta Log(Ouvcom_{it}) + \beta_2 \Delta POP_{it} + \beta_3 \Delta Log(GFCF_{it}) + \beta_4 \Delta Log(CONPUB_{it}) + \beta_5 \Delta Log(ABMobile_{it}) + \beta_6 \Delta Log(UTINT_{it}) + \beta_7 \Delta Log(ABOLB_{it}) + \beta_8 \Delta Log(CPI_{it}) + \beta_9 Log(CONCOR_{it}) \rho \varepsilon_{it-1} + \nu_{it}$$

Recall that the Error Correction Model encompasses the short-run equilibrium, where the variables are stationary in first difference, and the long-run equilibrium, where residuals of the long-run relationship are stationary in level based on unit root tests. The adjustment of this long-term relationship is caused by the negative and significant coefficient of residuals delayed by a single period.

Table 6. Estimation Results for ECM based on Fully-Modified Procedure

	Developed Countries		Developing Countries	
	Coefficients	**Signification**	**Coefficients**	**Signification**
Intercept	0.1525	0.0000	0.0841	0.000003
Δ LOUVCOM	0.0556	0.0001	-0.0343	0.0138
Δ POP	2.2112	0.9737	0.0025	0.1957
Δ LGFCF	0.1283	0.0000	0.1064	0.0000
Δ LCONPUB	-1.2675	0.3331	0.0245	0.0422
Δ LABOMO	9.7512	0.0236	0.0021	0.5781
Δ LUTINT	1.7961	0.5743	-0.0087	0.0000
Δ LABOLB	5.1666	0.0191	0.0077	0.0308
Δ LCPI	-0.0100	0.3164	0.0226	0.2203

http://doi.org/10.18080/jtde.v9n2.384

	Developed Countries		Developing Countries	
	Coefficients	**Signification**	**Coefficients**	**Signification**
Δ LCONCOR	-8.7676	0.1193	0.0013	0.5602
$Residuals_{it-1}$	**-0.0136**	**0.0000**	**-0.0078**	**0.0005**

From Table 6, the estimation results clearly show that most variables are significant for developed countries, except for the people's growth rate (Pop), the governments' current spending for the purchases of goods and services (Conpub), and individuals using the Internet (% of population) (Utint). Overall, the digital economy sector seems to exert a remarkable short-term influence on the gross domestic product per capita for the developed countries. As well, this sector appears to affect economic development in developing countries. As expected, the results clearly display that the ECM offers significant short-term coefficients with a negative and significant adjustment speed.

In the literature on the estimation of dynamic models using panel data, it is worth noting that a series of techniques, such as the methods proposed by Anderson & Hsiao (1982) and Arellano & Bond (1991), can be increasingly used. Although the Anderson & Hsiao (1982) method provides convergent estimators, it suffers from some shortcomings (e.g., it does not take into account the error structure). This is why it is interesting to use the Arellano & Bond (1991) method, which calls for instrumental variables to more explore the dynamic long-term relationship between variables. We also add the lagged gross domestic product per capita in the following model:

$$Log(GDPH_{it}) = \rho Log(GDPH_{it-1}) + \alpha Log(Ouvcom_{it}) + \beta POP_{it} + \chi Log(GBCF_{it}) + \delta Log(CONPUB_{it}) + \phi Log(ABMobile_{it}) + \varphi Log(UTINT_{it}) + \eta Log(ABOLB_{it}) + \lambda Log(CPI_{it}) + \mu Log(CONCOR_{it}) + \alpha_i + e_t + \varepsilon_{it}$$

where:

- $GDPH_{it}$ is the gross domestic product per capita for the country i at year t;
- $Ouvcom_{it}$ is the degree of economic openness for the country i at year t;
- POP_{it} is the people's growth rate for the country i at year t;
- $GFCF_{it}$ is the gross fixed capital formation for the country i at year t;
- $CONPUB_{it}$ is the public consumption for the country i at year t;
- $ABMobile_{it}$ is the mobile subscription for the country i at year t;
- $UTINT_{it}$ corresponds to individuals using the Internet in percentage of population for the country i at year t;
- $ABMobile_{it}$ is the mobile subscription for the country i at year t;
- CPI_{it} is the consumer price index for the country i at year t;
- $CONCOR_{it}$ is the control of corruption for the country i at year t.

http://doi.org/10.18080/jtde.v9n2.384

In the aforementioned model, α_i and e_t represent the specific and temporal effects. Using a lagged dependent variable does not allow us to employ standard econometric techniques. Indeed, the model estimation based on classical methods (OLS and Within) leads to biased and non-convergent estimators. That is why one might apply the generalized moments method on dynamic panel data, which can control the specific individual and temporal effects and overcome the endogeneity bias of explanatory variables. Overall, the model is presented as follows:

$$\begin{aligned}\Delta Log(GDPH_{it}) = {} & \theta \Delta Log(GDPH_{it-1}) + \beta_1 \Delta Log(Ouvcom_{it}) + \beta_2 \Delta POP_{it} + \beta_3 \Delta Log(GBCF_{it}) \\ & + \beta_4 \Delta Log(CONPUB_{it}) + \beta_5 \Delta Log(ABMobile_{it}) + \beta_6 \Delta Log(UTINT_{it}) \\ & + \beta_7 \Delta Log(ABOLB_{it}) + \beta_8 \Delta Log(CPI_{it}) + \beta_9 \Delta Log(CONCOR_{it}) + \Delta e_t + \Delta \varepsilon_{it}\end{aligned}$$

where:

- $GDPH_{it}$ is the gross domestic product per capita for the country i at year t;
- $Ouvcom_{it}$ is the degree of economic openness for the country i at year t;
- POP_{it} is the people's growth rate for the country i at year t;
- $GFCF_{it}$ is the gross fixed capital formation for the country i at year t;
- $CONPUB_{it}$ is the public consumption for the country i at year t;
- $ABMobile_{it}$ is the mobile subscription for the country i at year t;
- $UTINT_{it}$ corresponds to individuals using the Internet in percentage of population for the country i at year t;
- $ABOLB_{it}$ is the fixed broadband subscriptions (per 100 people) for the country i at year t;
- CPI_{it} is the consumer price index for the country i at year t;
- $CONCOR_{it}$ is the control of corruption for the country i at year t.

The estimation results for developed and developing countries over the period 1990-2020 based the two-step procedure of Arrelano & Bond (1991) are presented Table 7.

Table 7. Estimation Results based on the Method of Arrelano & Bond (1991)

	Developed Countries		Developing Countries	
	First Step Coefficients	Second Step Coefficients	First Step Coefficients	Second Step Coefficients
Intercept	-8.6392	2.9706**	-0.4397	-0.0097
$LPIBH_{it-1}$	0.0247	1.0869*	-0.9730*	-0.9966*
$LOUVCOM_{it}$	4.0499	-0.0902***	-0.0367	0.0023
POP_{it}	-0.00000038	0.000000102	-0.0529**	-0.0151*
$LGFCF_{it}$	-4.3967	-0.3339**	0.1055**	0.0224***
$LCONPUB_{it}$	5.1684	-0.0122	-0.1462	-0.0193**
$LABOMO_{it}$	-0.0835	-0.1254	0.0139	0.0020
$LUTINT_{it}$	0.0958	0.1100	-0.0136	0.0111

http://doi.org/10.18080/jtde.v9n2.384

	Developed Countries		Developing Countries	
	First Step	Second Step	First Step	Second Step
	Coefficients	Coefficients	Coefficients	Coefficients
$LABOLB_{it}$	-0.1869	-0.0032	-0.0044	-0.0091
$LCPI_{it}$	0.0333	0.2051	0.0109	0.0210
$LCONCOR_{it}$	0.1256	-0.7011***	0.2483**	-0.0163
Over-identification Test				
Sargon	1.7138×10^{-9}	53204.0271	15.8103	339.1426
Signification of Sargon	1.0000	0.0000	0.9203	0.0000
Test of Absence of Residual Autocorrelation				
m2	0.8889	0.1519	0.6854	0.1789
LB = Q	1398.040 (0.0000)	7.175 (1.0000)	659.918 (0.0000)	2.907 (1.0000)

Notes: -*, ** and *** denote significant level at 1%, 5% and 10%, respectively;
- LB refers to LJUNG-BOX error autocorrelation statistic in level.
- The values in parentheses correspond to the probability of rejecting the null hypothesis.

From Table 7, estimating the dynamic long-term relationship between economic development and other variables provides insightful results for both developed and developing countries using the two-step procedure of Arrelano & Bond (1991). Most notably, the lagged value of the endogenous variable has a positive (respectively, negative) and significant effect on the economic development of developed (respectively, developing) countries under the second step of the procedure of Arrelano & Bond (1991). The other explanatory variables seem not to have a significant effect on economic development under the single step of the same procedure for different countries. In particular, the three indicators related to the digital economy sector have no effect on economic development for different countries. The instrumental variables seem not to be effective, given that the Sargon statistic is not significant and such variables are under-identified. Also, there is a two-order autocorrelation problem, given the LJUNG-BOX statistic.

Conclusion

Interestingly enough, the question of how digitalization exerts an important influence on economic growth in both developed and developing countries is still open. Cognizant of this fact, we attempt to examine the effect of digitalization on sustainable economic growth for the most and the least developed countries in the long and short term. The main reason for using two different groups of countries is to get some insights on if the effect of digitalization relies on the level of the economy's development. We perform a quantitative, empirical analysis on a panel of 28 developed and 27 developing countries from 1990 to 2020. At the empirical level, we apply cointegration analysis and the generalized moments method on panel data. The empirical results clearly show that the digital technologies seem to be significantly and positively associated with economic growth in both groups of countries. The digitalization

http://doi.org/10.18080/jtde.v9n2.384

impact level differs across countries. The effects of Internet users, cellular mobile phone subscriptions and fixed broadband subscriptions tend to be lower for the developing countries than developed countries. The short- and long-term dynamics of such relationships are well documented.

Our findings seem to confirm those of other researchers (e.g., Myovella, Karacuka & Haucap, 2019; Pradhan, Mallik & Bagchi, 2018), which show that digitalization positively contributes to economic growth, dependent on a country's development level. At the practical level, policymakers in developing countries should pay particular attention by developing a specific policy approach for the co-development of digital-technology infrastructure and economic prosperity in such countries. Developing countries should also undertake adequate actions to receive gains from the positive role of digitalization in boosting sustainable economic growth by enhancing human capital and adopting sound government policies in all sectors of the economy.

References

Acemoglu, D., & Zilibotti, F. (2001). Productivity differences. *Quarterly Journal of Economics*, *116*, 563–606.

Aghaei, M., & Rezagholizadeh, M. (2017). The impact of information and communication technology (ICT) on economic growth in the OIC Countries, *Economic and Environmental Studies*, *17*(2) [42], 257–278. https://doi.org/10.25167/ees.2017.42.7

Anderson, T. W., & Hsiao, C. (1982). Formulation and estimation of dynamic models using panel data. *Journal of Econometrics*, *18*, 47-82.

Arellano, M., & Bond, S. (1991). Some tests of specification for panel data: Monte Carlo evidence and an application to employment equations. *Review of Economic Studies, 58*, 277–297.

Arias, F. (2006). Desarrollo sostenible y sus indicadores [Sustainable development and its indicators]. *Revista sociedad y economía*, *11*, 200–229.

Armeanu, D.S., Vintilă, G. & Gherghina, S. C. (2018). Empirical study towards the drivers of sustainable economic growth in EU-28 countries. *Sustainability*, 10, 1-23.

Bahrini, R., & Qaffas, A. A. (2019). Impact of Information and Communication Technology on Economic Growth: Evidence from Developing Countries, *Economies*, 7, 1–13. https://doi.org/10.3390/economies7010021

Ben Youssef, A., Boubaker, S., Dedajc, B., & Carabregu-Vokshic, M. (2020). Digitalization of the economy and entrepreneurship intention. *Technological Forecasting and Social Change*, *164*(5), 1-14. https://doi.org/10.1016/j.techfore.2020.120043

Bjorkroth, T. (2003). Engine or wheels of our prosperity? Infrastructure and economic growth and effects of liberalisation of the Finnish telecommunications market, (PhD thesis) Abo Akademi Department of Economics and Statistics.

Brynjolfsson, E., & Collis, A. (2019). How should we measure the digital economy? *Harvard Business Review*, *97*, 140-146.

Bukht, R., & Heeks, R. (2017). Defining, Conceptualizing and Measuring the Digital Economy.http://www.informatics.manchester.ac.uk/news/latest-stories-updates/defining-conceptualising-and-measuring-the-digital-economy/

Canning, D. (1999). Telecommunications and aggregate output. *CAER II discussion papers 56*. Harvard Institute for International Development.

Castells, M., & Cardoso, G. (2006). The network society. Washington, D.C: Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies, Johns Hopkins University.

Curran, D. (2018). Risk, innovation, and democracy in the digital economy. *European Journal of Sociology Theory*, *21*(2), 207-226. https://doi.org/10.1177/1368431017710907

Dewan, S., & Kraemer, K. (2000). Information technology and productivity: Evidence from country-level data. *Management Science*, *46*, 548–562.

Fernández-Portillo, A., Almodóvar-González, M., Coca-Pérez, J. L., & Jiménez-Naranjo, H. V. (2019). Is sustainable economic development possible thanks to the deployment of ICT? *Sustainability*, *11*(22), 6307. https://doi.org/10.3390/su11226307

Ghosh, S. (2016). Does mobile telephony spur growth? Evidence from Indian states, *Telecommunication Policy*, *40*, 1020–1031.

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption and transformation in financial services. *Journal of Management Information Systems*, *35*(1), 220-265. https://doi.org/10.1080/07421222.2018.1440766

Habibi, F., & Zabardast, M. A. (2020). Digitalization, education and economic growth: A comparative analysis of Middle East and OECD countries, *Technology in Society*, *63*, 1-9. https://doi.org/10.1016/j.techsoc.2020.101370

Hansen, B. (1995). Rethinking the univariate approach to unit root testing: Using covariates to increase power. *Econometric Theory*, *11*, 1148-1171.

Hofman, A., Aravena, C., & Aliaga, V. (2016). Information and communication technologies and their impact in the economic growth of Latin America, 1990–2013.*Telecommunications Policy*, *40*(5), 485–501.

Im, K. S., Pesaran, M. H., & Shin, Y. (2003). Testing for unit roots in heterogeneous panels. *Journal of Econometrics*, *115*, 53-74.

Levin, A., Lin, C. F., & Chu., C. S .J. (2002). Unit Root Test in Panel Data: Asymptotic and Finite Sample Properties. *Journal of Econometrics*, *108*, 1-24.

Madden, G. (1998). CEE telecommunications investment and economic growth. *Information Economics and Policy*, *10*, 173-195. Available at https://mpra.ub.uni-muenchen.de/11843/1/MPRA_paper_11843.pdf

Manyika, J., & Roxburgh, C. (2011). The great Transformer: The impact of internet on Economic growth and Prosperity. *Mckisey Global institute.*

Myovella, G., Karacuka, M., & Haucap, J. (2019). Digitalization and economic growth: a comparative analysis of Sub-Saharan Africa and OECD economies. *Telecommunication Policy*, *44*(2), 101-110. https://doi.org/10.1016/j.telpol.2019.101856

Niebel, T. (2014). ICT and economic growth comparing developing, emerging and developed countries, *SSRN Electronic Journal*, *104*, 1-10.

Pedroni, P. (1995). Panel cointegration, asymptotic and finite sample properties of pooled time series tests with an application to the PPP hypothesis, *Working Paper in Economics*, 92-013, Indiana University.

Pedroni, P. (1997). Panel cointegration, asymptotic and finite sample properties of pooled time series tests with an application to the PPP hypothesis: New results, *Working Paper in Economics*, Indiana University.

Pradhan, R. P., Arvin, M. B., & Norman, N. R. (2015). Dynamics of information and communications technologies infrastructure, economic growth, and financial development: Evidence from Asian countries, *Technology in Society*, *42*, 135–149. https://doi.org/10.1016/j.techsoc.2015.04.002

Pradhan, R. P., Mallik, G., & Bagchi, T. P. (2018). Information communication technology (ICT) infrastructure and economic growth: A causality evinced by cross-country panel data, *IIMB Management Review*, *30*(1), 91–103. https://doi.org/10.1016/j.iimb.2018.01.001

Qiang, C. Z.-W., & Rossotto, C. M. (2009). Economic impacts of broadband. In *Information and Communications for Development, Extending Reach and Increasing Impact*, World Bank, Washington D.C, pp. 35–50. Available at https://documents1.worldbank.org/curated/en/645821468337815208/pdf/487910PUB0EPI1101Official0Use0Only1.pdf

Roller, L., & Waverman, L. (2001). Telecommunications infrastructure and economic development: A simultaneous approach. *American Economic Review*, *91*, 909–923.

Samimi, J. A., Ledary, R. B., & Samimi, J. F. (2015). ICT & economic growth: A comparison between developed & developing countries. *International Journal of Liability and Scientific Enquiry*, *1*, 26–32.

Sassi, S., & Mohamed, G. (2013). Financial development, ICT diffusion and economic growth: lessons from MENA region, *Telecommunications Policy*, *37*, 252–261.

Solomon, E.M., & van Klyton, A. (2020). The impact of digital technology usage on economic growth in Africa, *Utilities Policy*, *67*, 1-19. https://doi.org/10.1016/j.jup.2020.101104

Thompson, H., & Garbacz, C. (2011). Economic impacts of mobile versus fixed broadband. *Telecommunications Policy*, *35*, 999–1009.

Vasylieva, T., Lyulyov, O., Bilan, Y. & Streimikiene, D. (2019). Sustainable Economic Development and Greenhouse Gas Emissions: The Dynamic Impact of Renewable Energy Consumption, GDP, and Corruption. *Energies*, *12*, 3289.

Ward, M. R., & Zheng, S. (2016). Mobile telecommunications service and economic growth: Evidence from China. *Telecommunications Policy, 40,* 89–101.

Yousefi, A. (2011). The impact of Information and Communication Technology on Economic Growth: Evidence from Developed and Developing Countries. *Economics of Innovation and New Technology*, *20*(6), 581-596. https://doi.org/ 10.1080 /10438599.2010.544470

Endnotes

[i] We initially opted for capital services as a proxy for tangible investments. However, using this variable leads to a serious multicollinearity issue and the linear goodness of fit of the model appeared to be poor. That is why we replace this variable by Gross fixed capital formation (GFCF) to quantify tangible investments. As a matter of fact, Myovella, Karacuka & Haucap (2019), among others, use Gross fixed capital formation as a proxy of tangible investments.

[ii] The choice of variables is substantially related to the availability of the data, especially for the developing countries. It was challenging to provide detailed data for some of the indicators related to digitalization infrastructure for developing countries. Needless to say, it is interesting to consider a balanced panel in order to estimate the econometric model. Nonetheless, further studies can include variables related to digitalization infrastructure by choosing other sets of countries. As well, using a dummy variable to analyze the evolution of ICT usage is very interesting. But, in our case, the purpose is to analyze the degree of digitalization using a comparative approach.

[iii] For tests based on Between dimension, the alternative hypothesis is $\rho_i = \rho < 1 \ \forall$ i, while for tests based on Within dimension, the alternative hypothesis is $\rho_i < 1 \ \forall$ i.

[iv] The estimated results under the alternative hypothesis, $\hat{\varepsilon}_{it} = \rho_i \hat{\varepsilon}_{it-1} + \eta_{it}$, indicate that the autoregressive coefficients are stable over time.

Policy-based Interaction Model for Detection and Prediction of Cloud Security Breaches

Sara Farahmandian
Faculty of Engineering and IT, University of Technology Sydney, Broadway, Ultimo, Sydney, Australia

Doan B. Hoang
Faculty of Engineering and IT, University of Technology Sydney, Broadway, Ultimo, Sydney, Australia

Abstract: The ever-increasing number and gravity of cyberattacks against the cloud's assets, together with the introduction of new technologies, have brought about many severe cloud security issues. The main challenge is finding effective mechanisms for constructing dynamic isolation boundaries for securing cloud assets at different cloud infrastructure levels. Our security architecture tackles these issues by introducing a policy-driven interaction model. The model is governed by cloud system security policies and constrained by cloud interacting entities' locations and levels. Security policies are used to construct security boundaries between cloud objects at their interaction level. The novel interaction model relies on its unique parameters to develop an agile detection and prediction mechanism of security threats against cloud resources. The proposed policy-based interaction model and its interaction security algorithms are developed to protect cloud resources. The model deals with external and internal interactions among entities representing diverse participating elements of different complexity levels in a cloud environment. We build a security controller and simulate various scenarios for testing the proposed interaction model and security algorithms.

Keywords: Cloud infrastructure, security policies, security isolation, interaction, security boundaries.

Introduction

Security issues in a virtual cloud environment are more complex and challenging than in traditional infrastructures since resources are both virtualised and shared among numerous users. As a result, virtual boundaries among components or participants are not well defined and often undefined, and hence they not visible or controllable by the providers. In a multi-tenant cloud architecture, isolations are a crucial concept for both security and infrastructure management. They should be considered at functional entity levels and appropriate abstraction levels of the infrastructure. Physical isolation is

http://doi.org/10.18080/jtde.v9n2.364

relatively simple in traditional environments, as the boundaries between physical elements are well-defined and visible. The situation is not clear-cut in virtual environments unless one can keep track of all perimeters of all virtual objects created. Defining object boundaries is extremely difficult because virtual objects are dynamic in both characteristics and functionality. The task is resource-expensive due to the sheer number of virtual objects and the complexity of their dynamics. Building security boundaries is critical not only for recognising security violations but also in creating security solutions.

Practically, a security breach is defined in terms of the policies that define the interactions related to the breach. An event is considered a security breach either when it violates a defined security policy or violates the Confidentiality, Integrity, and Availability of security principles that could have been avoided if a relevant security policy had been in place. According to Kosiur (2001), a policy (or policy rule) is a simple declarative statement associating a policy object with a value and a policy rule. In general, a policy is not easy to work with as, at one extreme, a policy applies to the overall behaviour of a complex organisation (or entity) and, at the other extreme, it applies to a particular action on an element of the organisation, or a specific firewall rule on a network connection. To work with policy, one needs to clearly define the appropriate context in both scope and level; otherwise, it is not very useful or realisable.

In this paper, the policy context is on the interaction between entities with a defined set of interaction parameters. Security breaches primarily result from violations of the rule of interaction (or policy that governs the interaction) between objects when they interact. Unless one has a formal interaction model between objects, it is difficult to detect, predict, or prevent security incidents. The policy-based interaction model defines a security breach as when a security policy is violated over an interaction parameter. It has been recognised that security policies play a crucial role in all secured systems because they define what constitutes a security breach. In other words, security policies define the rules for secure interaction between objects of an environment. Security policies define the desired behaviour of the heterogenous application, systems, networks, and any type of object within the system.

Policies are complex in terms of definition and implementation in a distributed cloud infrastructure where resources are shared and dynamically changed. Different policies are often constructed for different architectural levels of a system, together with enforcement mechanisms. The ever-increasing number of virtual functions and the dynamic nature of cloud resources introduce more complexity in defining and enforcing security policies. Enforcing security policies at the interaction level enables system agility in detecting security breaches in cloud infrastructure. The policy-based interaction model is appropriate to impose and enforce dynamic, secure interactions among entities.

In this paper, we construct security boundaries dynamically at the interaction level between entities using the security policies or rules over a proposed interaction model parameter and the constraints

http://doi.org/10.18080/jtde.v9n2.364

imposed on the interacting entities. The construction of security boundaries in a cloud system is related to the characteristics of the interacting entities in the environment and the policies and constraints that govern their interaction. Our design focuses on building a robust, dynamic, and automated security boundary to protect cloud assets relying on a solid and innovative interaction model and security policy expressions that govern the interactions. A security boundary is thus a function or an expression that defines valid interactions among cloud entities.

The paper focuses on constructing security boundaries according to the interaction model and its parameters, object constraints, and dynamic security rules related to interaction parameters. We introduce a policy-driven interaction model that governs the relationship among entities in the cloud environment and develops algorithms to detect and predict security breaches. The interaction model is defined by parameters that control activities among components or entities in a cloud system. The model provides a framework for incorporating system security policies and entity constraints in constructing interaction boundaries and defining a security dictionary of expected/unexpected behaviour of cloud entities while accessing resources in the cloud environment. The main contributions of this research are:

- We propose a novel policy-driven interaction model that governs the interactions among entities in a cloud environment. According to our best knowledge, this is the first approach to use interaction parameters for building dynamic and automated security boundaries.
- We deploy an automatic detection and prediction algorithm called interaction security violation detection and prediction (ISVDP) to identify security breaches related to interaction parameters. The algorithm also maps out possible future attacks based on expected violations of the currently defined interaction parameters.
- We evaluate the proposed model and algorithms by implementing and simulating various interaction scenarios among cloud entities.

The paper is organised as follows. We first describe related work. We then briefly introduce the cloud object model and components used for the interaction model. After that, we describe the proposed general interaction model and its parameters. Building on the general interaction model, we then describe the security policy-based interaction model. We can then introduce our ISVDP algorithms, which we evaluate by simulating various interaction scenarios. Finally, we provide a conclusion.

Related Work

This section describes related work on cloud security isolation methods and security policy enforcement methods.

http://doi.org/10.18080/jtde.v9n2.364

Cloud resource isolation mechanisms

Mavridis & Karatza (2019) proposed a multi-tenant isolation solution using VMs as the boundary of security whereby applications run within containers on top of these virtual machines. To improve the security of running applications as containers in the cloud, running one container per VM was suggested. However, the drawback of such a system is its performance.

SilverLine (Mundada, Ramachandran, & Feamster, 2011) was proposed for enhancing data and network isolation for cloud tenant services. The model concentrated on providing isolation via OS-level and virtual instances. The method only focused on providing data and network isolation at the tenant level.

A mechanism known as Secure Logical Isolation for Multi-tenancy (SLIM) was introduced by Factor *et al.* (2013) as an end-to-end approach to providing isolation among tenant resources. The model only considered tenant-level isolation. Pfeiffer *et al.* (2019) proposed a method for solid tenant separation in cloud platforms by isolating components at the network level. It focused mainly on tenant separation via physical and cryptographic separation for large infrastructures.

Hoang & Farahmandian (2017) provided a classification of isolation techniques within a cloud infrastructure and proposed isolation solutions using existing technologies. Del Piccolo *et al.* (2016) conducted a research survey on network isolation solutions for multi-tenant data centres for isolating cloud services. It emphasised the main challenges related to isolation in a multi-tenant environment.

Chen *et al.* (2016) proposed a Highly Scalable Isolation Architecture for Virtualized Layer-2 Data Centre Networks. It used Software-Defined Networking (SDN) technology to provide isolation for a layer-2 data centre at the network level. The model only provided isolation at the network level. BlueShield was another method to provide isolation and security in a multi-tenant cloud infrastructure focusing only on network security (Barjatiya & Saripalli, 2012).

Security policy enforcement mechanisms

Karmakar *et al.* (2016) proposed a policy-based security architecture to secure SDN domains. The paper defined different modules within a proposed application to determine security policies related to packets. Wang *et al.* (2015) introduced a policy space analysis and focused on addressing network security policy enforcement issues on middle boxes.

Varadharajan *et al.* (2018) proposed a policy-based security architecture to secure inter- and intra-domain communication using software-defined networks between different hosts across multiple domains. Basile *et al.* (2019) introduced an approach for automatic enforcement of security policies in network function virtualisation according to dynamic network changes. It deployed virtual security functions for security policy reinforcement and introduced a security awareness manager in the orchestrator.

http://doi.org/10.18080/jtde.v9n2.364

A cyberspace-oriented access control model (CoAC) was proposed to provide access to sensitive data (Li *et al.*, 2018). The method considered operations as a combination of many atomic processes and defined a CoAC policy that permits access only if a particular operation's security risk is below a defined threshold.

Access control policy enforcement methods

Cai *et al.* (2018) reviewed existing access models and policies among different application scenarios focusing on cloud and user requirements. Damiani *et al.* (2007) proposed a geographical Role-Based Access Control. It relied on role-based mechanisms and defined constraints according to user location and position.

Rajkumar & Sandhu (2016) proposed POSTER for enhancing administrative role-based access control. It has integrated obligations via an administrative model by defining three main obligatory actions. However, the model only focused on administrative actions within the system. In 2016, Tarkhanov (2016) addressed the access control difficulties related to objects and linked object states.

The majority of existing research efforts on cloud security focus on users/intruders, traffic monitoring, and computing entities. Detecting and predicting security breaches based on object interaction and system policy have not received much attention. A thorough search of relevant literature yielded the conclusion that this research is the first to define and use interaction parameters to construct dynamic security boundaries and detect and predict security violations.

Cloud Object Model used for Interaction Model

This section describes the cloud object model and the required components to be used in our interaction model. Traditional physical security mechanisms are ineffective in dealing with threats and activities from virtual systems and virtual resource components (Jararweh *et al.*, 2016), as virtual boundaries between virtual components are not often well defined. The infrastructure desires a logically centralised security controller with visibility of security boundaries within different layers. For this purpose, a security model was proposed as a dynamic, intelligent, and automated security service/model to tackle the mentioned challenges in a multi-tenant cloud infrastructure (Farahmandian & Hoang, 2017). It provides a security model, and a security service called the Software-Defined Security Service (SDS_2) that applies to the object-oriented entities of a cloud environment, the interaction among them, and security policies that govern the interaction. The SDS_2 provides a security architecture to protect cloud assets with policies mapped to the cloud, tenant, and resource security policy levels.

The main idea of our centralized model centres around the interaction between constrained entities and is governed by system security policies for the detection and prediction of security breaches. An interaction can be defined as a *relation* between the objects during a specific time slot. To define the

http://doi.org/10.18080/jtde.v9n2.364

security boundaries in terms of interaction, the system requires a sustainable object model. In our security architecture, we define an object as *a component or a sub-component, both virtual and physical, that participates in a cloud environment and can access/be accessed by other objects according to their properties, security constraints, and system policies*. An object has a number of attributes, some are common among all objects (generic), and some represent specific constraints and characteristics of the object (specific). Each attribute defines some properties, and hence together they constitute a boundary for an object relative to other objects in its environment. An object can be simple or complex. A complex object includes nested attributes and may consist of a set of sub-objects. An object can be internal or external to a cloud, depending on its role/interaction.

It should be noted that the policy level is related to the role of an object, and location is associated with the logical or physical location of an object. The security model defines three main objects associated with the cloud, tenant, and resource security domains. Corresponding objects are Cloud Object, Tenant Object, and Resource Objects, which include Compute Object, Storage Object, Network Object, App Object, and User Object. The *cloud domain,* where cloud objects reside*,* classifies all the data, resources, and interactions at the cloud level while ignoring information related to lower domains like Tenant and Resource. At this level, the main parameters include cloud security policies (SPs), which govern interaction policies among objects at the cloud level; and data and resources policies, which concentrate only on cloud resource level (tenant, cloud-compute, -net, -storage resources). The *tenant domain* only reflects attributes and parameters related to the tenant objects in the cloud domain. The focus is only on the tenants' structure and their parameters and resources. The *resource domain* concentrates on the base underlying physical/virtual resources within the cloud system, as distinct from resources at the cloud and the tenant domains. They provide detailed information related to each resource object. Resource objects are defined similarly to cloud objects but for objects in the resource domain.

A *role (Rl)* assigns some responsibility to an object and the necessary authorities or privileges to discharge its duty. The role is often not static and may change as circumstances demand. A role may be simple or complex, assigned to an individual or a group of objects. A role is often associated with different layers of the architecture of a cloud system. It should be noted that 'role' is best defined using formal logic that entails complex rules to deal with dynamicity and multiple inheritances. In this paper, we avoid the complexity by simply equating a role with a hierarchical level in our defined cloud security architecture. Its attributes are defined explicitly when the role is assigned to a cloud object.

We define an *entity (E)* as an integrated object consisting of the object's role and object structure. The entity is a key concept in our structure to detect and predict security breaches in cloud infrastructure. The role assigned to the object will be considered based on object level and position within the system extracted from defined object parameters. An object may be assigned a role or

http://doi.org/10.18080/jtde.v9n2.364

group of roles activated at a different system level. Objects may assume more than one role with different levels of authority in different domains. We use E as the main component within the interaction model.

Interaction Model

In this section, we introduce our interaction model and its parameters. Security will always be a concern when entities start interacting with each other and with the infrastructure. In general, an interaction is *an act of performing an action by an object on another. A natural disaster can also be considered a special interaction between an external object on a set of objects.* An action always entails some effects or consequences. Potential security violations may occur when an interaction occurs against policies governing the relationship between two or more parties.

Consequently, interactions play a central role in security incidents in a system. The main focus of the Software-Defined Security Service (SDS_2) is on the protection of a cloud system by anticipating possible security breaches and preventing them from happening. The SDS_2 proposes a novel interaction model that defines exceptional interaction parameters to detect and predict security violations. The following sub-sections describe a detailed structure of each parameter. The scheme centres around a new model of interaction, entities connected to a cloud system, and security policies governing the system.

Table 1. Summary of Notations

Notation	Description
$\boldsymbol{E_i}$	Denotes entity i
$\boldsymbol{M}$	Denotes the interaction mode
$\boldsymbol{m_i}$	A set of mode relation values of the interaction mode
$\boldsymbol{d_n}$	A set of action direction values of the interaction mode
R	Denotes the positional interaction relationship
Rl	Refers to a set of roles of an object
$\boldsymbol{r_n}$	A set of positional relation values of R
T	Refers to interaction time consisting of $t_s(start\ time)$, $t_e(end\ time)$, $t_d(duration\ time)$, and $\alpha\ (interaction\ state)$
$\boldsymbol{A}$	Represents a set of all possible actions
P	Refers to system security policy
C	Refers to entities' constraints
$\mathbf{S_k}$	Refers to set of security policies on k
$\boldsymbol{L^k}$	Refers to location-based security policy of interaction k
$\boldsymbol{t^k}$	Refers to validate time for an interaction k
M	Set of permissible parameter values for interaction $I_{p,c}^k$
V	Set of non-permissible parameter values for $I_{p,c}^k$
I	Refers to an interaction

In its general sense, an interaction takes place between simple or complex entities in a defined environment such as a cloud system. Figure 1 shows simple and complex interactions between simple and complex entities. We propose an interaction model for characterising a relationship between objects. The interaction model describes how objects interact with one another; it characterises the

http://doi.org/10.18080/jtde.v9n2.364

modes of interaction, the *roles* of interacting entities, the *actions* one can perform against others, and the *time* of the interaction. To capture the essentials of an interaction, we define an *object model of interaction* with four parameters or variables: mode (M), positional relationship (R), action (A), and time (t). Each parameter may take on a range of values. The range is determined or constrained by a) the interaction environment such as organisational policies; b) participating entities of the interaction in terms of their nature, properties, capabilities, and constraints; c) roles of the participating entities such as their relative positional relationship; and d) the time of the interaction. These parameters will be defined later in this section.

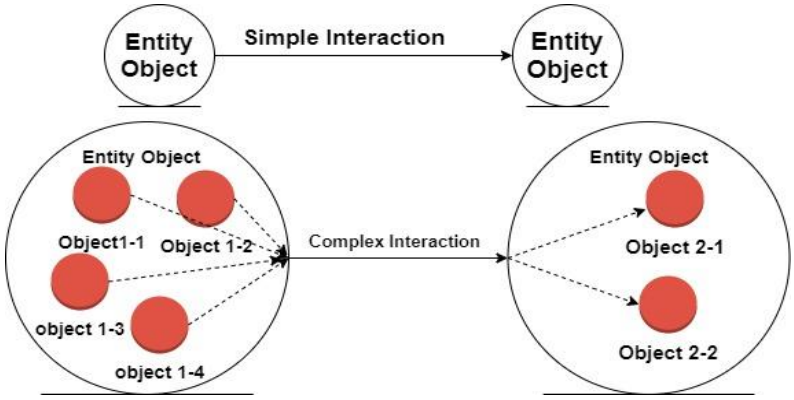


Figure 1. Interaction Types

With these descriptions of the interaction object, we will be interested in the following operations:

- We want to initialise an interaction, allowing default values for all parameters without any constraints.
- We want to know what actions are possible and what are not, due to the constrained nature of the entities involved in the interaction.
- We want to know if the interaction is permissible under a set of governing system policies.

Specifically, we can define several base operations on an interaction between entities:

- Initialise (I): Initialise I with default parameters M, R, A and t
- Mode ($I^k_{E_iE_j}$): Return all the possible modes between E_i and E_j for interaction k
- Relate ($I^k_{E_iE_j}$): Return all possible positional relations between E_i and E_j for interaction k
- Action ($I^k_{E_iE_j}$): Return all possible actions between E_i and E_j for interaction k
- State ($I^k_{E_iE_j}$, S_k): Return all allowed M, R, A and t once the constraints for participating entities and security policies (S_k) have been applied to the interaction.

Additional operations involving entities, their constraints, and system policies relevant to security violation and detection will be described in Security Policy-based Interaction Model below.

Interaction mode

Interaction mode (M) determines both the mode relationship (m) between objects, such as one to one, one to many, etc., and the action direction (d) of the interaction from one object to another, such

http://doi.org/10.18080/jtde.v9n2.364

as one way, both ways, etc. M consists of two parts: the first part refers to the mode relation (m_i), and the second refers to the action direction (d_n). So, M is defined as a set of pairs consisting of m_i and d_n: $M = m_i \times d_n$ where m_i refers to a set of possible relations between entities. $m_i \in \{m_1, m_2, m_3, m_4, m_5, m_6\}$. The values of m signify the following: $m_1 := 1{:}\,1 (one{:}\,one)$; $m_2 := 1{:}\,m\ (one{:}\,many)$, $m_3 := m{:}\,1 (many{:}\,1)$, $m_4 := m{:}\,m\ (many{:}\,many)$, $m_5 := 1{:}\,0\ (isolated)$, $m_6 := 0{:}\,0\ (no\ relation)$.

An interaction's action direction may take on one of three possible values, d_1 d_2, and d_3. Specifically, $d_1 = 1 :=\rightarrow (left\ to\ right)$, $d_2 = 2 :=\leftarrow (right\ to\ left)$, $d_3 = 3 :=\leftrightarrow (two\ way)$.

Interaction positional relationship

An object within a system or an organisation exists at a position either defined by its role within the organisation or the layer or the domain within the system architecture. In an interaction, the role of an entity and its standing relative to the role of the other entities is important, as this may dictate whether the interaction is legitimate. For this reason, we consider a positional interaction relationship (R) as the relative positional relationship between the entities of an interaction. The positional relationship determines the validity of an interaction action through defined rules, roles, layers, and policies associated with an entity's interaction.

For example, a security policy may specify that only objects in the same domain or at the same level may interact. Interaction level is entangled with the role-based level assigned to each domain in the design. Each level entails classified security policies associated with object roles that determine a set of authorised actions. As "roles" may be of a complex nature with inheritance and may change during an entity's lifetime, we simply restrict and associate roles with three positional interaction relationships in any interaction between objects to three different security isolation layers of the security architecture: Cloud, Tenant, and Resource.

In this design, *R* denotes the positional interaction relationship according to entities' relation during an active interaction. $R \in \{r_1, r_2, r_3\}$, where r_1 is mapped to **down,** representing the interaction between objects from a high layer to a lower layer; r_2 is mapped to **up**, representing interaction from a lower layer to a higher layer; r_3 is mapped to **equal,** representing the interaction between objects in the same layer. Knowledge about positional relationships among objects helps to define the nature of an interaction and the security policy decision.

Interaction time

Interaction time (t) refers to the valid time for an interaction to take place in the system. The interaction time can be specified either by its start time and its end time (t_s, t_e) or by start time and duration (t_s, t_d). There may be cases where the start time of an interaction is known but its end time may be indeterminate depending on some environmental conditions. For such cases, t_d is replaced

http://doi.org/10.18080/jtde.v9n2.364

by the *interaction state* (α) to indicate if the interaction is still ongoing (**on**) or has stopped (**off**). Interaction time can thus be specified by $t = \{(t_s, t_e)\ or\ (t_s, t_d)\ or\ (t_s, \alpha)\}$

Interaction action

An interaction is meaningful if it conveys a particular set of actions. A security breach occurs when objects perform an action that violates their permissible interactions. An action is defined as a possible set of actions over an interaction between system objects by virtue of their specific relationship connected to the system. An action is a set of possible activities that an event may trigger; however, the set of possible actions is often limited by the nature and constraints on object/entities involved and security policy rules governing them and their interactions. Let $\boldsymbol{A}$ represent a set of possible actions that are chosen based on the types of objects found in a cloud environment. For our cloud security model, we studied cloud objects and established the set $\boldsymbol{A}$ of actions as follows: 'read', 'write', 'modify', 'create', 'delete', 'execute', 'migrate', 'suspend', 'enable', 'disable', 'reset', 'lock', 'activation', 'unlock', 'clear'. Clearly, an object cannot perform all actions, as they are subject to system policies and object constraints. Table 2 describes the meaning of actions in $\boldsymbol{A}$.

Table 2. Action Description

Action	Description
Read (Re)	Permission to read the data on another Object
Write (W)	Permission to write data onto another Object
Modify (Md)	Permission to change (Write and Delete) existing data on another Object
Create (Cr)	The right to create instances of another Object
Delete (D)	The right to remove instances of another Object
Execute (Ex)	The rights to run an instance of another Object
Migrate (Mi)	The rights to re-map an instance of another Object
Suspend (Sp)	The rights to pause an instance of another Object
Enable (En)	The rights to run or power up another Object
Disable (Di)	The rights to power down another Object
Reset (Rt)	The rights to delete metadata and reboot instances of another Object
Lock (Lk)	The rights to deny user access to another Object
Unlock (U)	The rights to permit user access to another Object
Activate (Av)	The rights to make another Object available to a User
Clear (Cl)	The rights to remove user data from another Object

Security Policy-Based Interaction Model

This section describes our policy-based interaction model and how we use security policies at the interaction level to detect and predict security breaches. In our design, security policies are mapped to rules that determine the interaction parameters between entities. The proposed policy-based interaction model constructs dynamic security boundaries formed by legitimate interaction parameters according to security rules extracted from the governing security policies. Our model

http://doi.org/10.18080/jtde.v9n2.364

focuses on security policies at the interaction level between entities through a set of interaction parameters. The complex structure of cloud infrastructure and the shared and dynamic nature of their resources demand robust security policy enforcement. This requires a clear definition of a boundary between violated and non-violated policies. Applying security policies at the interaction level allows a system to make visible previously undefined virtual boundaries between engaged entities through their interaction parameters. In the following, we describe our policy-based interaction model and its required components.

A policy can be defined as "an aggregation of policy rules", where policy rules are used to construct sets of conditions consistent with the set permissible actions (Stone, Lundy & Xie, 2001). Policy rules are often derived from human language statements extracted from service level agreements (SLAs) between users and service providers. NIST (2015) defines security policies as *"Aggregate of directives, regulations, rules, and practices that prescribe how an organisation manages, protects, and distributes information"*. In our design, security policies address rules and conditions that establish valid interactions between entities in a cloud environment. In the SDS_2 architecture, we define a security policy (SP) as *a directive that governs the interaction among simple/complex entities through specific constraints applied to the entities, their location, and their interaction parameters*. Security constraints extracted from security policies determine the validity of a set of actions taking place during an interaction. Figure 2 illustrates the relationship among these components.

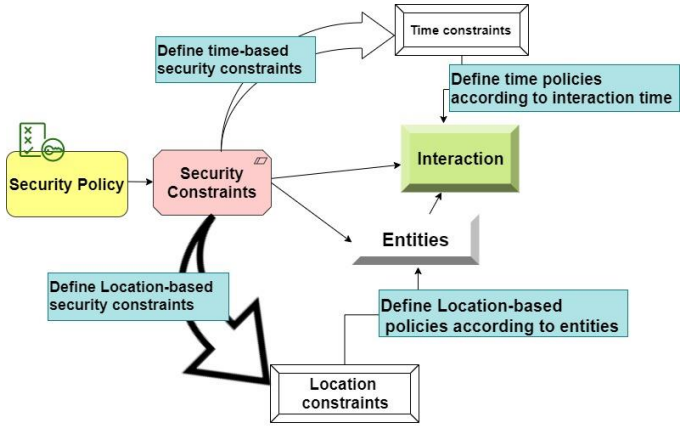


Figure 2. Security policy and its components

As discussed, system security policies, when applied to an interaction between the initiator (E_i) and the target entity (E_j), determine sets of parameters (described in the cloud object model) that are secure (valid or permissible) for the interaction. We define a *Security Policy-Based Interaction* model, as shown in Figure 3. Security policies govern the validity of the parameters of the interaction. Together with the system security policies (P), security constraints (C) on entities further limit the interaction in time, isolation level, and location, as defined by legitimate interaction parameters. The SDS_2 architecture logically divides cloud infrastructure into three main security isolation levels (SILs) or boundaries for the Cloud, Tenant, and Resource cloud domains. Recently, Yin *et al.* (2018)

http://doi.org/10.18080/jtde.v9n2.364

introduced a security service framework with three security layers according to security domain divisions; however, the system only focused on divisions related to tenant resources and VMs in building isolation layers. We map security domains into security isolation levels that isolate each domain's entities according to their security policy levels and the entities' locations. Figure 4 shows these isolation levels.

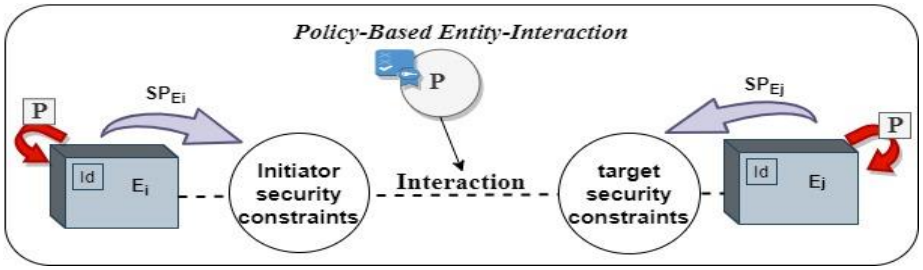


Figure 3. Security Policy-Based Interaction Model

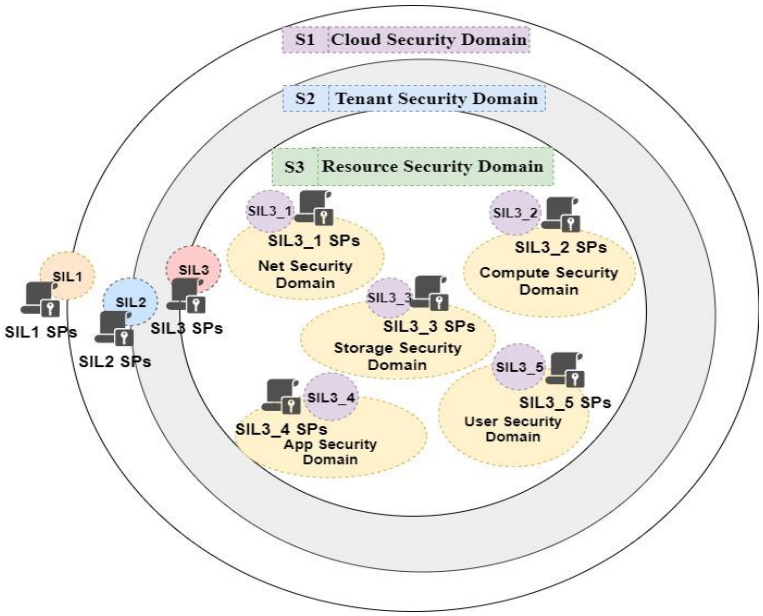


Figure 4. Security Isolation levels

Security policy in our context covers 4 aspects: system interaction policy; time-based security policy; dynamic location-based security policy; and entity-specific constraint policy. System interaction security policies are organisational sets of security policies that dictate allowable object interactions, as specified by valid parameters of an interaction. Time-based security policies dictate the valid time or time duration of an interaction. These policies are often specified at runtime because they are needed when dynamic operational circumstances demand. Location-based security policies are required to deal with dynamic aspects of a cloud entity, such as changes in responsibility and logical/physical zone placement over time. Entity-specific constraint policies deal with the specific nature and properties of an entity. Some entities may not perform some activities because they do not possess the capability, while others are capable but their actions are constrained by relevant policies when they were instantiated. With these definitions, the set of security policies (S_k) relevant to an interaction I^k between E_i and E_j may be expressed by the following equation:

http://doi.org/10.18080/jtde.v9n2.364

$$S_k\left(I^k,(E_i,E_j)\right)=P_{E_iE_j}\left(L^k(E_i,E_j),t^k\right)=P_{E_iE_j}^{L^k,t^k}\quad where\ i,j\in N\ and\ i\neq j.$$

The notations are defined in Table 3. P denotes the system policy governing the entities, location, and time; L denotes location-based policies for each entity. If E_i, E_j are placed in the same zone and same group zone policy, the location policies are the same for both. The security policy-based interaction model concentrates on two main policy concepts: general policies and local policies. General policies apply to all requests within the system, and local policies apply separately to each entity and their interactions within the system according to their location and assigned constraints. Both sets of policies are stored in separate security databases. Security policies are extracted during an interaction, and rules and constraints are assigned and applied to the interaction over the valid interaction time duration.

Interaction Security Violation Detection and Prediction Algorithm (ISVDP)

With the introduction of the formal model of an interaction and its relationship with security policy, we propose an interaction security violation detection and prediction (ISVDP) algorithm. The ISVDP operates over the SDS_2 cloud infrastructure with three levels of security isolation. The algorithm automatically detects and predicts security breaches in relation to a requested interaction according to valid/invalid interaction parameters. The main parameters of ISVDP include:

- Initiator entity: an entity that initiates a relationship with another entity and establishes an interaction;
- Target entity (or Reactor): the entity of an interaction on which the initiator intends to perform certain actions;
- Entity's constraints: the constraints extracted from local policies related to both initiator's and target's role, type, and their intrinsic properties;
- A complete set of system security policies defined over the SDS_2 cloud and its isolation levels: Cloud, Tenant, and Resources;
- A requested interaction between the initiator and the target entities (for violation detection).

In ISVDP, a constraint is represented as "a security statement which defines a set of conditions that limits the scope and the property of an interaction between an initiator and its target entity". High-level security policies are written in human-language policies, which will be translated using a policy-translator within the SDS_2 controller. Armed with the translated security policies, a security controller determines the validity of an interaction between entities based on their defined interaction parameters. The detection and the prediction algorithms form two fundamental components of the ISVDP model. Both of them share and are built upon the initial three processing stages, as shown in Figure 5 for a specific interaction k. We define the required notations in Table 3. We define the basic set of operations on an interaction object with these notations in Table 4.

http://doi.org/10.18080/jtde.v9n2.364

Table 3. Required Notations

Notation	Meaning	Detailed expression
c_{jv}	Set of constraints associated with entity j	
E	An entity composed of role and object i	E= E_i^{jk}
I	An interaction object	
I_{init}^k	Interaction object k initialised with default parameters (unconstrained)	$I_{init}^k(*,*)$
I_C^k	Interaction object k with object constraints applied	$I_C^k(E_i, E_j)$ *or* $I_C^k\left(E_i(c_{iu}), E_j(c_{jv})\right)$
I_P^k	Interaction object k with system policies applied	$I_P^k(E_i, E_j, S)$
$I_{P,C}^k$	Interaction object k with both system policies and object constraints applied	$I_{P,C}^k(E_i(c_{iu}), E_j(c_{jv}), S)$
I_{req}^k	Interaction object k with parameters derived from an interaction request	$I_{req}^k(E_i, E_j)$
S_k	Interaction k policies derived from the system policies	$S_k = P_{E_iE_j}^{L^k,t^k}$

Table 4. Operations Defined on an Interaction Object

Operation	Meaning	Detailed expression
Initialise (I)	Initialise I with default parameters M, R, A and t	
Mode (I^k)	Return possible modes between Ei and Ej for interaction k	*Mode of* (I_C^k *or* I_P^k *or* $I_{P,C}^k$)
Relate (I^k)	Return possible positional relations between Ei and Ej for interaction k	*Relate of* (I_C^k *or* I_P^k *or* $I_{P,C}^k$)
Action (I^k)	Return possible actions between Ei and Ej for interaction k	*Action of* (I_C^k *or* I_P^k *or* $I_{P,C}^k$)
Const (I^k)	Return possible interaction parameters after applying constraints on interaction k	*Const on* (I_{init}^k)
State (I^k)	Return all states of interaction k between Ei and Ej	*State of* (I_C^k *or* I_P^k *or* $I_{P,C}^k$)
State (I^k, req)	Return all states of the interaction, as required by the request	*State of* (I_{req}^k)
Policy (L, E_i)	Returns the set of system policies applied to entity i location	
Policy (I^k, req)	Return the set of system policies applied to interaction k	*Policy on (Ik or* I_{req}^k)
Compare (I_m, I_n)	Compare the states of interaction m and interaction n, return differences in M, R, A, and t	
Opposite (I^k)	Returns set of possible violated mode parameters extracted from valid interactions	

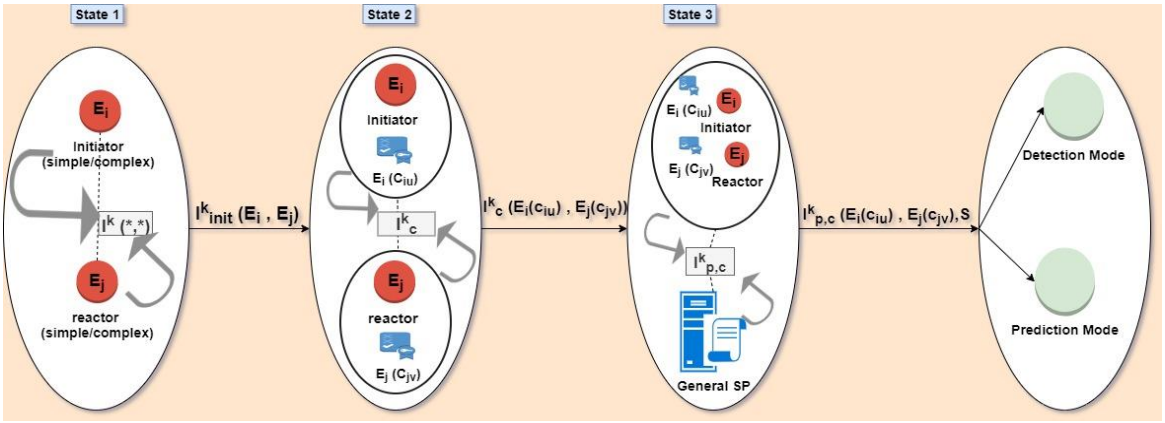


Figure 5. ISVDP stages

http://doi.org/10.18080/jtde.v9n2.364

Stage 1: Initialising the interaction. At this initial stage, the objects involved in the interaction are made available with their security-rated properties. The interaction template is initialised with no constraints on interaction parameters. The requested interaction is also made available. The result of this stage is the object $I_{init}^{k}(*,*)$. The algorithm intelligently identifies all involved entities and components in this stage. Additionally, the algorithm detects the interaction type and parameters. Dynamically it can change interaction parameters according to the location and nature of entities and create initial interaction parameters between two entities.

Stage 2: Application of entity constraints over the interaction k. At this stage, the interaction parameters are modified according to the properties and constraints of the entities involved. The result of this stage is the object $I_{c}^{k}\left(E_i(c_{iu}), E_j\left(c_{jv}\right)\right)$.

Stage 3: Application of the policy over the interaction k. At this stage, the parameters of interaction k will be modified by the constraints derived from the system policies that apply to interaction k. The result of this stage is the object $I_{p,c}^{k}\left(E_i(c_{iu}), E_j\left(c_{jv}\right), P\right)$. The policy-driven interaction algorithm encompassing stages 1, 2, and 3 is shown in Algorithm 1.

Algorithm 1. Policy-driven interaction (PdI ())

Input: Ei, Ej, SDS2 cloud objects' DB, System Policy statement (P)

Output: $I_{p,c}^{k}$ *(M', R', A', t')*

1: while request is valid do

2: for Ei, Ej do

3: Intialize (Ik) //get interaction parameters for E_i, E_j *without applying constraints and set* I_{init}^{k}

4: if $I_{init}^{k} \neq Null$

Const (I_{init}^{k}) *//get interaction parameters by applying constraints on* I_{init}^{k} *and set* I_{C}^{k}

5: I_{C}^{k} *= State* (I_{C}^{k}) *// return parameters after applying constrains*

6: Policy (Ik) // get system policies (P) applied to the Ik

7: $I_{p,c}^{k}$ *= State (Ik) // return parameters after applying policy system*

8: end if;

9: end for;

10: end while;

Interaction Security Violation Detection

Consider an interaction within a cloud system. The detection algorithm determines if the interaction is safe or violates the system's security policy or, specifically, if a security breach has occurred. With the global knowledge of the cloud environment and the interactions among entities, the security controller intelligently schedules the execution of the Interaction Security Violation Detection (ISVD) algorithm on suspicious circumstances, on a specific request or triggered events, or on a regular basis. The algorithm considers each interaction parameter under consideration to discover if any

http://doi.org/10.18080/jtde.v9n2.364

inconsistency has occurred relative to the security policies, and hence the interaction parameters dynamically applicable to the interaction. The module goes through the three fundamental stages as described above and proceeds to stages 4d, 5d, 6d and 7d for violation detection as follows.

Stage 4d: The requested interaction policy level is analysed according to defined security isolation levels explained for the security policy-based interaction model *(Domain (I^k_{req}))*.

Stage 5d: The interaction under consideration between the specified objects is analysed, resulting in a set of interaction statuses required by the request: $I^k_{req}(E_i, E_j)$.

Stage 6d: The algorithm intelligently detects each object interaction parameter rule based on security domain and location Domain, *($I^k_{req}(E_i, E_j)$)* and Loc *(E_i, E_j)*.

Stage 7d: By analysing $I^k_{p,c}\left(E_i(c_{iu}), E_j(c_{jv}), P\right)$, and $I^k_{req}(E_i, E_j)$ *interaction parameters*, the algorithm determines if requested actions are within the set of actions allowable by the policies and constraints imposed on the entities of the interaction.

The algorithm returns the validation status of the interaction: either Safe or Violate. “Safe” means that the requested interaction does not violate any policy related to any interaction parameter and is not a security breach. “Violate” means that the requested interaction violates one of the parameters (M, R, A, t) or location of the allowed security policy that governs the interaction. The algorithm returns whenever a violation of an interaction parameter is detected. However, in cases where policies governing the interaction parameter are undefined (either due to an oversight or situations not yet encountered), it will decide if there is a possibility to partially accept the interaction and initiate an alert for the decisionmaker to create a new policy to cover the newly discovered situation.

Figure 6 shows the decision process of the ISVD algorithm which determines interaction states using the ISVD algorithm. We use (M', R', A', t') to denote State $(I^k_{p,c})$ and (M'', R'', A'', t'') to denote State (I^k_{req}). In the detection process, all system policies, including location, and entity constraints are applied to the interaction k to obtain all the allowable parameters of the interaction. Figure 6 shows the detection approach in determining the validation status of the requested interaction k. The detection algorithm will stop the process on discovering the first interaction parameter violation and activate a security alarm within the security controller. Algorithm 2 describes the ISVD detection algorithm, which analyses the I^k_{req}, extracting number and types of involved entities during the requested interaction. Figure 6 demonstrates the state that an interaction will be considered to be in after using the ISVD algorithm. The results are based on two main conditions defined as equal (=) (where each specific interaction parameter of $I^k_{p,c}$ is equal to its I^k_{req} interaction parameter) and not equal (!) (where interaction parameters of $I^k_{p,c}$ are not the same as I^k_{req}).

http://doi.org/10.18080/jtde.v9n2.364

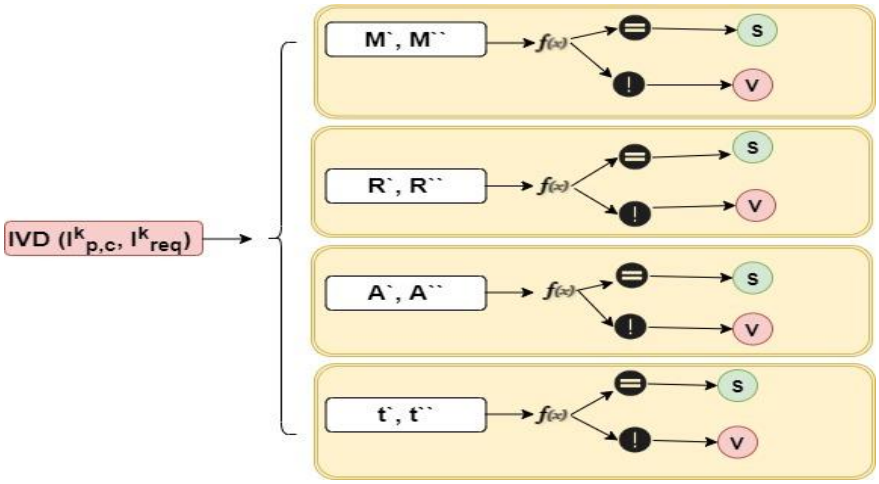


Figure 6. ISVD algorithm

Algorithm 2. Interaction Security Violation Detection (ISVD ())

Input: I^k_{req}*(requested interaction),* $I^k_{p,c}$,

Output: Safe | Violate

1: for received I^k_{req} *do*

2: if Domain (I^k_{req})*==True then*

3: Policy (L, E) //Returns set of system policies on the current location of entities during the initiation of I^k_{req} *and set L*

4: If L == True (location is verified) then

5: PdI () //call the algorithm 1 to get $I^k_{p,c}$

$I^k_{P,C} = State\ (I^k_{P,C})$

6: $I^k_{req} = State\ (Ik, req)$ *// get requested interaction parameters*

7: for I^k_{req} *and* $I^k_{P,C}$ *do*

8: diff := $Compare\ (I^k_{P,C}, I^k_{req})$ *// returns difference (diff) parameters between* $I^k_{P,C}$ *and* I^k_{req}

9: P := Policy (Ik, req) // returns system policies applied to interaction parameters

10: if diff satisfies P then

11: state (I^k_{req}*) is safe*

12: else state (I^k_{req}*) is Violate //rise security violation alarm to security controller, isolate the interaction*

13: end if;

14: end for;

15: end if;

16: end if

17: end for;

Interaction Security Violation Prediction

In this section, we describe the prediction algorithm and its functionality. The Interaction Security Violation Prediction (ISVP) algorithm enables interaction violation predictability based on

http://doi.org/10.18080/jtde.v9n2.364

permissible values of the parameters of the interaction. The algorithm is different from the detection algorithm in that it determines all "Safe" interactions and all potential "Violate" interactions under the system security policies and constraints imposed on the interaction parameters between given entities. The prediction algorithm automatically discovers the probability of a possible future violation according to the current state of validation interaction parameters. For each interaction parameter, it discovers upcoming violation values. It analyses the state of entities' interaction and predicts future violations according to unacceptable interaction parameters within the system. The prediction algorithm considers each interaction parameter and determines the invalid parameter values through prediction approaches. The prediction algorithm proceeds through the three stages of Algorithm 1 and proceeds through stages 4p and 5p, as shown in Algorithm 3.

Stage 4p: The stage outputs all possible "Safe" interaction parameters between the given entities considering all constraints and security policies.

Stage 5p: The outputs are all potential "Violate" interactions between the given entities.

This is done by inspecting each parameter (M, R, A, t) and applying security constraints on each parameter. If M_s (safe parameters defined for M during k interaction) is the allowed set of safe modes, then $M_v = M - M_s$ is the set of violate modes (M is all possible values). Similarly, R_s and R_v are the set of allowed relational positions and violate relational positions, respectively; A_s and A_v are the set of allowed actions and violate actions, respectively. Similar notations are used for time and the location. The results allow the system to predict possible security breaches if interaction parameter conditions are not met. These conditions display the predicted violations in terms of interaction parameters.

Ideally, all possible violations relative to the current interaction can be discovered/predicted; however, if all the interaction parameters are allowed to vary independently of one another, the analysis can be computationally expensive and not practicable. Realistically, we may want to address and predict most likely violations. We thus restrict ourselves to simple situations where one parameter varies at a time, just to illustrate the prediction process. In the predicting state, the system anticipates all possible different situations that current interaction parameters between defined entities can face. For instance, if the valid actions between two objects are defined as "read", all other possible actions can be considered violations of interaction parameters considering the object nature and constraints. So, the system can stop the violation using its stored predicted violation parameters rather than going through lower layers and nested policy discovery. In the presented prediction algorithm, all opposite interaction parameters against validation parameters are considered potential interaction parameter violations. The security controller runs the ISVDP algorithm to discover the probability of future attacks according to each interaction parameter for an interaction, say *k*. It is an intelligent mechanism that focuses on interaction parameters and their possible forthcoming violation during an interaction.

http://doi.org/10.18080/jtde.v9n2.364

Algorithm 3 Interaction Security Violation Prediction (ISVP ())

Input: $I_{p,c}^{k}$

Output: V set of possible potential violate interaction parameters

1: PdI () // set $I_{p,c}^{k}$

2: for $I_{p,c}^{k}$ do

3: while T_M = Mode ($I_{p,c}^{k}$) do // get all possible sets of M extracted from $I_{p,c}^{k}$ from safe mode

V_M= opposite (T_M) // set of possible violated mode parameters extracted from valid (T_M)

4: end while;

5: while T_M = Relate ($I_{p,c}^{k}$) do // get all possible sets of R extracted from $I_{p,c}^{k}$ from safe mode

V_R = opposite (T_R)// sets of possible violated R from $I_{p,c}^{k}$ from safe mode

6: end while;

7: while T_A = Action ($I_{p,c}^{k}$) do // get all possible sets of A extracted from $I_{p,c}^{k}$ from safe mode

V_A = opposite (T_v) // sets of possible violated A from $I_{p,c}^{k}$ from safe mode

8: end while;

9: V = (V_M, V_R, V_A) // set of predicted and possible violation interaction parameters according $I_{p,c}^{k}$

10: end for;

Interaction Scenarios and Results

In this section, we demonstrate our policy-driven security scheme by using a security controller in verifying allowable interactions and detecting policy violations between entities in a cloud infrastructure based on our proposed model of interaction. We built the security controller from scratch in Java language and run our ISVDP algorithm in an Ubuntu machine with 16 GB RAM, Intel® Core (TM) i7-7600U CPU. We set different scenarios according to various interaction types, and analyse the results to evaluate the proposed interaction model and its components for each case. We simulate the interaction between different types of objects within the system to detect and predict security violations according to our ISVDP model. We consider the CloudSimSDN-NFV framework (Son, He & Buyya, 2019) to simulate the cloud infrastructure and build our security controller and its ISVDP algorithm. Figure 7 demonstrates the implementation process.

Scenario 1: User interaction. In this scenario, the security controller (SC) receives interactions triggered by a user. The SC identifies the user and interprets the request for an interaction. According to the user level and rights, the security controller determines the security policies related to the user and involved objects. The requested interaction is sent to the interaction security domain controller to extract security policies and interaction parameters. The security controller then initiates a virtual security function (VSF) designed to monitor the interaction based on the received validated interaction, entities' policies, and constraints. The analyser function is responsible for running the ISVDP algorithm to detect and predict security violations.

http://doi.org/10.18080/jtde.v9n2.364

Scenario 2: Specific requested interaction. In this scenario, a specific interaction runs within the system. The specific interaction is considered as a request to monitor a specific interaction being performed by the security controller. This scenario occurs when the security controller decides to monitor an interaction between specific entities within the system. The security controller triggers an interaction to be monitored among specific entities. It will happen mainly in two sub-scenarios: 1) randomly monitor an entity based on its statistics received from its virtual security functions; 2) activate a scheduled monitoring of a sensitive entity within the system in specific time slots.

Scenario 3: Triggered interaction. The security controller activates a virtual security function to monitor a triggered interaction. This scenario occurs when an abnormal interaction is triggered between entities within the system. The security controller initiates and commands reports from relevant virtual security functions over suspicious entities and then executes the ISVDP algorithm to assess the situation.

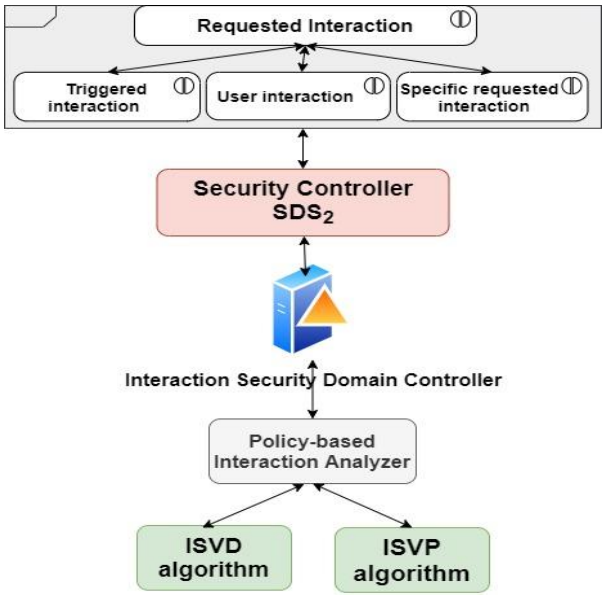


Figure 7. Implementation process

The functions within the security controller perform the ISVDP algorithms and produce the results. As demonstrated in Figure 8, the security controller analyses the requested interaction and involved objects. Security policies and objects' constraints are extracted according to object security isolation layers and entities' location. In this paper, however, we mainly concentrate on the interaction between simple objects and their interactions. Figure 5 shows the flow process of our ISVDP algorithms. In the first step, the security controller creates entities within the cloud system by substantiating the identified objects together with their defined role. In Figure 8 below, the security controller, after receiving the interaction, triggers and assigns a specific VSF to monitor each interaction. It extracts required policies for each interaction and assigns a unique policy ID (P.Id). It labels each interaction based on specific interaction ID (Int.Id) and extract validate time (V. Time) for each interaction as well. Each VSF lifecycle starts according to triggered requested interaction.

http://doi.org/10.18080/jtde.v9n2.364

Type	VSF Id	Src.	Dest.	P. Id	Int. Id	St. Time	count	V. Time	exec
SET	VSF 1	NETWORK	USER	243	1	22:36:31	1	13	n
UPDATE	VSF 2	STORAGE	NETWORK	244	2	22:36:39	0	31	n
GET	VSF 3	NETWORK	APPLICATION	245	3	22:36:41	8	34	n
GET	VSF 4	APPLICATION	STORAGE	246	4	22:36:46	8	75	y

Figure 8. Extracting involved objects and assigning a monitoring security function to each interaction

We consider cloud objects of different types and determine possible allowable interactions. For each scenario, objects can be at the same or different access levels. System policies are applied to achieve validate interaction parameters once an interaction is triggered. For simplicity, interaction time is assumed valid throughout the whole time under consideration. We detail below an interactive case study between two entities to describe the process of discovering and validating the interaction between the two entities. In the following case, we describe how a policy-based interaction analyser will extract required interaction parameters to be sent to the assigned security function.

VM-Storage interaction: interaction between a virtual machine and a storage entity. In the first step, the program at the controller level creates participating entities (if they have not existed yet) based on the information stored in the security database, SecDB. Then, the security controller analyzes the interaction and extracts policies applied to the requested interaction between the two entities according to each entity and their level within the cloud infrastructure.

As depicted in Table 5, the second and third columns show values of the VM and the storage entities' interaction parameters after their constraints have been applied. The fourth column shows the interpretation of the system policy on the objects' interaction parameters. The last column shows all possible interactions between the two entities as determined by the allowable interaction parameters after all constraints and system policies are considered. The results indicate that the only allowable actions are Re, W in an allowable pair of (m_1, d_2) mode of interaction between the VM and the cloud system's storage entities. In our program, we consider *t* as an acceptable duration time over which an interaction can take place. For violation detection, the security controller calls Algorithm 2. It analyses the incoming request and extracts the required parameters and call $State\ (I_{req}^{k})$. During this phase, the requested interaction statement requests the *removal of a file from the storage object requested by the virtual machine at the same level.*

Table 5. Collected data from the controller for VM-Storage interaction

	I (VM)	I(Storage)	SysPolicy	$I_{p,c}^{k}$
M (m/d)	(m1, d1)	(m1, d1)	(m1, d2)	(m1, d2)
r	Cloud	Cloud	cloud	cloud
A	Re, W, D	Re, W	Re, W, Cr, D	Re, W
t	600 ms	600 ms	300 ms	300 ms

The program translates the incoming request, which detects the *delete* violation as a delete action against $I_{p,c}^{k}$. It raises a security alarm, indicating a violation by the requested interaction. For violation prediction against possible attacks, the system will call Algorithm 3 to predict possible violations

http://doi.org/10.18080/jtde.v9n2.364

against the parameters of $I_{p,c}^{k}$. The system calculates possible violation parameters relative to allowable $I_{p,c}^{k}$ parameters. In this case, interaction actions except for Re, W are considered as action violations. More importantly, this algorithm can enumerate all possible interaction violations between two entities (those not allowable by $I_{p,c}^{k}$) by systematically going through the mode, the positional relationship, the action, and the interaction's time parameters. As an example, if we keep all parameters except the mode parameters fixed, we can declare that other modes except m_1 and d_3 are potential (or predicted) violations. Similarly, the system considers any positional relation except *cloud* as a security breach and stores the data. An insider/outsider request that involves any of the predicted violation parameters will be investigated in anticipation of potential security breaches: $ISVP\ (I_{p,c}^{k}) \rightarrow V\ (V_M, V_R, V_A, V_t)$.

We executed various tests according to various scenarios to show expected results. Table 6 reveals some result samples that the security controller captured by performing many cases. The results are simulation results we captured by running various simulated cases to test our security algorithm. Table 6 demonstrates extracted parameters for each scenario through running our security algorithm.

In the table *Int* reveals validated parameters expected after running the PdI () algorithm. After running the ISVD () algorithm, it shows the results using *Act* parameter (s: safe, v: violate). We monitored our security controller performance according to the number of interactions triggered within the system from any resources, the detection processing time, and the time until the system detects the status of the requested interaction. As explained before, each requested interaction monitors by a specific VSF with unique identity (VSF Id) to be distinguished by the security controller. Figure 9 illustrates the SDS_2 performance using detection processing time in the face of different interactions. In the figure, the average processing time increased as the number of interactions received by the security controller increased.

Table 6. Expected results of the simulated scenarios

VSF ID	Src.	Res.	Int. Init	Int.				Act.	P. Id	exec
				M	**R**	**A**	**t**			
VSF 6	VM	Storage	SC	(m_1, d_3)	Cloud	Re, W	3000 ms	s	3	Y
VSF 3	User	Storage	SC	(m_4, d_3)	Tenant	Re, W	900 ms	v	3	N
VSF 2	Storage	APP	UR	(m_1, d_1)	Cloud	Md	10500 ms	v	22	Y
VSF 9	User	App	AT	(m_4, d_2)	Resource	Md	1000 ms	v	23	Y
VSF 7	VM	Storage	SC	(m_2, d_2)	Tenant	Re, W	800 ms	s	30	Y
VSF 11	App	Storage	SC	(m_5, d_2)	Resource	Re, W	600 ms	v	13	N
VSF 8	Net	VM	UR	(m_4, d_1)	Tenant	Ex, Re	600 ms	s	19	N
VSF 22	Storage	VM	AT	(m_1, d_2)	Cloud	Re	300 ms	v	22	N

http://doi.org/10.18080/jtde.v9n2.364

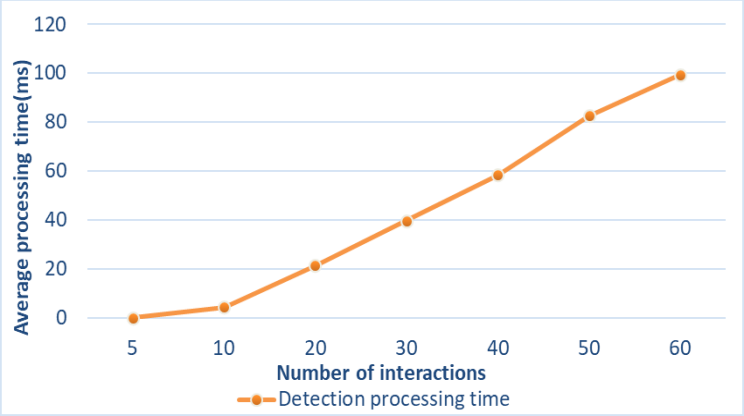


Figure 9. Performance monitoring according to interaction detection processing time

In this scenario, the security controller only considers simple interactions between two entities, while each interaction is initiated with pre-defined conditions, to test the SDS_2 security controller performance according to simple interaction types with pre-defined security policies.

Conclusion

This paper has taken a novel approach with the proposed Policy-based Interaction Model, to provide isolation within the cloud infrastructure. The proposed model introduced a dynamic construction of security boundaries based on our constructed interaction model and its parameters. To secure cloud resources, an intelligent security algorithm has been developed to provide proactive detection and prediction in relation to the interaction parameters. Security policy rules pertaining to entities and their location are further applied to the interaction parameters to determine the overall validity of the participating entities' interaction.

The policy-driven interaction model is, to the best of our knowledge, the first in a new direction for combatting security incidents systematically. A possible next step is to deploy the proposed SDS_2 in a real cloud scenario to detect and predict cloud security violations using new technologies, Software-defined Networking and Network Function Virtualisation.

References

Barjatiya, S., & Saripalli, P. (2012). Blueshield: A layer 2 appliance for enhanced isolation and security hardening among multi-tenant cloud workloads. Paper presented at the Proceedings of the 2012 IEEE/ACM Fifth International Conference on Utility and Cloud Computing.

Basile, C., Valenza, F., Lioy, A., Lopez, D. R., & Perales, A. P. (2019). Adding Support for Automatic Enforcement of Security Policies in NFV Networks. *IEEE/ACM Transactions on Networking, 27*(2), 707-720. http://doi.org/10.1109/TNET.2019.2895278

Cai, F., Zhu, N., He, J., Mu, P., Li, W., & Yu, Y. (2018). Survey of access control models and technologies for cloud computing. *Cluster Computing*, *22*, 6111–6122. https://doi.org/10.1007/s10586-018-1850-7

Chen, C., Li, D., Li, J., & Zhu, K. (2016). SVDC: A Highly Scalable Isolation Architecture for Virtualized Layer-2 Data Center Networks. *IEEE Transactions on Cloud Computing, 6*(4), 1178-1190. http://doi.org/10.1109/TCC.2016.2586047

Damiani, M. L., Bertino, E., Catania, B., & Perlasca, P. (2007). GEO-RBAC: a spatially aware RBAC. *ACM Transactions on Information and System Security (TISSEC), 10*(1), 2.

Del Piccolo, V., Amamou, A., Haddadou, K., & Pujolle, G. (2016). A survey of network isolation solutions for multi-tenant data centers. *IEEE Communications Surveys & Tutorials, 18*(4), 2787-2821. https://doi.org/10.1109/COMST.2016.2556979

Factor, M., Hadas, D., Harnama, A., Har'El, N., Kolodner, H., Kurmus, A., Shulman-Peleg, A., & Sorniotti, A. (2013). Secure logical isolation for multi-tenancy in cloud storage. Paper presented at the 2013 IEEE 29th Symposium on Mass Storage Systems and Technologies (MSST). https://doi.org/10.1109/MSST.2013.6558424

Farahmandian, S., & Hoang, D. B. (2017). SDS 2: A novel software-defined security service for protecting cloud computing infrastructure. Paper presented at the 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA). https://doi.org/10.1109/NCA.2017.8171388

Hoang, D. B., & Farahmandian, S. (2017). Security of Software-Defined Infrastructures with SDN, NFV, and Cloud Computing Technologies. In *Guide to Security in SDN and NFV* (pp. 3-32): Springer.

Jararweh, Y., Al-Ayyoub, M., Darabseh, A., Benkhelifa, E., Vouk, M., & Rindos, A. (2016). Software defined cloud: Survey, system and evaluation. *Future Generation Computer Systems, 58*, 56-74. https://doi.org/10.1016/j.future.2015.10.015

Karmakar, K. K., Varadharajan, V., Tupakula, U., & Hitchens, M. (2016). Policy based security architecture for software defined networks. Paper presented at the Proceedings of the 31st Annual ACM Symposium on Applied Computing. https://doi.org/10.1145/2851613.2851728

Kosiur, D. (2001). *Understanding policy-based networking* (Vol. 20): John Wiley & Sons.

Li, F., Li, Z., Han, W., Wu, T., Chen, L., Guo, Y., & Chen, J. (2018). Cyberspace-Oriented Access Control: A Cyberspace Characteristics-Based Model and its Policies. *IEEE Internet of Things Journal, 6*(2), 1471-1483. https://10.1109/JIOT.2018.2839065

Mavridis, I., & Karatza, H. (2019). Combining containers and virtual machines to enhance isolation and extend functionality on cloud computing. *Future Generation Computer Systems, 94*, 674-696. https://doi.org/10.1016/j.future.2018.12.035

Mundada, Y., Ramachandran, A., & Feamster, N. (2011). SilverLine: Data and Network Isolation for Cloud Services, HotCloud 2011, Portland, OR, USA. Available at https://static.usenix.org/event/hotcloud11/tech/final_files/Mundada6-1-11.pdf

NIST [National Institute of Standards and Technology]. (2015). Information security policy. Committee on National Security Systems Instruction, CNSSI 4009, Glossary. Revised April 6, 2015. US Department of Commerce.

Pfeiffer, M., Rossberg, M., Buttgereit, S., & Schaefer, G. (2019). Strong Tenant Separation in Cloud Computing Platforms. Paper presented at the Proceedings of the 14th International Conference on Availability, Reliability and Security. https://doi.org/10.1145/3339252.3339262

Rajkumar, P.V., & Sandhu, R. (2016). POSTER: security enhanced administrative role based access control models. Paper presented at the Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. https://doi.org/10.1145/2976749.2989068

Son, J., He, T., & Buyya, R. (2019). CloudSimSDN-NFV: Modeling and simulation of network function virtualization and service function chaining in edge computing environments. *Software: Practice and Experience*. https://doi.org/10.1002/spe.2755

Stone, G. N., Lundy, B., & Xie, G. G. (2001). Network policy languages: a survey and a new approach. *IEEE network, 15*(1), 10-21. https://doi.org/10.1109/65.898818

Tarkhanov, I. (2016). Extension of access control policy in secure role-based workflow model. Paper presented at the 2016 IEEE 10th International Conference on Application of Information and Communication Technologies (AICT). https://doi.org/10.1109/ICAICT.2016.7991691

Varadharajan, V., Karmakar, K., Tupakula, U., & Hitchens, M. (2018). A policy-based security architecture for software-defined networks. *IEEE Transactions on Information Forensics and Security, 14*(4), 897-912. https://doi.org/10.1109/TIFS.2018.2868220

Wang, X., Shi, W., Xiang, Y., & Li, J. (2015). Efficient network security policy enforcement with policy space analysis. *IEEE/ACM Transactions on Networking, 24*(5), 2926-2938. https://doi.org/10.1109/TNET.2015.2502402

Yin, X., Chen, X., Chen, L., Shao, G., Li, H., & Tao, S. (2018). Research of Security as a Service for VMs in IaaS Platform. *IEEE Access, 6*, 29158-29172. https://doi.org/10.1109/ACCESS.2018.2837039

Australian Mobile Survey 2021:

Mobile Buying and Churn Drivers Stable

David Kennedy
Venture Insights

Abstract: Venture Insights has been surveying Australian mobile consumers annually since 2018. The latest survey was conducted in March 2021 and included 1,019 respondents. The results show that price and network performance remain the main purchasing drivers for mobile services, with more than 90% of respondents rating them as important or very important. On price, 86% did not expect to spend more each year for their mobile phone services, which is consistent with previous surveys. The persistent importance of price shows that mobile services are seen as a commodity by many customers. A total of 38% of respondents were considering churning their mobile phone service; of these respondents, 40% chose price as the key churn driver. There is consistent focus on Mobile Virtual Network Operators (MVNOs) driven by price. The survey results suggested that the total market share for MVNOs could increase by 6 percentage points, if all respondents indicating a move to an MVNO actually did so. Only 20% of respondents indicated they were willing to pay more for 5G mobile services or handsets. A majority (55%) of respondents change their mobile phones every 2-3 years; 39% said they would consider purchasing a recycled/refurbished mobile phone at a lower price.

Keywords: Mobile consumers, Australia, survey, pricing, MVNO

Introduction

Venture Insights performs an annual consumer survey on mobile service and handset purchases across Australia. It asks questions around willingness to pay, intentions to switch service providers and handsets, and key factors responsible for this switching. We also ask which service provider the respondents are switching to, and thus determine the service providers that will gain or lose from this churn.

The survey shows that price remains a key driver for mobile purchasing, underlining the difficulty of maintaining price increases that would lift Average Revenue Per User (ARPU). Price continues to drive interest in Mobile Virtual Network Operators (MVNOs), but we expect

http://doi.org/10.18080/jtde.v9n2.422

that the Mobile Network Operators (MNOs) can at least defend market share through sub-brands like Belong and now GoMo and Felix.

Our latest survey was conducted in March 2021 for Australia, and the key findings are presented here. In this report, the term MVNO includes resellers that are subsidiaries of MNOs or owned by them. Note that, with a sample size of 1,019 respondents, sample proportions in the full sample can be determined with 95% confidence to within approximately 3 percentage points (under the Normal assumptions for an unbiased sample). Sampling errors for subgroups, such as age groups, may be larger.

Summary of key findings

Our latest consumer telco survey shows that price and network performance remain the main purchasing drivers for mobile services. More than 90% of respondents rated them as important or very important when deciding their next mobile service purchase, and 86% did not expect to spend more each year for their mobile phone services. Consumer reluctance to pay more for mobile services has been consistent across our surveys for three years.

Other key findings are:

- 38% of respondents were considering churning their mobile phone service. Of these respondents, 40% chose price as the key churn driver, far higher than any other factor. Data allowance came a distant second as the main factor, being picked by only 21% of these respondents.
- There is consistent focus on MVNOs driven by price. Data on intention to churn shows that the market share of MVNOs would increase by 6% if every respondent who indicated an intention to churn in fact did so. This 6% is a ceiling, not a forecast, but suggests that MNO defences against MVNOs are soft. The launch of new MNO sub-brands GoMo and Felix should help to address this.
- Only 20% of the respondents were willing to pay more for 5G mobile services or handsets. Although network performance/speed and price were chosen by equal numbers of respondents as the biggest factor when deciding their next mobile service purchase, price seems to be winning out when it comes to 5G. There is an appetite for 5G, but consumers are reluctant to pay more for it.
- 37% of the consumers have mobile phones between 1-2 years old, and a majority (55%) change their mobile phones every 2-3 years; 39% of respondents said they would consider purchasing a recycled/refurbished mobile phone at a lower price, suggesting handset price is also a factor for a segment of consumers when deciding their next mobile phone purchase.

http://doi.org/10.18080/jtde.v9n2.422

Pricing is Still a Key Driver

In our previous reports, we have raised issues around ARPU pressure on mobile service providers and highlighted the importance of price as a driver of mobile telecommunications buying by consumers. We have maintained that competitive intensity (along with COVID-19) (Venture Insights, 2020) will put pressure on ARPUs, which in turn requires a strong focus on keeping costs under control to maintain profitability. As the economic impact of the pandemic eases, consumers are spending more overall, but are still reluctant to spend more on mobile.

The importance of price was validated by our latest Australian consumer survey that asked respondents to rate the importance of factors such as price, data allowance, speed and coverage when deciding their next mobile service purchase. Price emerged as one of the leading factors for consumers, with 94% of the respondents rating it as important or very important (96% for current MVNO customers and 83% for MNO customers). Network performance and speed were considered equally as important as price by the respondents. The numbers in Figure 1 below are indistinguishable (within the margin of error) from our survey last year in March 2020. The persistent importance of price shows that mobile services are seen as a commodity by many customers.

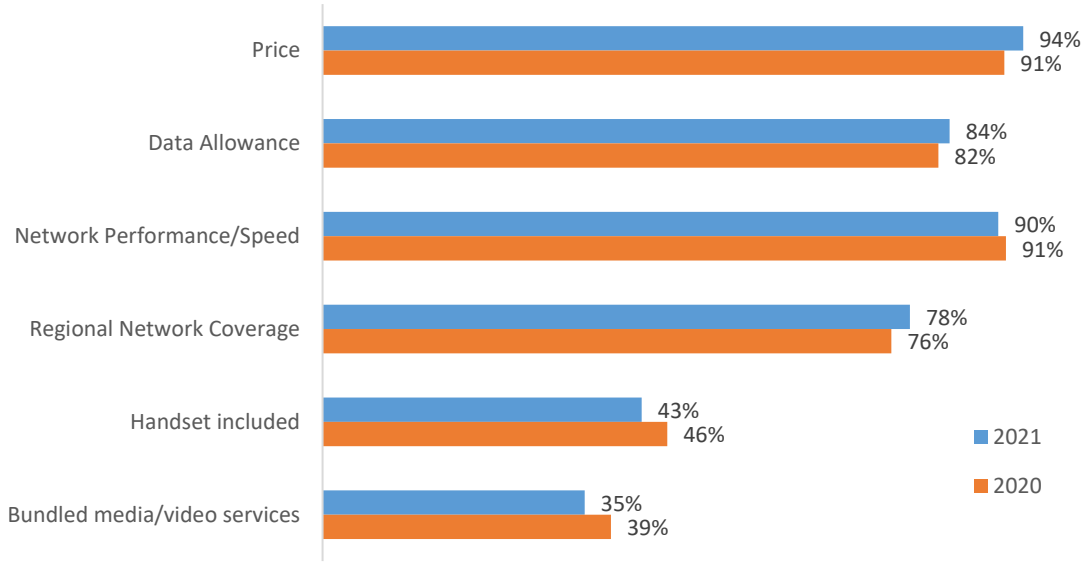


Figure 1. Percentage of survey respondents rating a factor between 4 and 5 on a scale of 1 (not important) – 5 (very important), when deciding their next mobile service purchase
SOURCE: Venture Insights Consumer Survey March 2021, n=1,019

Only 13% of the respondents expected to pay more for their mobile phone service each year. A majority expected to pay about the same, and 11% expected to pay less. These numbers did not shift significantly from our 2020 survey. This means that mobile service providers will find it difficult to lift ARPUs unless all operators lift them. An increase in prices by a service provider may trigger churn by the consumers who are reluctant to pay more for their services.

http://doi.org/10.18080/jtde.v9n2.422

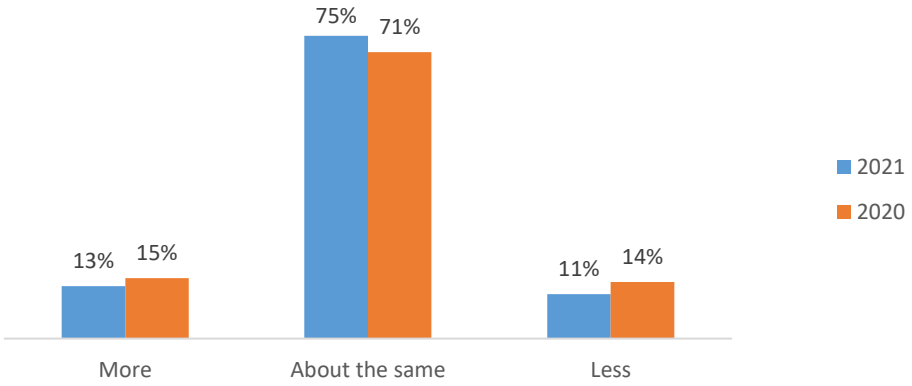


Figure 2. Survey question: In general, do you plan to pay more, less or about the same each year for your mobile phone service?
SOURCE: Venture Insights Consumer Survey March 2021, n=1,019

We also asked how likely respondents were to change their service providers and the reasons for this change. Overall, 38% were likely to change their mobile phone providers (12% within 1 year, 7% within 2 years, and 19% sometime).

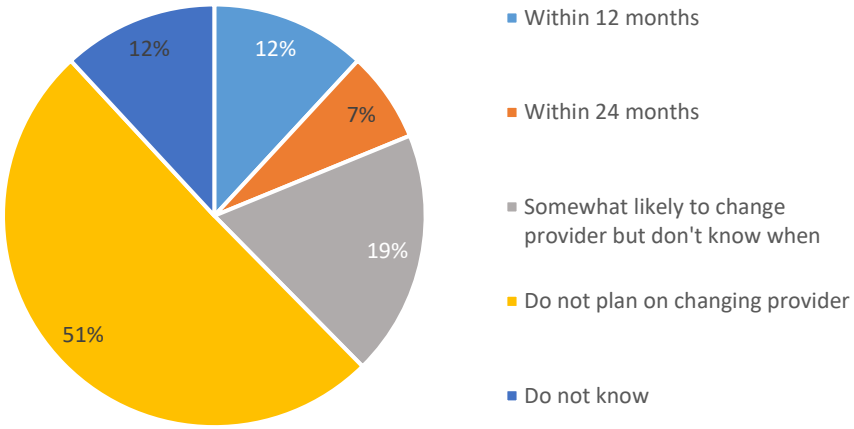


Figure 3. Survey question: How likely are you to switch mobile phone service providers?
SOURCE: Venture Insights Consumer Survey March 2021, n=1,019

These 38% of respondents were then asked to choose the main reason for switching their mobile service providers, and price was picked by 40% of these respondents. Data allowance was a distant second, which was picked by only 21% of these respondents. This again shows that price is a key driver of mobile service buying. It is also interesting that network performance and customer service were less likely to be top reasons for churn. This suggests that mobile consumers are more satisfied with MNO performance in these areas than with price and data allowances.

http://doi.org/10.18080/jtde.v9n2.422

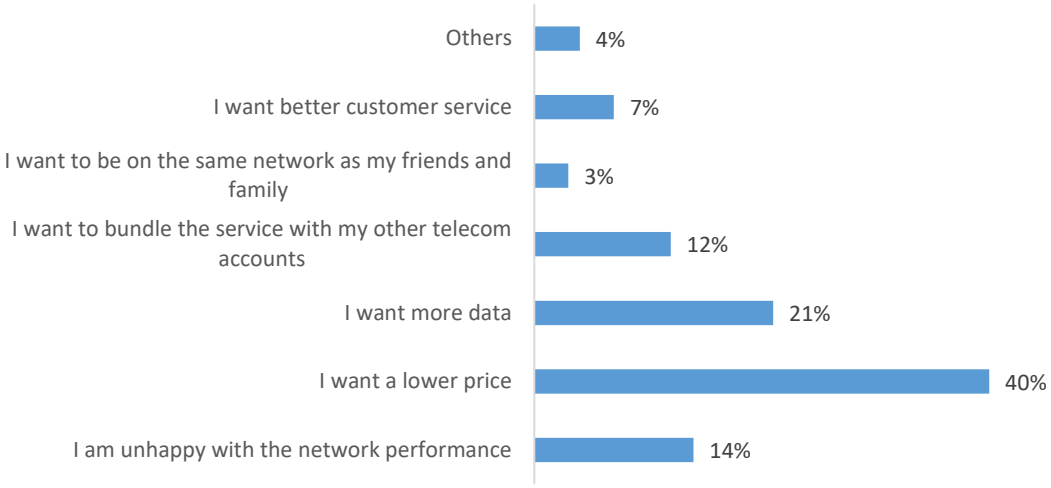


Figure 4. What is the main reason you are thinking about changing your mobile service provider?
SOURCE: Venture Insights Consumer Survey March 2021, n=383

Renewed Focus on MVNOs?

We start by emphasizing that the market share of MVNOs has largely remained unchanged (within the error margin) at around 22% since 2018, when Venture Insights started its annual consumer market surveys. In 2021, MVNO share rose 4% to 25%; this is outside the margin of error, but only slightly. In 2021, MVNOs had 27% and 20% share in metro and regional areas, respectively.

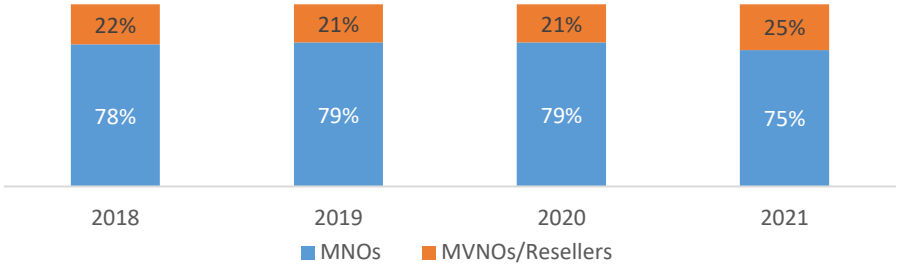


Figure 5. Market share of MVNOs in Venture Insights surveys
SOURCE: Venture Insights Consumer Survey 2018, 2019, 2020, 2021

Our view is that COVID-19 reinforced consumer interest in low-priced offers during the economic disruption of lockdown. Post-COVID-19, we are seeing higher consumer spending and high levels of consumer confidence. However, this does not seem to translate into the mobile market. As a result, we expect MVNOs to remain competitive as consumers remain reluctant to pay more for mobile.

For the 38% of respondents in Figure 3 who were planning on switching mobile phone service, we asked which service provider they were looking to switch to. Of these respondents, 35% were looking to switch to an MVNO. This is approximately one-and-a-half times the market share of MVNOs, suggesting an increased focus on them.

http://doi.org/10.18080/jtde.v9n2.422

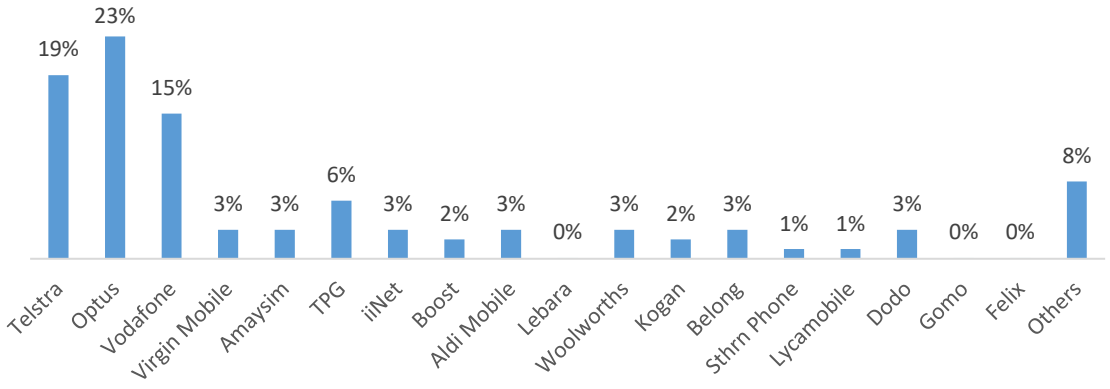


Figure 6. Survey question: Which mobile phone provider are you thinking about moving to?
SOURCE: Venture Insights Consumer Survey March 2021, n=383

We also looked at the potential churn of the consumers from a service provider: i.e., we split consumers by service provider. As can be seen in Figure 7 below, the percentage of respondents planning on churning out of MVNOs was generally lower than the MNOs. This is again consistent with the fact that consumers do not want to spend more on mobile services.

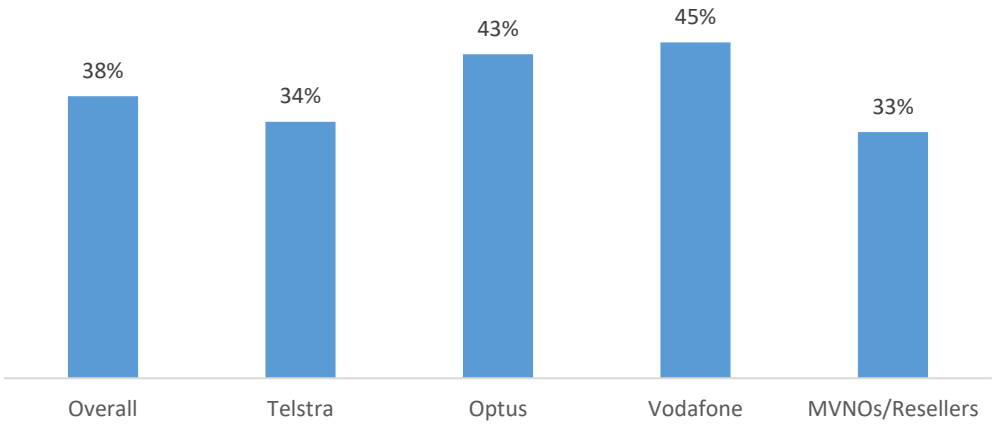


Figure 7. Percentage of current customers (in Figure 3) planning on churning by service providers
SOURCE: Venture Insights Consumer Survey March 2021, n=383

We also looked at which service providers consumers were looking to move to. For existing Telstra customers, 65% were looking to move to other MNOs and 28% to MVNOs. For Optus, 39% were looking to move to MVNOs, and this number was 38% for Vodafone. Of current MVNO customers, 45% were looking to switch to MNOs (Figure 8).

We used this potential churn data and the current market share of MVNOs to calculate the new market share for MVNOs, on the assumption that all these consumers go ahead with their planned churn. In this scenario, the total market share of MVNOs would increase to 31%, which is 6% more than the current market share of 25% as measured in this survey.

Of course, it does not follow that every respondent who indicated an intention to churn will in fact do so. The 31% is therefore a ceiling, not a forecast. In fact, consumer intentions were similar last year, but MVNO share seems to have risen only slightly. However, the survey data

http://doi.org/10.18080/jtde.v9n2.422

suggest that MNO defences against MVNOs are soft. The launch of sub-brands GoMo and Felix by Optus and TPG (Vodafone), respectively, which are the two MNOs most vulnerable to MVNO churn, should help them to capture some of these customers, but at a cost in ARPU. A full response should not involve just retail price cuts. We remain of the view that MNOs need to keep a close eye on mobile wholesale pricing to avoid undercutting themselves.

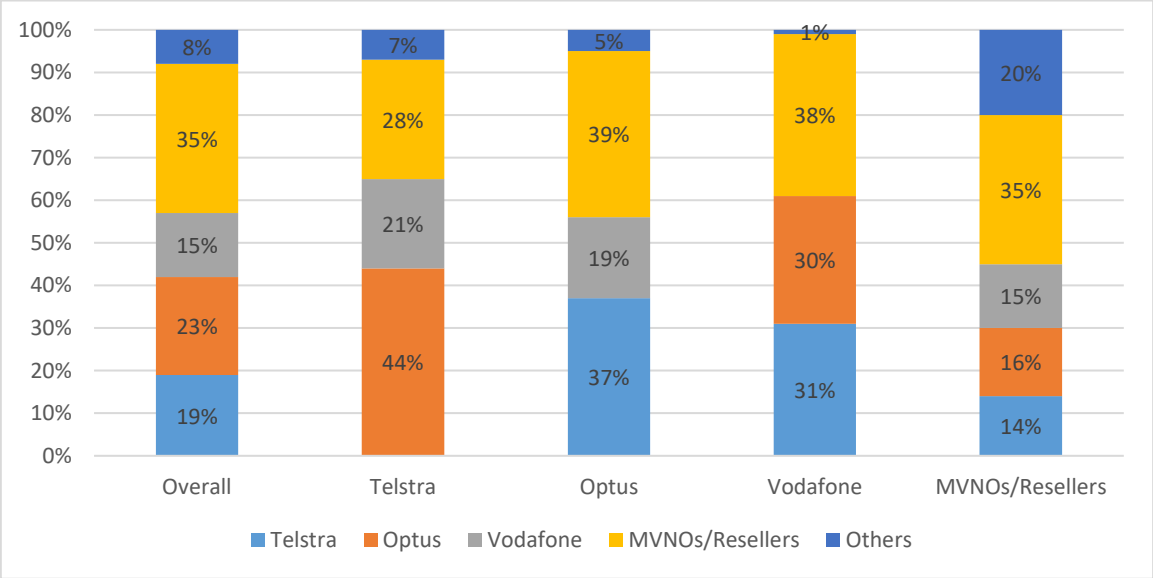


Figure 8. Survey question: Which mobile phone provider are you thinking about moving to (by current provider)?
SOURCE: Venture Insights Consumer Survey March 2021, n=383

What This Means for 5G Mobile Services

Above we noted that network performance/speed and price were the two biggest factors for consumers when deciding their next mobile service purchase. This suggests that there is an appetite for 5G services, but that consumers are reluctant to pay more for it.

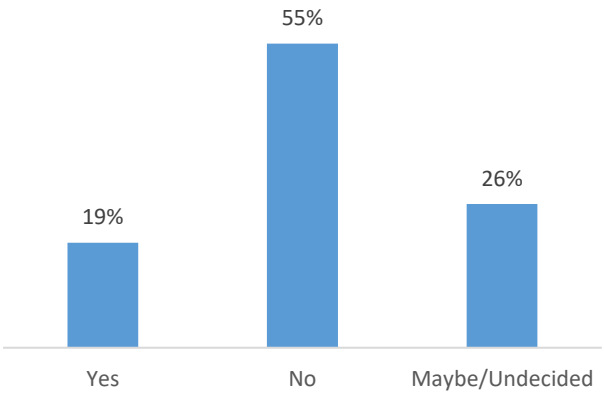


Figure 9. Survey question: Would you pay/Are you paying a premium for a 5G mobile phone service?
SOURCE: Venture Insights Consumer Survey March 2021, n=1,019

In our 2021 survey, only 19% of the respondents said they will be willing to pay more or are paying more for 5G mobile services (Figure 9). In this survey, 55% said they did not want to

http://doi.org/10.18080/jtde.v9n2.422

pay more, and 26% were unsure. These numbers are similar to our 2020 survey, indicating that willingness to pay a premium has not increased over the last year.

Preference for Bundled Services

While pricing is a major factor for consumers when choosing a mobile product, bundled services and diversified offerings offer another avenue for telcos to reduce churn. In Figure 1, we saw that 35% of respondents said bundled media/video services were important to them, and in Figure 4, 12% said they were planning to churn in order to bundle their mobile service with other telecom accounts.

In Figure 10 below, we asked the respondents if they would consider purchasing their mobile phone service from a utility company if bundled with their electricity or gas service, and about one-third of them said yes. Thus, bundling is attractive to a significant number of consumers, and it can help telcos gain more share of wallet and deepen their relationship with customers.

The interest in bundling drops with age. The percentage of respondents saying yes was approximately 40% for respondents younger than 34 years, and less than 20% for respondents above 55 years of age. There was no significant difference between metro and regional areas with respect to bundling.

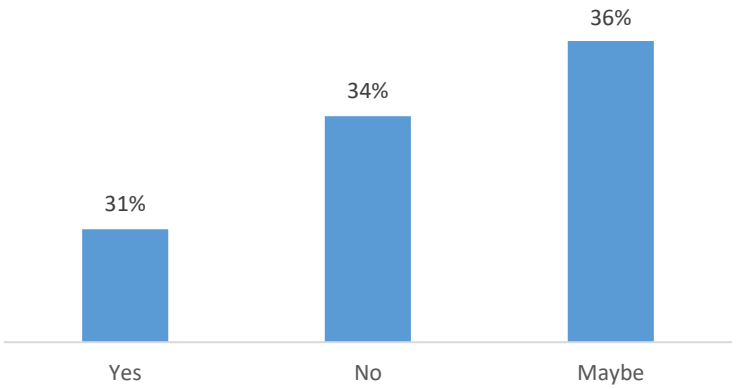


Figure 10. Survey question: Would you consider purchasing your mobile phone service from a utility company if bundled with your electricity or gas service?
SOURCE: Venture Insights Consumer Survey March 2021, n=1,019

Convergence with media is a popular offering by telcos, and we asked the survey respondents if they would change their mobile providers if another provider offered their favourite sports content bundled with their mobile plan. Of the respondents, 17% said yes, and another 22% said they may change their service provider for a bundled sports content. There was a difference between metro and regional areas too, and 19% said yes for metro areas and only 11% for regional areas. Further, there was a difference between MNO and MVNO customers. Of the MNO customers, 19% said yes, while only 13% of MVNO customers said yes.

http://doi.org/10.18080/jtde.v9n2.422

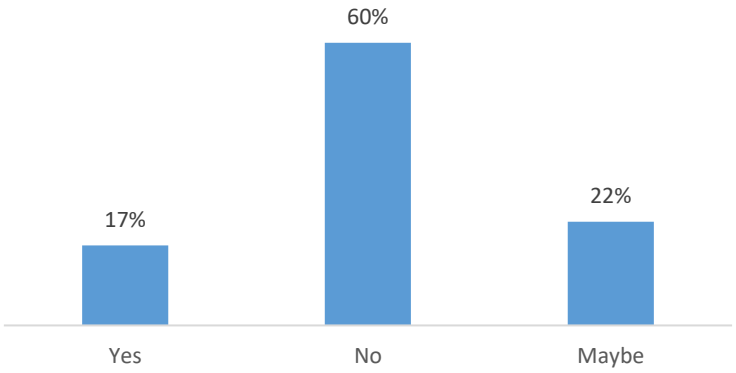


Figure 11. Survey question: Would you change telco mobile providers if another mobile operator offered your favourite sports content bundled with your mobile plan?
SOURCE: Venture Insights Consumer Survey March 2021, n=1,019

Overall, bundling is a strategy that is attractive to significant minorities of customers, but not for all. It is therefore an element in an overall churn reduction strategy, not a panacea.

Handset Purchase Preferences

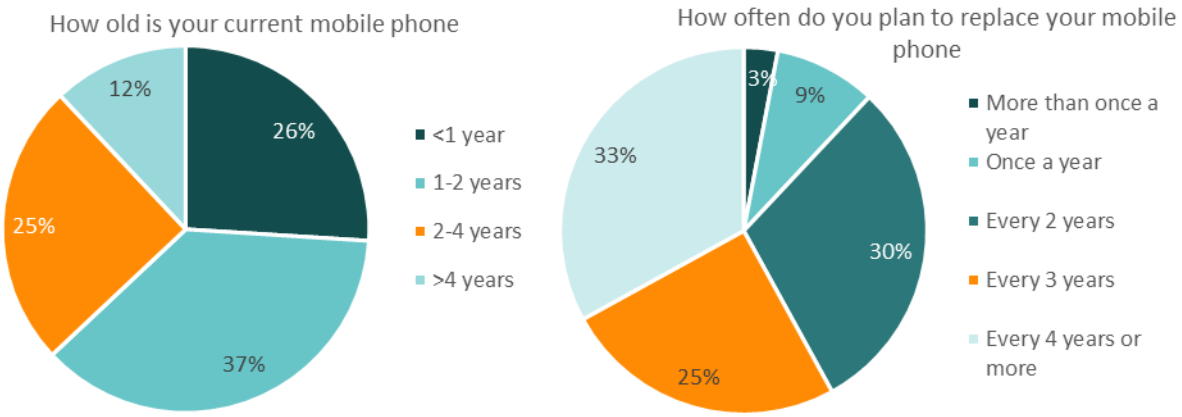


Figure 12. Survey question: How old is your current mobile phone (left) and how often do you plan to replace your mobile phone (right)?
SOURCE: Venture Insights Consumer Survey March 2021, n=1,019

We asked the respondents how old their current phones were and how likely they were to change their mobile phones. The survey showed that 26% had a phone less than one year old, 37% had phones between 1-2 years old, and 37% had phones more than two years old. Around 12% changed their phones at least once a year, 30% changed every two years, 25% changed every three years, and 33% changed after four years or more. Thus, a majority of consumers (55%) change their mobile phone every 2-3 years.

Of the respondents, 39% said they would consider purchasing a recycled/refurbished mobile phone at a lower price, but 35% said they will not consider it. This suggests that handset price is a consideration for a significant segment of consumers when considering their next mobile phone purchase.

http://doi.org/10.18080/jtde.v9n2.422

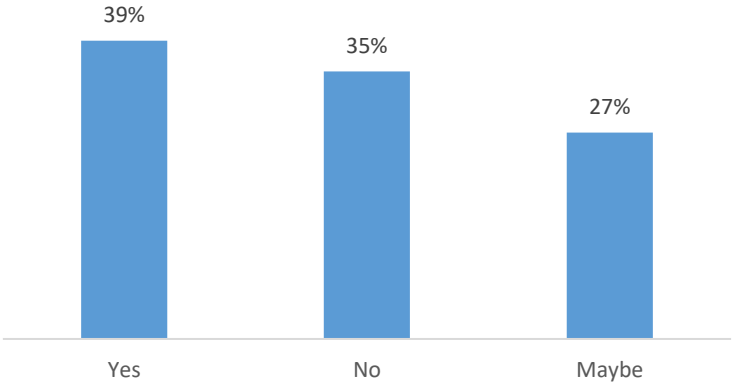


Figure 13. Survey question: Would you consider purchasing a recycled/refurbished mobile phone at a lower price than a new phone (assuming it had a warranty)?
SOURCE: Venture Insights Consumer Survey March 2021, n=1,019

Only 20% of the respondents were willing to pay more for their 5G mobile handsets; 55% did not want to pay more; and 25% were undecided. These numbers are virtually identical to the response of survey respondents regarding paying more on 5G services.

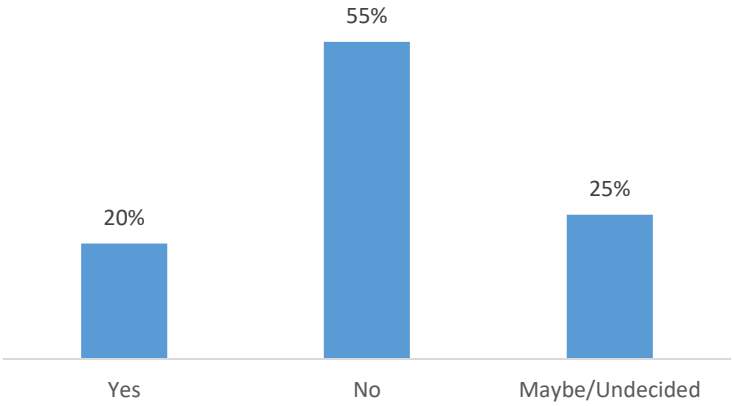


Figure 14. Survey question: Would you pay/Are you paying a premium for a 5G mobile handset/phone when available?
SOURCE: Venture Insights Consumer Survey March 2021, n=1,019

Conclusion

According to Venture Insights surveys, the market share of MVNOs has shifted only slightly in the last few years. However, price competition has placed downward pressure on mobile ARPUs. Our view is that the launch of sub-brands by all three MNOs will shore up MNO market share against MVNO pressure, but this will come at a cost in ARPU.

Bundled services, on the other hand, provide an avenue for the telcos to differentiate themselves, but this will only work in certain segments of customers.

There is an appetite for 5G and technology upgrades, but the consumers are getting conditioned to getting upgrades but not paying more. This has implications for return on investment in 5G going forward. While we see no alternative to a 5G rollout by all three MNOs,

http://doi.org/10.18080/jtde.v9n2.422

consumer reluctance to pay will have a material effect on the MNOs' financial capacity to improve 5G network performance over time.

On handsets, our survey also shows that a majority of consumers like to change their mobile phones every 2-3 years, and price is a consideration for a segment of consumers when purchasing their next mobile phone.

References

Venture Insights. (2020). *COVID-19 impact on mobile ARPUs, 5G adoption and MVNO wholesale prices*. Available at [payment] https://www.ventureinsights.com.au/product/covid-19-impact-on-mobile-arpus-5g-adoption-and-mvno-wholesale-prices/

http://doi.org/10.18080/jtde.v9n2.422

eLaunceston Revisited – A Novel Regional Research Project from 1999

Simon Moorhead
Ericsson Australia and New Zealand

Abstract: An historical paper from 1999 is republished because of its relevance to using digital communications to boost regional communities and their digital economies. Telstra Research Laboratories created a community website for Launceston Tasmania, with local stakeholder oversight, to test whether locally oriented information can increase the value of the Internet to existing users and make digital access more attractive to non-users.

Keywords: history, telecommunications, eLaunceston, Internet, social media

Introduction

This historic paper (Jenkins & Dragun, 1999) describes a social engineering project undertaken by the Telstra Research Laboratories (TRL), to test whether the use of a website focussed on the local community and local businesses would increase local use of the Internet.

Launceston in Tasmania was selected as a regional centre for the establishment of an Internet Portal. The TRL team worked at the grass-roots level with Launceston stakeholders to develop a project that not only met the expectations of Telstra but could make a substantial contribution to the local community.

The reader needs to be aware that, in 1999, access to the Internet in Australia was typically achieved via dial-up modems with maximum speeds of around 56 kbit/sec. In the eLaunceston project, Telstra offered subsidised ADSL connections with speeds around 100 times faster than dial-up.

This regional Portal provided an ideal environment to test the hypothesis that localised content and applications would stimulate greater Internet usage and take-up. A collaborative approach was adopted to identify community stakeholders and undertake workshops with these stakeholders.

Broader community consultation and focus groups were established to understand local Internet usage and identify wants and needs. Collaborative design workshops were then

http://doi.org/10.18080/jtde.v9n2.419

undertaken to convert those community needs and wants into Portal features and functionalities. Finally, the Portal was tested and deployed with further development and evaluation.

As the paper notes, the "project has generated significant interest both within Telstra and in the wider community" (p. 83) and the "consolidation of local information in one place within a Regional Portal has been noted as providing a valuable service to the community" (p. 83).

Reading the paper through a contemporary lens, one cannot help but notice the hints at the possibility of social media platforms, almost ten years before Facebook became the world's most popular social media web site.

Reference

Jenkins, A., & Dragun, N. (1999). eLaunceston – A Novel Regional Portal Research Project, *Telecommunication Journal of Australia*, *49*(2), 79-83.

http://doi.org/10.18080/jtde.v9n2.419

The Historic Paper

eLaunceston -

A Novel Regional Portal Research Project

Amanda Jenkins & Natasha Dragun, Telstra Research Laboratories

eLaunceston is a Telstra Research Laboratories project designed to test the hypothesis that locally-oriented information and services can increase the value of the Internet to existing users and make the Internet more attractive to non-Internet users. A Regional Portal provides an ideal environment to test this hypothesis and the eLaunceston Portal is being developed for this purpose. The project is novel because TRL is working at a grass roots level with Launceston stakeholders to develop a project that not only achieves Telstra objectives, but also has the potential to make a substantial contribution to the Launceston community.

Amanda Jenkins

Natasha Dragun

BACKGROUND

The Internet is a powerful tool that offers businesses, groups and individuals new ways to conduct their commercial and personal affairs. Telstra has made a significant investment in the Internet and it is clearly both in the public interest and in Telstra's interest for people to be able to exploit its enormous potential. There is a large proportion of people, however, for whom the Internet is not currently a meaningful or useful tool.

Telstra Research Laboratories (TRL) has the task of researching new social and technical trends that may impact Telstra, and has undertaken a project to examine the factors that influence Internet uptake and usage.

Research into the social factors impacting Internet uptake and usage has already been completed overseas. The preliminary results of this research has led us to believe that localised content and applications may increase the value of the Internet to existing users, and make it more attractive for people who are not currently using the Internet. TRL has designed a project to investigate this hypothesis in an Australian context.

Clearly we want to encourage people to go online, and this project gives Telstra the opportunity

Journal of Telecommunications and the Digital Economy, ISSN 2203-1693, Volume 9 Number 2 June 2021

http://doi.org/10.18080/jtde.v9n2.419

to explore ways of increasing the perceived value of the Internet. The primary objective of the project is to test whether localised content and applications motivate increased Internet usage. We also expect to learn about the range of other factors that influence Internet uptake and usage.

The intention is to grow the Internet business generally. Projects of this nature should ultimately benefit everyone in the Internet industry.

THE PROJECT

A regional 'portal' provides us with an ideal environment to test the hypothesis that localised content and applications increase Internet uptake and usage.

Our definition of a 'regional portal' is a Web site that attracts a high number of repeat users through:

- aggregating local content that is useful and desirable, and streamlining access to that content;
- supporting community building at macro and micro (community of interest) levels; and
- providing communication functionality and commerce services.

The Regional Portal that will provide the vehicle for this research project has been titled the *eLaunceston* Regional Portal. TRL staff are currently developing it in co-operation with the community of Launceston, Tasmania.

Launceston has characteristics that make it an ideal city to use as a base for the project. The main factors influencing the decision to select Launceston as the site for the project were the following:

- The Tasmanian Community Network process has energised the community around information technology and given the project fertile ground to work.
- Launceston City Council is innovative and was very receptive to this project concept.
- Launceston is large enough to provide the project with demographic diversity, but not so large that the project will be overwhelmed by other activities.
- There was strong support from Telstra staff based in Launceston for the project. The enthusiasm and commitment of local staff will be key to the success of the project particularly as TRL will be managing the project from Melbourne.

The *eLaunceston* project will involve:

- Existing products - the *eLaunceston* Regional Portal will include well-established functionality such as email and chat.
- Trialling of new products and services with the Launceston community - these products and services may be tested via the *eLaunceston* Regional Portal or they may be tested separately.
- (Perhaps) the generation of new product ideas
- Social and technical research.

A COLLABORATIVE APPROACH

Research conducted within a community should strive to contribute to the local region in ways that are desirable and useful. To ensure that the *eLaunceston* Regional Portal is developed to reflect and extend the needs and wants of the Launceston community, TRL invited local representatives to participate in the development and design of the Portal, and such collaboration will be encouraged for the duration of the project.

This interactive approach between TRL and the local community imposes some overhead costs on project management. However, the project will significantly benefit from the collaboration, as people are more likely to engage with something that they feel they some stake in. A regional portal is driven by content generated by the community and, in that sense, we are reliant on community input to make *eLaunceston* work in any case.

The process for involving the Launceston community in the *eLaunceston* project is multi-faceted, with a number of steps.

Step 1 - Introduction to Stakeholders

Initially key community stakeholders were briefed on the project concept and their ongoing participation in the development of the project was invited.

Step 2 - Workshopping with Stakeholders

A workshop was held with key stakeholders to flesh out the project concept and scope. The goals for this workshop were to:

- Develop a shared vision for the *eLaunceston* project and a shared understanding of the project scope; and
- Establish a Local Project Management Team for the project.

Two clear community goals were articulated during the Workshop:

- The Launceston community wants to increase understanding and use of the Internet for the economic and social benefit of the region.
- They want to use *eLaunceston* as another vehicle to promote the Launceston region nationally and internationally.

Journal of Telecommunications and the Digital Economy, ISSN 2203-1693, Volume 9 Number 2 June 2021

http://doi.org/10.18080/jtde.v9n2.419

It is important for the project to acknowledge these goals and, as much as is possible, to support their achievement. It was agreed that a useful and important part of the project would be a local Project Management Team, to:

- Provide a local perspective on the project, its role and impact on the community;
- Identify local community goals for the project
- Identify possible local community and management contributions to the project; and
- Provide guidance on involving other members of the community in the project.

The Local Project Management Team currently consists of representatives of:

- The Launceston City Council
- The Examiner newspaper
- Tasmanian Electronic Commerce Centre
- TAFE Tasmania
- Australian Maritime College
- University of Tasmania
- The Department of Education
- Tasmanian Community Network
- Launceston Chamber of Commerce
- Business North
- Northern Tasmania Division of General Practice
- Telstra Business Solutions

Step 3 - Community Consultation

Consultation was then expanded to cover a broader cross-section of the community. TRL goals were to:

- Identify and understand related projects (existing and planned)
- Identify and contact people and groups who might be impacted (positively and negatively) by the project
- Explore community needs, wants, concerns, and priorities.

Step 4 - Focus Groups

Focus Groups were conducted with randomly selected local Internet users to discuss:

- Activities currently undertaken within the Launceston community
- Interaction within Launceston community
- Trends in local Internet usage
- Launceston community needs and wants.

The goals associated with the focus groups were:

- To increase the project team's understanding of

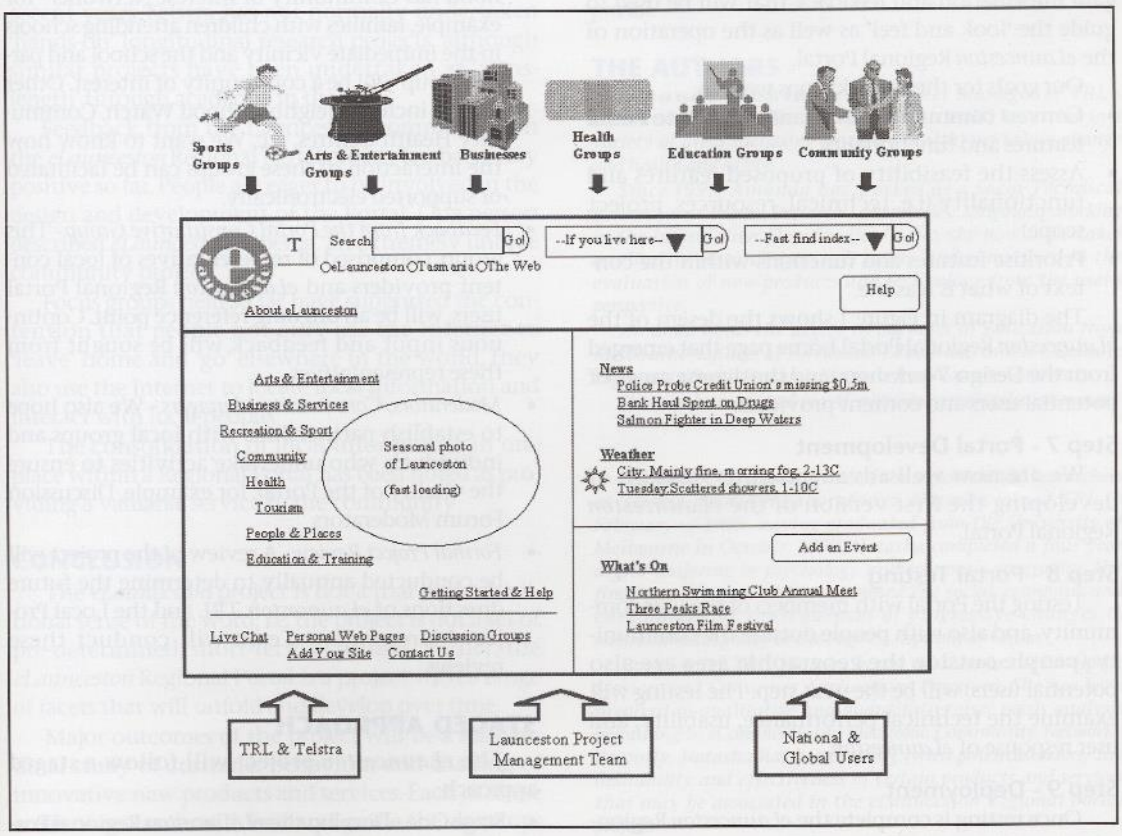


Fig. 1 - The Regional Portal Home Page

Journal of Telecommunications and the Digital Economy, ISSN 2203-1693, Volume 9 Number 2 June 2021

http://doi.org/10.18080/jtde.v9n2.419

the local context for the *eLaunceston* Regional Portal
- To identify the range of local information and services that are already online
- To get an indication of the services and activities that could be migrated to an online environment or that could be augmented by an electronic service.

Step 5 - Extended Community Consultation

Consultation with the Launceston community has been expanded to address issues raised in consultative forums. TRL is now working closely with representatives from the local IT industry to explore the ways in which *eLaunceston* may provide mutual benefit to TRL and the local IT industry. TRL are also in discussions with the Management Committee of the new public Internet access facility in Launceston, to consider the role of the facility within the *eLaunceston* project.

Step 6 - Collaborative Design Workshops

Collaborative Design Workshops were held with participants invited from key sectors, such as health, education and tourism, within the Launceston community. The aim of the Design Workshops was to gain information and feedback that will be used to guide the 'look and feel' as well as the operation of the *eLaunceston* Regional Portal.

Our goals for these workshops were to:
- Convert community needs and wants into Portal features and functionality
- Assess the feasibility of proposed features and functionality (i.e. technical, resources, project scope)
- Prioritise features and functions within the context of what is feasible.

The diagram in Figure 1 shows the design of the *eLaunceston* Regional Portal home page that emerged from the Design Workshops and the diverse range of potential users and content providers.

Step 7 - Portal Development

We are now well advanced in the process of developing the first version of the *eLaunceston* Regional Portal.

Step 8 - Portal Testing

Testing the Portal with members of the user community, and also with people outside the community (people outside the geographic area are also potential users) will be the next step. The testing will examine the technical performance, usability, and user response of *eLaunceston*.

Step 9 - Deployment

Once testing is complete the *eLaunceston* Regional Portal will then be deployed.

Step 10 - Ongoing Development and Evaluation

Development and evaluation of the *eLaunceston* Regional Portal will be an ongoing feature of the project to ensure that content and applications remain useful and desirable to users. We expect that the *eLaunceston* Regional Portal will evolve throughout the course of the project.

The evaluation of the Portal will include:
- *Feedback received via the Portal Site* - feedback forms will be available via the Portal site.
- *Server statistics* - popular pages, number of users, etc.
- *In-depth research* - (eg interviews, focus groups, and questionnaires) with a sample of the Launceston community: approximately 200 households and 10-15 small businesses. This sample, comprising existing Internet users and non-Internet users, will be our Research Reference Group.

  We plan to recruit the households from a particular area within Launceston. We are seeking people within neighbourhood proximity because one of the topics of interest for the project is Community of Interest Networks. Every neighbourhood has Community of Interest Networks - for example, families with children attending schools in the immediate vicinity and the school and parent group will be a community of interest. Other groups include Neighbourhood Watch, Community Health Centres, etc. We want to know how the interaction of these groups can be facilitated or supported electronically.
- *Feedback from the Portal Consultative Group* - This group, comprised of representatives of local content providers and *eLaunceston* Regional Portal users, will be an ongoing reference point. Continuous input and feedback will be sought from these representatives.
- *Moderators/Community Managers* - We also hope to establish partnerships with local groups and individuals who undertake activities to ensure the vitality of the Portal, for example, Discussion Forum Moderators.
- *Formal Project Review* - A review of the project will be conducted annually to determine the future directions of *eLaunceston*. TRL and the Local Project Management Team will conduct these reviews.

STAGED APPROACH

The *eLaunceston* project will follow a staged approach:
- Stage One - Develop the *eLaunceston* Regional Portal

http://doi.org/10.18080/jtde.v9n2.419

The goal of stage one will be to enhance access to locally oriented Web content. We shall deploy advanced searching tools and directories to facilitate the users' access to this content.

- Stage Two - Support the community.
  In this stage, we shall add the functionality that will give the Launceston community additional communication mechanisms. For example, email, chat and bulletin boards will be features of the *eLaunceston* Regional Portal. These features will enhance communication within the Launceston community.
- Stage Three - Create a supportive online environment for businesses.
  The focus of this stage will be on e-Business applications.

It is possible that the *eLaunceston* project will be greatly expanded by a proposed Telstra and Federal Government initiative to develop a Telstra Multimedia Development Laboratory in Launceston. The *eLaunceston* project will be folded into this initiative.

INSIGHTS FROM THE PROJECT

This project has generated significant interest both within Telstra and in the wider community. In recent years Telstra has not normally undertaken 'hands-on' longitudinal research projects, although similar projects have been undertaken at 'arms-length' through academia in the past.

Feedback from the Launceston community on the *eLaunceston* Regional Portal project has been very positive so far. People are eager to be involved in the design and development of the Portal. One person described *eLaunceston* as being 'an extremely unique community project'.

Focus groups held so far have supported the contention that people not only use the Internet to 'leave' home and 'go' elsewhere in the world, they also use the Internet to locate local information and interact with local people.

The consolidation of local information in one place within a Regional Portal has been noted as providing a valuable service to the community

CONCLUSION

The *eLaunceston* project is not a trial in the traditional sense of the word; i.e. the project is not a set of pre-determined, short-term activities. Rather, the *eLaunceston* Regional Portal is a project with a range of facets that will unfold and develop over time.

Major outcomes of the project will be a longitudinal study of customer behaviour and trialling of innovative new products and services. Each of these areas of research will feed and guide the development of other areas. This convergence of inquiry and evaluation over an extended period of time is what makes *eLaunceston* such a novel research project.

Not only is the project novel within contemporary spheres of Australian Internet research, but the role of TRL within the project represents an innovative departure from tradition. TRL, with other Telstra stakeholders, will work at a grass roots level with the Launceston community over a period of years. We will not be trialling a single, specific piece of technology and then withdrawing. Instead we will be building a strong relationship with a community through a project which recognises both Telstra and Launceston goals, and which involves social and technical research and commercial relationships which will be of benefit in the present and in the future. The research will not only address lifestyle and technology, but also the usefulness and usability of specific technologies.

The key message of this project proposal is one of collaboration and co-operation.

Whilst *eLaunceston* is still very much a work-in-progress, we believe the *eLaunceston* project can be a model for projects that involve the community. We also expect that *eLaunceston* can provide important insights into the value and viability of the regional portal.

THE AUTHORS

Amanda Jenkins *is the Project Manager of TRL's eLaunceston project. She has worked as a social researcher in a variety of areas including women's health, workplace change and health and safety.*

Since 1993, Amanda has worked as a Socio-Technical Researcher at Telstra Research Laboratories. Originally working in the Information Flow Studies Group, she now undertakes qualitative research into user needs, and is involved in the evaluation of new products and technology from the user's perspective.

Amanda holds the degree of Bachelor of Education from Melbourne College of Advanced Education, and a Graduate Diploma in Social Research Methods from Latrobe University.

She may be contacted via AJenkins@vtrlmel1.telecom.com.au

Natasha Dragun *is one of the sociotechnical researchers at Telstra Research Laboratories. Natasha joined TRL in February of 1999, having graduated from the University of Melbourne in October, 1998. Natasha completed a four year degree majoring in psychology and economic geography. Her final year Honours thesis examined the social, economic and environmental consequences of progressive changes to environmental policy in the People's Republic of China.*

Upon joining TRL, Natasha began work across the Enterprise Services and Consumer Applications Programs. She has been involved in qualitative and quantitative user needs analysis pertaining to eCommerce and Electronic Community Networks. Recently, Natasha has been testing (with potential users) the desirability and effectiveness of certain products and services that may be associated in the eLaunceston Regional Portal project.

She may be contacted via NDragun@vtrlmel1.telecom.com.au

Journal of Telecommunications and the Digital Economy, ISSN 2203-1693, Volume 9 Number 2 June 2021

http://doi.org/10.18080/jtde.v9n2.419