FOREWORD

ROGER CLARKE*

I INTRODUCTION

The law is of course an object worthy of study for its own sake. My role in UNSW Law is unusual, however. As a consultant, as a researcher into strategic and policy impacts and implications of information technologies, and as a public interest advocate, my interest in the law relates to the extent to which it does and does not provide a reliable, understandable and balanced framework for the lives and livelihoods of people and organisations. In this Foreword, I outline some key concerns that an instrumentalist such as myself brings to the topic of 'Cyberspace and the Law'. I have not grounded my comments in the literature, but I have taken the liberty of indicating some of my own materials that provide greater detail on those concerns.

The preliminary discussion considers first the principle, or perhaps mantra, of 'technology neutrality'. It then reviews experiences that have led me to have serious doubts about the levels of understanding of information technologies achieved during court proceedings. Consideration of current and emergent information technologies suggests that the complexities of future issues will be well beyond the capacity of courts. I then review the articles in this thematic Issue, paying particular attention to how they throw light on my concerns.

II TECHNOLOGY NEUTRALITY AND CYBERSPACE

The term 'technology neutrality' has been widely discussed as a principle underlying the drafting of laws. The expression implies that a requirement

* Roger Clarke is Principal of Xamax Consultancy Pty Ltd, Canberra. He is also a Visiting Professor in Cyberspace Law & Policy at the University of New South Wales, and a Visiting Professor in the Research School of Computer Science at the Australian National University. Valuable comments were received from David Lindsay (Monash University), Dan Svantesson (Bond University), Lyria Bennett Moses, Ross Buckley, Graham Greenleaf and Kayleen Manwaring (UNSW Law), John Selby (Macquarie University), Louis de Koker (La Trobe University), Nicolas Suzor (Queensland University of Technology) and Lee Bygrave (University of Oslo). Needless to say, all opinions, and all aspects that any reader regards as problematic, are my responsibility alone.

'operates effectively and fairly in different technological contexts',[1] including in respect of foreseeable and preferably even unforeseeable future technologies.

To what extent is technology neutrality a laudable principle? There are clearly benefits in expressing requirements functionally rather than procedurally. Unnecessarily technology-specific expression can result in accidental advantages and disadvantages for particular technologies, can stifle innovation, and can shorten the life of regulatory measures and render them ineffective and even harmful during the later parts of their life span. Australia is afflicted with parliaments in which excessive attention to party politics greatly reduces the time spent on un-newsworthy proposals for adaptations to laws. Meanwhile, the climate of politicians' hostility to the judiciary limits the scope for case law to deliver refinements and protections to existing laws. An attraction of the technology neutrality principle is that it might help address the problem of the glacial pace of law reform.

On the other hand, to what extent is technology neutrality an unachievable aspiration? And does it create the risk of encouraging expressions that are excessively inclusive and/or insufficiently specific? Broad requirements can be expressed for any undertaking that is, say, 'large' and/or 'intrinsically dangerous'. On the other hand, chemical factories give rise to many different kinds of risk, and so do extractive industry operations, and so do power plants. To achieve safety at Windscale, Three Mile Island, Chernobyl and Fukushima, the need was for the formulation of 'technology-specific' rather than 'technology-neutral' requirements. Any broad, functional statement would have been either too vague and ineffective to cope with the particular and very substantial risks of nuclear power, or an unjustifiable and unaffordable imposition on other forms of past, present and future power generation, let alone on extractive and manufacturing undertakings. Hence the suitability of the technology neutrality principle is likely to be highly dependent on the scope of the domain to which a requirement is to be applied.

Another topical example of a challenge to technology neutrality is the need for noise control for motor vehicles. That is far from a new idea. However, the preoccupation in the past was with controlling excessively loud noise. For example, rule 291 of the *Australian Road Rules* requires that vehicles do not emit 'unnecessary noise'.[2] Our current world includes electric cars (pun intended). This has given rise to an additional, safety-oriented need for the establishment of a minimum noise-level, to provide warning to pedestrians of the presence of a vehicle. It would have required an extraordinarily broad and flexible mind to have drafted a requirement that was sufficiently technologically neutral to encompass this current need.

Perhaps we need a meta-principle along the lines of 'choose an appropriate scope for technology-neutral requirements statements, and declare it'. How might such a meta-principle be applied to information technologies in general, and

---

1 Lyria Bennett Moses, 'Recurring Dilemmas: The Law's Race to Keep Up with Technological Change' [2007] *University of Illinois Journal of Law, Technology & Policy* 239, 239.

2 *National Transport Commission (Road Transport Legislation – Australian Road Rules) Regulations 2006* (Cth) sch 1 ('*Australian Road Rules*') r 291.

more specifically to the internetworked information technology-complexes that give rise to 'cyberspace'? And would it help?

III UNDERSTANDING OF COMPUTING IN THE COURT SYSTEM

Further questions that concern me are how much understanding exists of features of IT and of the cyberspace behaviours that they enable, and whether a lack of understanding matters. The discussion in this and the following sections has as its focus the understanding achieved during court proceedings, which of course depends on the specifics of the matter, and on the information placed before the court by the parties.

Being a non-lawyer, my first significant exposure to the vagaries of court processes and judgments was in my early 30s, in a key 1980s software copyright case. In 'the case of the Wombat ROMs' (*Apple v Computer Edge*[3]), the court needed to rule on perhaps the simplest of all challenges in the information technology arena – whether copyright subsisted in a program written in a low-level language and/or in the machine-executable code generated from it. During public discussions about an appropriate response to the decision at first instance in 1983, I endeavoured (without success) to represent the interests of the software industry. I subsequently examined the succession of seven judgments by nine judges during the three phases from the Federal Court to the High Court.[4] In relation to the key question as to whether the assembly-language source-code was a literary work, many misunderstandings were evident in the texts. One of them was particularly relevant:

> Gibbs [J] considered Condition A fulfilled since the source programs 'afford instruction to the operator' (p. 7). Deane [J] disallowed Conditions C, E and F because 'source code consisted essentially of instructions … to be read and followed by a human reader … [and] … [the programmed ROM] resulted from the following of the directions of [the source code]' …
>
> [But] [w]ritten source-code is not a set of directions; not to a computer, and certainly not to a human. Although a suitably trained human can infer from it what the effect of the resulting machine-executable program will be, the written source code is merely a set of symbols punctuated by line-feeds. When read, as inanimate data, by a suitably programmed translator [program], the source code will result in machine-executable code which does have the ability to direct a machine's actions. *However, there is no sense in which such a language directs any human's actions.* In view of the fact that the same remarkable misunderstanding occurs in two judgments, the inescapable conclusion is that counsel were at fault. Denied their premise, Gibbs and Deane [JJ] may well have reached their conclusions by other routes. None the less, the actual reasoning in their judgments is undermined by the error.[5]

---

3 *Apple Computer Inc v Computer Edge Pty Ltd* (1983) 50 ALR 581; *Apple Computer Inc v Computer Edge Pty Ltd* (1984) 1 FCR 549; *Computer Edge Pty Ltd v Apple Computer Inc* (1986) 161 CLR 171.

4 R A Clarke, 'Judicial Understanding of Information Technology: The Case of the Wombat ROMs' (1988) 31 *Computer Journal* 25.

5 Ibid 31–2 (emphasis altered).

In short, one particular misunderstanding of technology may have had a significant impact on the result, particularly given that the decision was made by the slimmest possible majority.

A related issue that concerned me at the same time was the application of product liability law to software.[6] At that time, only goods were subject to product liability provisions. In the case of a good that contained 'intrinsic' software, because the good as a whole was subject to that law, harm arising from embedded software was actionable. If, on the other hand, the software was a separate product, then it was not a good, and hence it was not subject to product liability law. A seemingly important change took place in 2011, when the *Australian Consumer Law* ('*ACL*')[7] defined software to be goods for the purposes of consumer law (section 2), and imposed on services the requirements of due care and skill (section 60) and reasonable fitness for purpose (section 61). In neither case does the *ACL* contain any detail, and I gather that there may be to date limited jurisprudence to clarify what the provisions actually mean.

The change appears to have had very little effect to date on quality standards in software and services. Quality remains very low, presumably because there is still almost no prospect of the provider being held liable for harm arising from carelessness, blunders in design or coding, or even cavalier disregard for standards and conventions. Society has become dependent on software and communications-based services that are inherently unreliable and insecure, and that even have designed-in insecurity. Data loss and data breach are commonplace, yet people appear to be becoming inured to frequent, unpredictable and incomprehensible misbehaviour of the devices and services that they depend on. The scale of this problem is rapidly increasing, as device-types diversify and proliferate. Beyond desktops, laptops and handhelds, we now have what are most usefully described as eObjects, including the variety of device-types within the heavily-hyped 'Internet of Things'. Further complexity is arising as supply-chains morph into complex service networks.[8]

My subsequent experiences were also somewhat mystifying. In 2000, in the first major case in which I provided expert evidence (*Welcome Real-Time SA v Catuity Inc*[9]), the legal interpretation of 'obvious' in patent law was anything but 'obvious' (at least to me, but apparently also to the legal team that secured my services). An application of smart cards that anyone in the industry would have regarded as obvious was found to be not so, and hence a French patent survived and an Australian business built around an application of the relevant kind did not. In 2004–06, in a (to the technical specialist) straightforward patent case before the Federal Court (*Visible Results Properties Inc v Sushi Train*[10]), the meaning of the patent was determined based on whether or not a lengthy

---

6 Roger Clarke, 'Who Is Liable for Software Errors? Proposed New Product Liability Law in Australia' (1989) 5(1) *Computer Law & Security Review* 28.

7 *Competition and Consumer Act 2010* (Cth) sch 2 ('*Australian Consumer Law*').

8 Kayleen Manwaring and Roger Clarke, 'Surfing the Third Wave of Computing: A Framework for Research into eObjects' (2015) 31 *Computer Law & Security Review* 586.

9 (2001) 113 FCR 110.

10 (2007) 71 IPR 282.

sentence could be construed as having a meaning without inferring a comma in its midst to indicate the end of a lengthy phrase. The grammatical issues and the constructions that they did or did not support were clearly regarded as of being prime importance, whereas the technology itself appeared to be of limited relevance to the matter.

IV UNDERSTANDING OF INFORMATION TECHNOLOGIES IN THE COURT SYSTEM

The computer industry that I entered at the end of the 1960s became 'the IT industry' by the mid 1980s, triggered by the marriage of computing with communications. Among the many benefits this offered, it created further opportunities for the technical specialist to be mystified by court processes.

The banking mechanisms for settling value-transfer transactions have operated for many decades, and have used computing since the 1960s, and networks since the 1970s. I was very surprised to be asked to provide expert evidence about the basic question of the date on which (and, spuriously, also the time at which) a business transaction occurred. My surprise was not because the question is unimportant, but because, by the time I was given the request, in 2008, the layperson would have anticipated that the courts would have long since taken judicial notice of the Australian Payments System.[11] The District Court judge in *AAV Australia Pty Ltd v Regency Media Pty Ltd*[12] was very attentive to the evidence I provided, both in court and in his judgment, making clear that the question did indeed still need to be addressed.

That example postdates the marriage of computing with star-configuration telecommunications between an organisation and a hub service-provider. Such simple applications of computing-and-communications have been to quite some degree superseded by highly-connected internetworking arrangements – of which the TCP/IP-based Internet is our most common, but far from unique, instance – together with the shared hallucination that such arrangements give rise to, conventionally referred to as cyberspace. This phenomenon is being compounded by the proliferation of computing and communications capabilities embedded in other objects (toasters, refrigerators, rubbish-bins), but also in vast numbers of very small devices (environmental monitors, drone swarms, smart dust).

In 2001-02, the *Gutnick v Dow Jones* proceedings[13] were one of a number of cases that have raised the issue of supra-, multi- and trans-jurisdictionality (a new approach to this challenge has recently been investigated in depth by Svantesson in 2017[14]). I provided what I hoped were clear explanations that would assist the

11 Roger Clarke, 'How Business Payments Get Processed in Australia' (Working Paper, Xamax Consultancy Pty Ltd, 17 August 2010) <http://www.rogerclarke.com/EC/BusPay.html>.

12 [2008] NSWDC 106.

13 *Gutnick v Dow Jones & Co Inc* [2001] VSC 305; *Dow Jones & Co Inc v Gutnick* (2002) 210 CLR 575 ('*Gutnick*').

14 Dan Jerker B Svantesson, *Solving the Internet Jurisdiction Puzzle* (Oxford University Press, 2017).

court to understand the realities of the then Web[15]. During the Victorian Supreme Court proceedings, however, counsel negotiated to keep the expert witnesses out of the witness box. It felt as though there was a desire to avoid the technical nature and processes involved in the World Wide Web clouding the seemingly far more important legal considerations. My notes on the *Gutnick* case identify specific and deep misunderstandings by two High Court Justices that appeared to me to undermine their capacity to apply the law to the technology in a reliable manner.[16] For completeness, I should make clear that my 2001 description is now outdated, because the Web's original, user-oriented architecture has since been completely inverted by the imposition of Web 2.0 features, many of which are highly business-friendly and consumer-hostile.[17]

In the Kazaa case (*Universal Music Australia Pty Ltd v Sharman License Holdings Ltd*[18]) before the Federal Court in 2004, a fleet of QCs and SCs lined up to commit character assassination of the expert witnesses, with, it transpired, more than a little success (an alternative expression such as 'impugn the character of the expert witnesses' would fail to capture the intensity of the attacks that are permitted in superior courts). This limited the judge's sources of information on peer-to-peer ('P2P') technology, giving rise to the risk that he might have to apply the law *in vacuo*. One remarkable feature of this highly-charged case was the lack of clarity to all but the judge as to whether or not privilege applied to communications between an expert witness and the law firm that arranged for the evidence to be placed before the court.

More relevantly, the title of one of my self-published papers was misquoted at me by a QC as 'Information Wants to Be Free'. He was seeking to demonstrate that I had a policy position relevant to the case and therefore was not an appropriate witness. The QC conveniently omitted the fact that the title of the article includes an ellipsis: 'Information Wants to Be Free …'[19]. The whole point of the article was that the popular expression is misleading, and that the succinct expression of the statement, dating to 1987, was that: 'Information wants to be free. Information also wants to be expensive. That tension will not go away'. My impression was that my worth as an expert witness may have survived that particular attack (but not the further and persistent barrage that it was subjected to). The court must, or course, satisfy itself that expert testimony is not unduly biased. On the other hand, the ad hominem approach that routinely opens the cross-examination phase appears to me to be a far from effective mechanism, and can leave the bench with limited information and/or a lingering air of taint.

---

15 Roger Clarke, 'Defamation on the Web' (Working Paper, Xamax Consultancy Pty Ltd, 2 October 2001) <http://www.rogerclarke.com/II/DefWeb01.html>.

16 Roger Clarke, 'Defamation on the Web: *Gutnick v Dow Jones*' (Working Paper, Xamax Consultancy Pty Ltd, 29 June 2002) <http://www.rogerclarke.com/II/Gutnick.html>.

17 Roger Clarke, 'Web 2.0 as Syndication' (2008) 3(2) *Journal of Theoretical and Applied Electronic Commerce Research* 30; Roger Clarke, 'Risks Inherent in the Digital Surveillance Economy: A Research Agenda' (Working Paper, Xamax Consultancy Pty Ltd, 19 September 2017) <http://www.rogerclarke.com/EC/DSE.html>.

18 (2005) 220 ALR 1.

19 Roger Clarke, '"Information Wants to Be Free …"' (Working Paper, Xamax Consultancy Pty Ltd, 24 February 2000) <http://www.rogerclarke.com/II/IWtbF.html>.

In the 20 or so cases that I've been involved in, each of the District Court judges, Tribunal members and Patents Examiners has worked at gaining an understanding of the relevant technology, and has reflected that in their written determination. On the other hand, in each case before superior courts, it has appeared to me that there has been limited understanding by the bench of the technical aspects of the case, and multiple instances of misapprehensions and ambiguities that, to the lay observer, appeared significant enough to undermine the chances of coherent technical analysis and hence of an appropriate application of the law to the circumstances.

If judges come to understand that their pronouncements on the technical aspects of cases are perceived as less credible than they expected, they may adapt their procedures to address the problem. One possible outcome could be a more positive attitude towards amicus curiae submissions. A more direct approach would address the present, to technical specialists, incongruous situation in which all technical and expert evidence is passed through the filter of the parties' self-interest, rather than being commissioned by the bench itself. Is the common law tradition really so fragile that it cannot contemplate the adoption of useful elements of civil code judicial systems?

V THE CURRENT ROUND OF CHALLENGES

There are a great many more challenges in the IT space, and to me it appears far from clear that law enforcement agencies, judicial communities, law reform commissions and parliaments are in any meaningful way prepared for them.

There have been multiple generations of software development tools, of which three need close attention. Algorithmic or procedural approaches, conventionally referred to as '3rd generation' software development tools, dominated from about 1970 until at least 2010. These enable the coder to express a step-by-step solution to a problem. Since the late 1980s, '5th generation' expert systems have also been used. These do not express a solution, or even declare a problem, but rather provide a structured representation of a problem-domain, by which is meant the logical framework within which some category of problems can be resolved. An expert system most commonly comprises a set of rules. The 6th generation, which has become more widely used during the current decade, refers to empirical techniques, typified by neural nets.[20] Neural nets are seeded by a small amount of pre-thought metadata, such as some labels and relationships among them. Thereafter, the process is essentially empirical, in the sense that it is based on a heap of data shovelled into pre-existing software in order to assign weights to relationships.

How has the law coped with these changes in software development approaches? Against all lay logic, the 1984 amendments to section 10 of the

20 Roger Clarke, 'A Contingency Approach to the Application Software Generations' (1991) 22(3) *Database* 23.

Copyright Act 1968 (Cth)[21] declared that the notion of a 'literary work' includes 'a computer program or compilation of computer programs'. The term 'computer program' was defined in legislation during the period 1984–2010 in a convoluted form. In 2010, that was replaced with the simpler formulation 'a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result'.[22]

A 3rd generation procedural language comprises expressions written in a designed-for-purpose language (which is presumably covered by either 'a set of statements' or 'a set of instructions', and hence by both the 1984 and 2010 versions) that is processed by software (a compiler or interpreter), with the intention of generating machine-readable language that will cause specified processing to be performed by a computer (which also appears to be covered by the remainder of both the 1984 and 2010 definitions).

In relation to a 5th generation rule-base, both the definition in 1984: 'intended … after either conversion or reproduction', and the definition in 2010: 'used … indirectly', might well be sufficient to finesse the fact that a rule-set defines not a solution but rather a problem-domain. On the other hand, a rule-base would appear not to be covered by the 1984 definition (which only included 'expression … of a set of instructions'), whereas it is encompassed by the 2010 wording 'a set of statements'. So a layperson would anticipate that copyright did not subsist in 5th generation approaches under the 1984 definition, but has done so since 2010.

The situation in relation to 6th generation approaches is more problematic. Both the 1984 definition and the 2010 formulation 'used … indirectly' may be sufficiently broad; but mere data is neither a set of statements nor a set of instructions, and hence it would appear to the layperson that techniques such as neural nets do not attract copyright protection under either the old or the new definition. Alternatively, do the tools developed in this manner really qualify for copyright coverage as a factual compilation or database in which sufficient authorial contribution has been invested? The data comprises representations of real-world transactions, and it would seem challenging to construct an argument that its collection satisfies, for example, the Australian law's criterion of intellectual effort and hence originality.

The ongoing difficulties arising in relation to the definition of 'computer program' illustrate that the aspiration of technology neutrality can only reach so far. At some point, technologies leap a previously-unappreciated boundary into uncharted territory.

A further concern is that the use of empirical techniques such as neural nets represents an abandonment of systemic reasoning. The inferences that are drawn lack a humanly-understandable explanation of the reasons underlying them, thereby denying decision-transparency. It simply cannot be determined whether or not decisions based on such inferences are rationally justifiable. Under these

21 *Copyright Amendment Act 1984* (Cth) s 3(f).
22 *Copyright Act 1968* (Cth) s 10.

circumstances, there can be no meaningful form of accountability.[23] That is a feature held in common with a range of 'big data analytics' techniques that are currently in vogue in business and government, including those promoted under the 'machine learning' badge. A recent Centrelink debacle arose because incompetent application of data matching and data analytics techniques resulted in false accusations of breaches by large numbers of welfare recipients. In this case, the errors were so gross that their nature could be readily inferred and publicly exposed. Yet, unabashed and brazenly, government agencies are continuing to apply such techniques. It is far from clear that any technologically neutral regulatory measures are in place that can prevent powerless individuals from suffering a great deal of heartburn and gross injustices, because of blunders more obscure than those in the Centrelink case, arising from empirical approaches to decision-making.

The abandonment of reason and the deification of data are dangerous enough, but one further segment of information technology needs to be factored in. The combination of computing and communications from the 1960s onwards delivered automation of data-handling across physical space, but impacts on the real world have still depended on actions by human beings. That has the beneficial effect of bringing into play self-preservation instincts, and hence caution. Slowly, however, effectors have been integrated with computing and communications. Familiar examples include the moving parts of ATMs, which ferry a card into the machine and dispense banknotes. More substantial examples include the automated opening of dam sluice gates and control of manufacturing equipment. Within-car IT has expanded well beyond fine-tuning the mix entering the cylinder, and hence robotics is becoming more evident to us all in the form of driverless cars.

A polygamous marriage is currently in train, involving computing-and-communications with empiricism and robotics. The new union gives rise to change whose nature is appropriately represented as a discontinuity or a quantum shift. Every existing assumption of technologically neutral expression in IT contexts needs to be reconsidered; and a great many of them may require adaptation or replacement. Further, there has to be considerable doubt as to whether current court processes will cope with the technological complexities, and hence it is reasonable to expect that the lottery element in judgments will increase.

VI THE THEMATIC ISSUE

The Call for Submissions for this thematic Issue had as its focus 'Cyberspace and the Law'. It sought submissions that consider 'how new developments in the realm of cyberspace technology fit within existing legal frameworks, and potential problems this may cause' and 'how the law must change to

23 Roger Clarke, 'Quality Assurance for Security Applications of Big Data' (Paper presented at the European Intelligence and Security Informatics Conference, Uppsala, Sweden, 17–19 August 2016).

accommodate these developments in cyberspace technology'. The collection as a whole reflects the diversity of technologies and topics within the broad area. A common feature was that each authorial group judged that in order to provide a sufficiently thorough treatment, a fairly tight focus was necessary.

The first article, by David Lindsay, considers the increasingly prevalent impositions on Internet intermediaries to access and even interfere with the data that they handle on behalf of their clients. Arguments by analogy with the postal, telegraph and telephone services that preceded Internet services by over a century have transpired to be of very limited relevance because the nature of the technologies that overlay the mere data transmission level are so much more sophisticated, and the value of the content so much higher, that the conflicts in interests among the parties are so much more intense.

The particular focus of the article is injunctions to block access in order to prevent copyright infringements, and what principles might be applied in order to achieve reasonable balances among the multiple interests. One important insight is the relativity of the term 'proportionality', and the necessity of developing interpretations of the term that are quite specific to the particular technical and commercial context. In the case of traffic-blocking injunctions, careful judicial analysis is needed of the very different technical mechanisms involved in blocking IP-addresses, domain-names, pathnames and URL's. Further confirming my layperson concerns about understanding of the relevant technology by the courts, Lindsay draws attention to a potential compromise of one Australian judgment due to 'an apparent conflation between a domain name and a URL'.[24]

Another issue that the article draws attention to is the application of the Australian provisions to an 'online location'. Terms such as location and space have hitherto applied solely to the physical world. Their use in the new context of a non-physical world is unlikely to deliver any kind of clarity until a large number of cases have been litigated to completion – by which time a new wave of technology is likely to have rendered the now-clear application of the law irrelevant. This particular endeavour to achieve technology neutrality, by generating uncertainties rather than resolving them, is seriously unhelpful to enterprises that are trying to get on with business.

The next two articles in the thematic Issue consider aspects of monetary value in cyberspace. That by Katharine Kemp and Ross Buckley is concerned with the powers needed by regulators when an e-money provider experiences financial distress. This is particularly challenging where the provider is not a bank, and hence no regulator has the 'resolution powers' conventional in banking regulation. Orderly, regulator-imposed bailouts may not be feasible and insolvencies can easily become 'worst-case scenarios' for balance-holders, for other providers of similar services, and for public confidence in the financial system. A variety of approaches are canvassed, intended to cope with the changing patterns of risk wrought by changing e-technologies.

---

24 David Lindsay, 'Website Blocking Injunctions to Prevent Copyright Infringements: Proportionality and Effectiveness' (2017) 40 *University of New South Wales Law Journal* 1507, 1529.

Cheng-Yun Tsang, Louise Malady and Ross Buckley are concerned that the lack of interest earnings on balances held as e-money acts as a disincentive to savings. This disadvantages the poor, by denying some small returns to help cover the providers' fees, and by failing to encourage 'the unbanked' to become and remain accumulators of monetary value. It is to be expected that providers of e-money services would try to keep for themselves the financial benefits from their customers' balances. On the other hand, the widespread approach of regulators whereby interest-payments on such amounts are banned has significant negative economic and social impacts on consumers. The harm of the perverse policy is greatest in respect of the least well-off in economically developing countries. In part, the problem arises from the treatment of e-money as though it were akin to bank deposits, rather than a technologically-enabled new way of doing things, which requires a regulatory framework sui generis, of its own kind.

In the thematic Issue's fourth article, Hadeel Al-Alosi addresses the topic of technology-facilitated domestic abuse. The range of 'controlling and coercive' behaviours it encompasses includes 'threatening phone calls, cyber-stalking, location tracking via smartphones, harassment on social media sites, and the dissemination of intimate images of partners without consent ("revenge porn")'[25].

As with other usages of words from the physical world in the electronic context, I have misgivings about the use of the short form 'cyber-violence' to refer to these behaviours. The absence of physical contact, and even of the immediate prospect of it, suggests to me that more apt terms should be adopted instead, to avoid imputing non-relevant characteristics to the behaviours under discussion. For clarity, I am not contesting the importance of studying technology-facilitated domestic abuse. As the author argues, it is vital to take into account the facts that most of the abuse is by males and that remote abuse can be psychologically very harmful, to appreciate that these forms of abuse are sometimes closely linked with and/or precursors to physical assault, and to recognise the urgent need for improvements in law and practice. My concern is that effective solutions need to reflect the realities of the context, including the technologies involved.

An important insight is that '[t]echnology … allows abusers to overcome geographic and spatial boundaries … [and] create "a sense of omnipresence … eroding [the victim's] feelings of safety after separation"'.[26] The evidence presented is substantial and compelling. The author also identifies several specific measures that represent safeguards against such abuses. Some, such as a wave of overly-specific 'revenge porn' laws – which, to be effective, must inevitably contain excruciating detail – would not be needed if legislatures had not failed to establish a privacy right of action. This is one area in which a generic approach, coupled with the various Law Reform Commissions' carefully formulated recommendations for powers and discretions, would lay the foundation for legal responses to a wide variety of such problems. A further

25 Hadeel Al-Alosi, 'Cyber-Violence: Digital Abuse in the Context of Domestic Violence' (2017) 40 *University of New South Wales Law Journal* 1573, 1573.

26 Ibid 1578.

critical element is specific guidance and training to assist people subjected to abuses to help themselves, and to know where to turn when external assistance is needed.

In the fifth article, Rachel Hews and Nicolas Suzor consider uses of IT during a trial that give rise to prejudicial publicity, possibly in breach of sub judice contempt laws that are intended to assist in the fairness of the trial process. The study's focus was on postings on Twitter, which may reach jurors during the trial or the jury's deliberations. The authors analysed a 22.5 per cent sample of over 30 000 tweets during the 5 weeks of a particular, highly-publicised murder trial during which both the judge and defence counsel reminded jurors 'to ignore media headlines about the guilt of the accused'.

Modest concern arose in relation to the two-thirds of tweets that were by professional journalists. A key finding was that 'the concentration of key themes or messages into 140 characters could create a more distorted or exaggerated view than traditional news reporting'.[27] The other third, on the other hand, showed 12 per cent 'low level' prejudicial content and 2.7 per cent 'high level'. Among the general public's content, the authors found that, as a dominant pattern, tweets 'accept and reinforce the prosecution's theory of the case', whereas 'the case for the defence was muted'.[28] Imbalance of this kind is not currently addressed by sub judice law. The current approach to assuring fairness is severely challenged in the new context of pervasive social media and bandwagon effects.

The final article, by Kerstin Braun, examines the concept of 'social media misconduct' by jurors. Her assessment of available reports identified few instances in Australia where a juror is known to have materially breached their responsibilities, at least at the level that would result in a mistrial. On the other hand, a wide range of circumstances exist that can be problematic. The article also considers 'whether viable avenues exist to sufficiently address this potential challenge in the Australian context', and concludes that 'the effectiveness of many of the suggested approaches remains questionable and that their implementation is politically unrealistic'.[29]

VII CONCLUSIONS

This thematic Issue makes valuable contributions to specific challenges in the broad area of law and cyberspace. Referring back to the second of my two themes, the articles offer some valuable insights into my personal concerns about the capacity of court processes to deal with technological complexity. Understanding the alternative approaches to blocking Internet traffic was shown

27 Rachel Hews and Nicolas Suzor, '"Scum of the Earth": An Analysis of Prejudicial Twitter Conversations during the Baden-Clay Murder Trial' (2017) 40 *University of New South Wales Law Journal* 1604, 1626.

28 Ibid 1622, 1627–8.

29 Kerstin Braun, 'Yesterday Is History, Tomorrow Is a Mystery – The Fate of the Australian Jury System in the Age of Social Media Dependency' (2017) 40 *University of New South Wales Law Journal* 1634, 1635–6.

to be (overly) challenging. Risks arose because of the framing of some cyberspace issues by means of metaphorical uses of terms that originally referred to real-world rather than virtual phenomena (location, violence). Multiple examples were provided of courts not appreciating the realities of cyberspace threats in the context of domestic disputes.

In relation to my other theme, I looked at the articles through the lens of technology neutrality. Each of them underlines the need for either techno-specific measures or re-formulation of technologically neutral requirements in order to encompass contemporary IT. I tentatively suggested a meta-principle for technologically neutral statements ('appropriate scope'). The Issue subjects this to severe testing in the context of social media, because the characteristics of services vary so much. Microblogs (Twitter), social networking services targeted at different demographics (Facebook, LinkedIn), and services oriented towards image and video rather than text (Instagram, YouTube) have rather different features, uses and impacts, and require rather different safeguards, mitigation measures and controls.

Broad, functional expressions of requirements need to apply to many current, but also hopefully to many near-future, IT capabilities and cyberspace behaviours. Given the nature of 'affordances' – or, in William Gibson's less intellectualist and more grounded terms, 'the street finds its uses for things' – that seems like it might be a pious hope.

VIII POSTSCRIPT: SINGULARITY, DUALITY OR MULTILARITY?

The articles in this thematic Issue continue the fine tradition that has arisen in the mere 35 years since the emergence of the word cyberspace, and the 25 years since the emergence of the phenomena associated with it. However, none of these articles confronts the much more substantial challenges that the maturing complex of information technologies presents to humankind.

Cyberspace can no longer be thought of as just a blizzard of data. Nor is it enough to imagine emergent intelligence amidst that blizzard. Cyberspace now includes devices that act directly on the world. The actions that those devices take are in some cases actively managed by humans, and in others the devices are subject to human oversight. Increasingly, however, those actions are being delegated – accidentally and in some cases even intentionally – and often without the scope for humans to exercise control. A conventional aspect of the design process for large-scale systems has been the careful allocation of the risks. But many of the schemes that society is sleepwalking its way into involve risks that no-one has assessed, coupled with an absence of accountability. We're generating a monstrous technology-complex, and we have no understanding of what kind of relationship our children and grandchildren will have with it.

A few 'visionaries' at the intersection of marketing and metaphysics talk excitedly about the (or perhaps a) impending 'singularity'. Most people, on the other hand, anticipate that the real world will continue, and that the main change

will be in who, or perhaps what, holds the power. What does technology neutrality have to offer in the circumstances confronting us? And if court processes are severely challenged by even moderate levels of technological complexity, and are pleased to escape from it and get back to legal questions, is there any real prospect of survival of principles such as evaluation, fairness, proportionality, evidence-based decision-making, accountability, and the right to challenge decisions?

Legal analyses of very specific topics have value; but they need to be complemented by much broader considerations of law as an instrument of policy, and of policy as a tool for protecting the interests of humankind. Perhaps the *Journal*'s editors will consider commissioning a thematic Issue on these much more substantial shifts in the nature of IT, and on the scope for adaptations to court processes in order to sustain quality in their outcomes.