RACING TO THE FUTURE: SECURITY IN THE GIGABIT RACE?

Mark A Gregory[1] and Lucy Cradduck[2]
[1]RMIT University, Melbourne, Australia
[2]Queensland University of Technology, Brisbane, Australia

ABSTRACT

This research seeks to identify the differing national perspectives towards security and the 'gigabit race' as those nations transition to their next generation broadband networks. Its aim is to critically appraise the rationales for their existing digital security frameworks in order to determine whether (and what) Australia can learn from the alternative legislative and regulatory frameworks implemented by key nations and trading blocks. This paper provides an outline of the research motivation and direction. The research will fill major knowledge gaps about the motivation, rationale, legal and social implementation, and impacts on security for next generation broadband networks and will inform the development of digital security and communications policies.

KEYWORDS

Telecommunications regulation, cyber security, public policy, privacy, NBN

1. INTRODUCTION

Investment by government, industry and business in broadband networks and digital systems has been increasing consistently. Attempts to protect digital security can be seen in a variety of jurisdictions. The effectiveness those measures in practice will depend on the specific jurisdiction and its method of regulation (Lodder, 2013). The rapid and radical transformation of society’s participation in the digital era (Cradduck, 2015) has led to efforts by the Australian federal government to legislate for improved digital security while seeking to facilitate investment in next generation telecommunication networks. However, as Guadamuz (2011) observed “[n]ational laws tend to treat the subject of cybercrime by a combination of the application of old norms and the enactment of new legislation” (p.179). An understanding of the relationship between public policy, legislation, regulation and technical outcomes has failed to keep pace with the rapid changes to global telecommunication markets and governments’ responses to technological changes during the ‘gigabit race’. The significant advances driving the development of digital networks, in Australia and globally, have resulted in the need for improved digital security and telecommunications capabilities (Gregory & Glance, 2013). Stakeholders have a variety of perspectives as to how to achieve the inter-related outcomes necessary for success to be achieved, however, it is often far from certain whether any success in fact was achieved (Gregory, 2014). Decisions affecting digital security and telecommunications infrastructure provision based on technical, legal and or investment criteria can be identified. Absent from the literature, however, is an evaluation of the inter-relationship between digital security, consumer protection and provider satisfaction.

This research investigates the different perspectives for security in the 'gigabit race' as nations transition to next generation broadband networks. Data collection and modeling of the major knowledge gaps has required studying the linkages between motivation, rationale, legal and social implementation and impacts of security for next generation broadband networks; and the development of communications policies. The research project has commenced and initial work into the development of a data structure and model is presented in the paper. The paper concludes by identifying matters requiring further consideration.

2. RESEARCH CONTEXT

The Seoul Declaration for the Future of the Internet Economy 2008 provided its signatories (including Australia) would “promote ubiquitous access to ICT networks and services enabling widespread participation in the Internet Economy”. However, the resulting increased ease of access to the internet brought with it increased risks of breaches of security and privacy (Cradduck & McCullagh, 2007). Importantly, an individual’s perception of their level of security and privacy when engaging on the internet influences their desire to engage (Cradduck, 2015). Therefore, if those perceptions are negative, this will impact negatively upon Australia’s place in the ‘gigabit race’. As Cutler (2008) identified a “lack of user trust in the security of the transactions” will act as inhibitor of e-Commerce (Cutler 2008, 62). In order to encourage participation, and ensure Australia’s position in the gigabit race, issues of reliability of access and security must be addressed (OECD, 2013). It is for this and similar reasons that digital security and privacy concerns receive international attention (OECD, 2013a; Ponemon Institute, 2011).

As Kee et al. (2011) observed “where the conduct to be regulated or the product to be protected will have an impact on the international stage, it … requires collective policy making” (Kee et al. 2011, 175). As the global digital network is a combination of the many national networks decisions made in one jurisdiction regarding digital security and telecommunications functionality will affect other jurisdictions. This is particularly relevant to issues of security due to the transnational nature of cybercrimes (Guadamuz, 2011). This means that, in order for Australia to affect a smooth transition to its next generation networks, there is a need to study the different jurisdictional perspectives and approaches being utilised to legislate and implement digital security. Significantly whether, and what, Australia can learn from the legislative and regulatory frameworks implemented by key nations and trading partners to support their various digital security policies during the ‘gigabit race’ has yet to be critically examined.

3. AIM AND METHODOLOGY

This research aims to contribute to the public policy and national security discourse in two significant ways. First, by examining the motivations for security and broadband related legislation internationally it will create a single source of empirical data that can made available as a resource for use by other researchers. Second, by undertaking a comparison between the collated data and the Australia position it will identify how the approaches to security can be used appropriately to influence investment in infrastructure.

The research methodology consists of three interrelated and concurrent research strands – 1. policy and technology; 2. policy, legislative and regulatory; and 3. theoretical, policy, legal and technical model generation. These will be used to address issues arising from the identified empirical and theoretical knowledge gaps. These strands draw on the linkages between the data items shown in Table 1, an understanding of the history that led to the legislative, regulatory, technical and competitive landscapes.

Table 1. Data Items and Categories

Item	Category	Item	Category
Telecommunications Act	Legislation	Privacy Regulator	Regulation
Companies Act	Legislation	Competition Regulator	Regulation
Consumer Protection Act	Legislation	Telecommunications Ombudsman	Regulation
Competition Act	Legislation	Industry Technical Regulator	Regulation
Data Breach Notification Act	Legislation	Telecommunications Department	Government
Privacy Act	Legislation	Consumer Advocate	Industry funded
Trade Practices Act	Legislation	Universal Service	Industry funded
		Industry Peak Body	Industry funded

The *policy and technology* research strand will undertake a review of public policy decisions, related technical outcomes and field research. In this way the authors will develop an understanding of why different approaches have been adopted in the targeted nations and trading blocks for digital security and telecommunications during the ‘gigabit race’.

The disparate global policy, legislative and regulatory digital security and telecommunications environments have resulted in a range of affects that require investigation, or to identify best practice, in the formation of government policies, legislation and regulations. The *policy, legislative and regulatory* research strand will engage the authors in extensive field research. This will include interviews and surveys in order to determine governance, international relationships, innovations and political motivations. Drawing on Australian and international data gathered during the research project, the authors will contribute to theoretical and applied knowledge in this area. In the *theoretical, policy, legal and technical model generation* research strand, the authors will develop new theoretical, policy and technical evaluative models which can be used to guide an understanding of the broader implications and motivations resulting in different global approaches to digital security and telecommunications in the 'gigabit race'.

3.1 Limitations

The authors acknowledge a significant research constraint regarding available data and information. Information regarding national digital security strategies is fragmented and often not publically available. The limited availability of such information results in a constrained view of digital security and telecommunications and impedes upon any researchers' ability to accurately identify related themes.

4. DISCUSSION

A consideration of the available literature identifies two knowledge gaps. The first gap is empirical as currently there is no single reference source available that provides an overview, or in-depth case study, of the global perspectives of digital security and telecommunications. This renders an assessment of the benefits or otherwise of the effectiveness of various approach/es to digital security and telecommunications during the 'gigabit race' more difficult to achieve. Available information about national digital security strategies also is fragmented and there is a lack of a cohesive structure regarding domestic laws. An impact is that stakeholders cannot readily identify best practices, nor measure how legislation will affect digital security and telecommunications or whether there will be any associated affect on consumer and business confidence. The second gap is theoretical. In policy terms is there a conceptual framework that ties together the different aspects of providing digital security and telecommunications. However, the theoretical model will need to provide the basis for an analysis on the effectiveness of legislation and technology change. It also will need to be able to be use to identify what is being affected or being missed as a result of current policy decision-making processes. To investigate the theoretical knowledge gap it will be necessary to conceptualize the provision of digital security and telecommunications as a disruption to, rather than an extension of, existing systems and infrastructure. In this way it will be possible to critically examine arguments that policy, legislation and technology can bring together the right mix to achieve improved outcomes (Kee et al., 2011).

Politics has a significant role in domestic policies (Reed, 2012). As such, the development of international policy into appropriate domestic laws is not straightforward and can be exacerbated by the political divide in many countries (Gulati & Yates, 2012). This is perhaps more clearly seen in those jurisdictions where the process of creating legislation is a competitive, rather than collaborative, process as the sides seek to best position their own interests (Inoue, 2007). There is a need therefore for any domestic laws and policies to "address the tension that exists between the efficiency benefits for a uniform global policy and the variation in national and regional tastes for different politics" (Metcalf & Weisbach, 2012, 110). Also important is the need to ensure the ability of policy and law to develop as easily as society does. Internationally, divergent domestic government policies, and often changes of government, mean that at any given time one jurisdiction can view the need for regulation of the same activity in numerous, and potentially inconsistent ways (De Vos, 2010). This affects the existence, and content, of policy and related legislation (Dutton & Blank, 2011). Issues of digital security, privacy and confidentiality of information, remain inextricably linked (Swink, 2001). Mechanisms to encourage individual's participation absent overcoming any lack of individual digital skills (EC, 2015) merely increase concerns for both digital security and privacy generally. For the immediate future as well as beyond there are a variety of matters that policy makers need to consider and act upon. In particular cybersecurity for countries, as well as security issues for businesses and individuals will become more essential (OECD, 2013a). Importantly considerations of what is appropriate regulation is linked with what are appropriate enforcement powers and what is the necessary level of funding required in order to enable those powers to be effectively used (OECD, 2013).

5. CONCLUSION

The global nature of digital security and telecommunications warrants investigation of the various alternate approaches and the development of a model that provides a framework for understanding the inter-related public policy, legislation and technology solutions. The existing provision of digital security and telecommunications during the 'gigabit race' is a significant investment with rationales currently grounded in the public good, notions of fairness and market failure in terms of access to an essential resource. However, while these rationales may be justified in terms of promoting market competition, it is the authors' contention that, currently, there is no effective measure for global or Australian outcomes and as such these rationales may not fully capture the intent of the legislation or technical solutions being implemented.

By clarifying these problems, this research is the start of the first in-depth study of global perspectives on digital security and telecommunications focused on public policy, legislation and technology. This research is on the cusp of public policy, crime policy and computer communication network research as the authors by theorising the digital security and the 'gigabit race' as a form of constrained digital security focus on the impacts to Australian and global infrastructure. The research will significantly expand the current literature, as well it will create a new evidence base, which may be accessed by other researchers.

REFERENCES

Cradduck, L., and McCullagh, A. 2007. Identifying the identity thief: is it time for a (smart) Australia Card? *International Journal of Law and Information Technology*, Vol.16, No.2, pp. 1-34.

Cradduck, L. 2015. *Individuals, Innovation and the Internet: Why access is essential*. Common Ground Publishing, Champaign, IL, USA.

Cutler, T., 2008. *Venturous Australia – Building Strength in Innovation*. North Melbourne: Cutler & Company Pty Ltd.

De Vos, S., 2010. The Google-NSA Alliance: Developing Cybersecurity Policy at Internet Speed, *Fordham Intellectual Property Media and Entertainment Law Journal*, Vol. 21, pp.173-227.

Dutton, W., and Blank, G., 2011. Next generation users: The Internet in Britain. *Oxford Internet Survey 2011 Report*. Oxford: Oxford Internet Institute, University of Oxford, UK.

European Commission ('EC'), 2015. The Digital Economy and Society Index.

Gregory, M. and Glance, D., 2013. *Security and the Networked Society*, Springer, New York, USA.

Gregory, M., 2014. From leader to follower: Running the gigabit broadband race, *Business Spectator*, News Limited, 29 April 2014.

Guadamuz, A., 2011. *Networks, Complexity and Internet Regulation: Scale-Free Law*. Edward Elgar, Cheltenham, UK.

Gulati, G. and Yates, D., 2012. Different paths to universal access: The impact of policy and regulation on broadband diffusion in the developed and developing worlds. *Telecommunications Policy*, Vol.36, pp.749-761.

Inoue, T., 2007. 'The Rule of Law as the Law of Legislation' in L. Wintgens (Ed) *Legislation in Context: Essays in Legisprudence*. Ashgate Publishing Ltd, Aldershot, UK.

Kee, K., et al. 2011. Cyberinfrastructure inside out: Definition and influences shaping its emergence, development, and implementation in the early 21st century. *In Nexus: New Intersections in Internet Research*, D. Araya, Y. Breindl, and T. J. Houghton (Eds.), Peter Lang, New York, USA, pp.157-189.

Lodder, A., 2013. Ten Commandments of Internet Law revisited: Basic principles for Internet Lawyers, *Information and Communications Technology Law*, Vol. 22, No.3, pp.264-276.

Metcalf, G., and Weisbach, D., 2011. Linking Policies When Tasters Differ: Global Climate Policy in a Heterogeneous World, *Review for Environmental Economics and Policy*, Vol. 6, No.1, pp.110-129.

Organisation for Economic Co-operation and Development ('OECD'), 2013. Review of the Seoul Declaration for the Future of the Internet Economy: Synthesis Report. *OECD Digital Economy Papers*, No. 225. OECD Publishing.

Organisation for Economic Co-operation and Development (OECD'), 2013a. Broadband Networks and Open Access. *OECD Digital Economy Papers*, No. 218. OECD Publishing.

Ponemon Institute, 2011. The Security of Cloud Infrastructure: Survey of U.S. IT and Compliance Practitioners, Ponemon Institute LLC, Research Report, November 2011,

Reed, C., 2012. *Making Laws for Cyberspace*, Oxford University Press, Oxford, UK.

Swink, D., 2001. Telecommuter Law: A New Frontier in Legal Liability, *American Business Law Journal*, Vol.38, No.4, pp.857-900.