INTERNET POLICY REVIEW
Journal on internet regulation

Volume 6 | Issue 1

Internet policy and Australia's Northern Territory Intervention

Ellie Rennie
Swinburne Institute for Social Research, Swinburne University of Technology, Melbourne, Australia

Jake Goldenfein
Swinburne Law School, Swinburne University of Technology, Melbourne, Australia, jgoldenfein@swin.edu.au

Julian Thomas
Social Change Research Platform, RMIT University, Melbourne, Australia, julian.thomas@rmit.edu.au

Published on 14 Mar 2017 | DOI: 10.14763/2017.1.456

Abstract: In 2007, Australia's Commonwealth Government took a dramatic new approach to the governance of remote Indigenous communities. The 'Northern Territory Intervention' aimed to combat abuse and violence in remote Indigenous communities, and included far-reaching changes to welfare administration, employment programmes and policing. This paper considers a hitherto obscure aspect of the Intervention: the surveillance of publicly funded computers and internet use. Between 2007 and 2012, providers of internet and computer access facilities in the affected communities were required to audit and record computer use. In this paper we examine the legal and policy dimensions of this case of governmental surveillance, using interviews, published materials and documents obtained through freedom of information processes.

Keywords: Digital divide, Surveillance, Computer surveillance, Child protection, Remote Indigenous communities

Article information

Received: 02 Jun 2016 **Reviewed:** 01 Dec 2016 **Published:** 14 Mar 2017

Funding: We gratefully acknowledge the support of Google Australia, which provided funding for this project.
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/internet-policy-and-australias-northern-territory-intervention

Citation: Rennie, E. & Goldenfein, J. & Thomas, J. (2017). Internet policy and Australia's Northern Territory Intervention. *Internet Policy Review*, 6(1). DOI: 10.14763/2017.1.456

INTRODUCTION

In 2007, the Australian government took a dramatic new approach to the governance and management of remote Indigenous communities. The 'Northern Territory Intervention', as it became commonly known, was introduced as a means to combat child abuse and domestic violence in remote Indigenous communities, and included far-reaching changes to welfare administration, employment programmes and policing. Although the Intervention, which persisted until 2012, has been the subject of a great deal of public commentary and critique, one dimension has remained surprisingly obscure: the surveillance of publicly funded computers. In this respect, as this article describes, the Intervention is an important episode in the history of Australian internet policy, with ramifications for policy debates today.

Between 2007 and 2012, providers of internet and computer access facilities in the more than 70 affected communities were required to audit, or document, the use of their computers, keep detailed records of computer users, and install filters on computers and networks. In this paper we provide the first analysis of this attempt at official ICT surveillance, designed to target a specific group. Looking beyond the statutory provisions, we are interested in the implementation and consequences of policy. We therefore consider the outcomes of the auditing and reporting process.

The topic and our approach require a combination of legal, policy, and social research methods. We draw on several main sources: published sources, and official documentation, obtained from the Australian government through freedom of information (FoI) requests; and interviews with people in the communities involved; and others concerned with administering the scheme. In this introduction, we explain in more detail how we went about the research, and foreshadow our main findings.

In the first half of this paper, we examine the legal framework for those aspects of the Intervention related to publicly funded computers. No convictions resulted from the auditing process, and alleged pornography was found on less than five per cent of all computers. However, we note that the auditing process enabled the provision of general intelligence to the Australian Crime Commission (and likely the National Indigenous Intelligence Taskforce) pursuant to a Memorandum of Understanding. That memorandum, as well as other documents concerning the mechanics and result of the audits, were obtained through FoI requests, to both the Australian Crime Commission and the Department of Families, Housing, Community Services and Indigenous Affairs ("FaHCSIA"). The documents obtained included only a small fraction of what was requested, and all were highly redacted on the basis of FoI exemptions including: 'prejudice to law enforcement methods and procedures', public interest in that it would prejudice the effectiveness of the auditing process as well as the effectiveness of ACC's intelligence gathering, and 'personal privacy'. These documents, in particular the Memorandum of Understanding between FaHCSIA and ACC, suggest that despite the auditing policy being implemented on the basis of reducing the harm of pornography in communities, criminal intelligence gathering was another significant motivation.

In the second half of the paper we draw on evidence gathered through interviews with community members, and other participants in the process, to discuss the experience of complying with the audits and the factors that may have contributed to the demise of this instance of legislatively mandated surveillance. Those interviews included discussions with computer centre users and administrators while in the Indigenous community of Papunya in

2012. Other shire staff and technical officers, and members of the NT Library service were interviewed over telephone. Researchers visited Papunya with the permission of its elders, the Shire President and the Central Land Council, as well as the support of the Central Australian Youth Link up Service (CAYLUS), in May 2012. We met with the traditional owner, discussed the research project with him and he gave permission for us to undertake the study. Participants gave their consent by signing a consent form (explained verbally to them by the researcher, if need be) or by giving verbal (recorded) consent. Vouchers and USB sticks were offered in exchange for participating in the study: memory sticks were the most popular gifts.

We carried out a survey of residents at Papunya from 9 to 11 May 2012. During this period, various factors combined to limit the number of formal surveys conducted. Many people spent the previous long weekend at the Hermannsburg football carnival and did not return to Papunya until midway through the survey period. There were other competing demands on people's time, including filming and recording at the Warumpi Studio as part of a Suicide Prevention Program, a couple of funerals and some Land Council meetings. An unexpected week long closure of the main computer room beginning on 10 May also impacted on its usage and the number of people we were able to formally interview. These impacts were offset to some extent by undertaking a series of informal discussions with various groups and individuals, as well as conducting some interviews at locations other than the computer room, such as outside the community store. This proved advantageous as we made contact with some ICT room non-users as well as users.

Our researchers also held in-depth, semi-structured interviews with a Linkz Recruitment Volunteer Co-ordinator; a Papunya community member and Computer Centre supervisor; MacDonnell Shire youth workers based at Papunya and Mt Liebig; and a former ICV Computer Centre volunteer (Alice Springs, 30 April). In addition, we spoke with the Art Room Co-ordinator and a school teacher about the use of ICTs in their respective areas, and had informal conversations with CAYLUS workers about Papunya ICT arrangements before and after the study.

In this article, our argument is that it was the 'digital divide' between Indigenous and other Australians which made this particular policing of internet use possible, and that its impact was compounded by the low rates of internet adoption among Indigenous households. Further, the policy exacerbated the divide by imposing costly requirements on those attempting to provide some level of access. As a distinctive 'moment' in Australian internet policy, the Intervention is also significant, demonstrating not only the practical and political difficulties in applying highly centralised 'national' solutions to diverse, highly localised situations, but also the fragility and contingency of policy settlements. Internet policy stretches across technology, social and cultural administration: its scope is a source of power for governments, but also, as the Intervention episode shows, may give rise to instability.

The episode of the Intervention also illustrates some important interconnections between domains of internet and information policy often regarded as discrete. Public policy debate has long been concerned with the social distribution of internet use, and the capacity of governments to ameliorate the digital divide (see Rennie et al., 2010, and Rennie et al. 2016, especially chapter 1). The Intervention acted, highly reactively, upon and across the diverse policy fields of policing, official surveillance, and the regulation of offensive or illegal content. It was driven, we suggest, by an unstable mixture of governmental motivations, and it exemplifies the difficult legal, administrative and political questions likely to arise from such a volatile, and (as it transpired) transient policy compound.

THE NORTHERN TERRITORY INTERVENTION

On 15 June 2007 the then Northern Territory (NT) Chief Minister, Clare Martin, publicly released *Little Children Are Sacred*, a report produced by the Board of Inquiry into the Protection of Aboriginal Children from Sexual Abuse (Northern Territory Government [NT], 2007). The report made 97 recommendations to promote the safety of children in remote Indigenous communities. At the time, there were 73 communities with more than 100 residents in the Northern Territory that fell under this category. In the *Little Children Are Sacred* report, child sexual abuse and violence was linked to background conditions of alcohol and drug abuse, gambling, deficient parenting, problems with education, housing, poverty (NT, 2007, 7), intergenerational trauma and the breakdown of cultural restraints (NT, 2007, 63). The abuse of children was seen as symptomatic of a broadly failing regulatory and administrative environment. In particular, pornography was identified in the report as highly problematic in Indigenous communities because of its use in 'grooming' children for sex (NT, 2007, 199). Troubling anecdotes were recorded about children as young as three performing sexual behaviours (NT, 2007, 65), and children as young as ten being exposed to 'degrading and depraved pornography' and subsequently being forced to 'act it out' (NT, 2007, 65). Although the connection between pornography exposure and sex offending was recognised as tenuous (NT, 2007, 209), the report argued for 'situational prevention', by addressing the inappropriate exposure and normalisation of children to sexual material.

To this end, *Little Children Are Sacred* recommended introducing a new offence of exposing a person under 16 years of age to pornography; it also proposed better education about the rationale and meaning of the media classification system (NT, 2007, 32). However, the legal and policy responses to the report would eventually be far more extensive. The then conservative national government introduced a suite of legislative measures dubbed the Northern Territory National Emergency Response, widely known as 'the Northern Territory Intervention'. Because the legislation was operative solely for individuals living in 'prescribed areas', [1] being Indigenous communities, those measures required exemption from the *Racial Discrimination Act 1975* (Cth).

The *Northern Territory National Emergency Response* [*NTNER*] *Act 2007* (Cth) (hereafter, "the Act") was the primary statutory instrument enacting recommendations from the *Little Children Are Sacred* report. Several provisions dealing with pornography were introduced. These included prohibiting certain material in prescribed areas, [2] creating new offences, [3] and giving the Australian Crime Commission new powers (discussed below). [4] The Report identified DVD, video and pay television as the problematic media for pornography at the time. [5] However, measures to assuage the availability of pornography on 'publicly funded computers' (as defined in the Act, s3) were also included, without explanation, even though these were not identified as a problem in the report. Those measures are the focus of this paper, particularly the prescription that such computers be subjected to periodic auditing with the results collected and processed by the Australian Crime Commission (the Act, s27).

The implementation of computer auditing in remote communities under the Act was a remarkable case of institutional surveillance of a marginalised and vulnerable group. Similar policies have not been enacted elsewhere in Australia. As we explain in this article, the Act created new restrictions on freedom of expression in Indigenous communities in ways that went considerably beyond established Australian information and communication law. Further, the experience of implementing this kind of surveillance regime illuminates some of the more

fundamental concerns regarding technology dissemination in remote areas and for marginalised communities. We argue below that only in circumstances of significant digital inequality could an approach such as this have been proposed and considered viable.

Broadly speaking, the analysis that follows shows that the computer auditing aspects of the Intervention were flawed. Since the expiry of the *NTNER* legislation in 2012, the auditing requirements have moved to the private Commonwealth funding agreements for computer centres in the 'prohibited material areas' of the *Stronger Futures in the Northern Territory Act 2012* (Cth), with little public information as to their continuation. This paper seeks to identify the rationale for that regulatory adjustment, observing that uptake and adoption of computers and the internet in these areas generally has moved away from a focus on 'publicly funded' computers as community members increasingly obtain their own devices.

AUDITING OF PUBLICLY FUNDED COMPUTERS

According to a 2009 Government Discussion Paper, the auditing requirements were designed to prevent women and children from being exposed to prohibited material on public computers: "They were introduced in response to complaints from Aboriginal women about their distress at finding pornographic, violent and possibly illegal material on computers provided to community organisations through government grants or other funding" (Cth 2009a, 21). The measures therefore addressed the 'destructive impact pornography can have on the lives of children' (Cth 2007, 10). However, the auditing requirements had a broader scope, including tracking computer use, criminal prosecution, and the control of copyright infringement, breaches of privacy and other instances of misuse such as fraud and stalking (Explanatory Memorandum, NTNER Bill 2007). It is far from clear how the programmes intended to achieve those latter objectives, but our research did uncover the processes by which general intelligence on computer use in remote communities would be gathered for relevant federal law enforcement and criminal intelligence agencies.

There were numerous Intervention policies targeting pornography in prescribed areas, including a controversial requirement that communities display a 'highway and community' road sign, otherwise known as a 'big blue sign' indicating that pornography was illegal. Mal Brough, the then Minister for Families, Community Services and Indigenous Affairs (FaHCSIA) noted when introducing the Act that although 'a ban on the possession and dissemination of prohibited pornographic material is addressed in another bill in this package', computer audits were necessary because 'sexually explicit and other illegal material can be accessed using the internet through misuse of publicly funded computers as well' (Cth 2007, 10).

'Publicly funded computer' was defined in section 3 of the Act and included computers in prescribed areas whereby:

> The computer is owned or leased by an individual who, or a body (whether or not incorporated) that, receives funding from the Commonwealth, a State, a Territory or a local government authority; or

> The computer is on loan from a body (whether or not incorporated) that receives funding from the Commonwealth, a State, a Territory or a local government

> authority; or

> The computer is owned or leased by an individual who, or a body (whether or not incorporated) that, receives money directly or indirectly from the Commonwealth under an arrangement for the delivery of services, or programs, related to employment (*NTNER ACT*, *2007* (Cth), s3).

Although that definition could be narrowly read, the Senate Standing Committee on Legal and Constitutional Affairs asserted that the definition should be construed broadly. Their August 2007 report stated:

> It is important to note that the definition of a "publicly funded computer" is very broad and is not limited to a computer that is actually purchased with government money or is used in the provision of a service funded by the government. The definition includes a computer that is owned or leased or in the possession of **somebody who receives government funding and is in a prescribed area** (Senate Standing Committee on Legal and Constitutional Affairs, 2007, 71, our emphasis).

The Committee's suggestion could be taken to mean that the measures applied to anyone receiving welfare payments or income who was also in possession of a computer. Conversely, the Explanatory Memorandum to the 2007 Bill stated that 'funding' did not include income derived from governments in the form of a salary, income support payments and the like (Explanatory Memorandum NTNER Bill, 2007). A 2009 policy statement issued by the Commonwealth government affirmed that the measures were introduced to protect Indigenous people living in remote communities from sexually explicit and very violent material on computers 'provided to community organisations under government grants or other funding' (Cth 2009, 12).

Section 26 of the Act specifies the obligation for a 'responsible person for a publicly funded computer' to install, maintain, and update an accredited filter. On 10 August 2007 then Prime Minister John Howard also announced initiatives for providing free online filters to public libraries and Australian families (Stafford, 2007). Senator Helen Coonan, then Minister for Communications, Information Technology and the Arts, called on Premiers and the NT Chief Minister to 'take this matter seriously' (Senate Standing Committee on Legal and Constitutional Affair, 2007, 30). Section 27 of the Act obliged those 'responsible persons' to keep records of the time, day, and identity of each person who used a computer for three years. That requirement was designed to assist in any investigation after access to illegal material was detected, by providing a mechanism to identify the person using a computer at any particular time (Explanatory Memorandum NTNER Bill, 2007).

Section 28 required the development of an 'acceptable use policy' in computer centres specifying any matter the Minister determined necessary by legislative instrument. All acceptable use policies were required to state that a person cannot use the computer to access, or to send a communication, material or a statement that:

> contravened, or formed part of an activity that contravened, a law of the

> Commonwealth, a State or a Territory; incited a person to contravene a law of the Commonwealth, a State or a Territory; was slanderous, libellous or defamatory; was offensive or obscene; was abusive or that threatened the use of violence; harassed another person on the basis of sex, race, disability or any other status that was protected by a law of the Commonwealth, a State or a Territory; was an anonymous or a repeated communication designed to annoy or torment.

Computer centre administrators were also required to make each user aware of the content of the policy, the fact that the user would be audited, and the fact that an audit report, possibly including the user's name and usage of the computer, would be given to the Australian Crime Commission. The explanatory memorandum to the *NTNER* Bill also stipulated that the requirement for acceptable use policies should also apply to individual private computers and anyone using them, although this was never legislated (Explanatory Memorandum NTNER Bill, 2007 (Cth), 21).

Section 29 contained the principal component of the scheme – the actual auditing provisions intended to identify the extent of illegal material on publicly funded computers. It specified that the person responsible for a computer must ensure the audit be performed at the appropriate time, provide the audit report to the Australian Crime Commission and keep a record of the report for three years. While special restrictions on use may not seem unusual for computers in public spaces, or those designed for public internet access, the distinctive element of these provisions was their application to a much wider range of computers: all those that would fall into the broad category of "publicly funded".

THE AUDIT PROCESS

The first audit occurred on 2 June 2008. Precise technical details are unclear, however evidence suggests FaHCSIA distributed a USB drive containing software (an in-house developed auditing script) to be inserted individually into each relevant computer. The material collected from that software was then forwarded to the Australian Crime Commission (ACC) Cyber Support Unit which compiled an 'audit report' that was distributed back to FaHCSIA and any other relevant agency (for example the Australian Federal Police). The ACC received advice from FaHCSIA that approximately 183 organisations and over 300 individual computers would be audited (Australian Crime Commission (ACC) 2008), with reports due in 14 days. Only 38 per cent of organisations responded in the first audit. According to a NTNER Monitoring Report, delays were apparently due to compliance costs, hardware incompatibility with the software distributed, varying levels of computer literacy in communities, and a lack of awareness of audit requirements (FaHCSIA, 2009).

It seems likely that the poor outcome provoked FaHCSIA to use more specialised software. Pinpoint Auditor was licensed and supported by the Queensland-based network services firm Bridge Point Communications Pty Ltd. The June 2008 Audit Report indicated that the ACC Cyber Support Unit had provided technical advice to FaHCSIA about negotiations with a software developer. The contracts between Bridge Point and FaHCSIA show that Bridge Point supplied the software and 'information technology services to support the audit of publicly funded computers in prescribed areas' for the price of AUD $337,519.77 (FaHCSIA 2009b). The contract between FaHCSIA and Bridge Point included the provision of 650 USB keys loaded with the 'PinPoint Auditor' software, and required Bridge Point to modify the software when

requested, delete and reload the USB keys, assist with audits, resource and manage a helpdesk, collate reports, maintain a master list of organisations and provide a final briefing to FaHCSIA and the ACC. This was undoubtedly the largest expenditure of the auditing project, with no additional resources supplied to the wider range of actors involved in the auditing process, including the communities themselves, the shire offices (the local government agencies in the Northern Territory), the Northern Territory Library, or other groups.

The second audit also altered the technological process from exclusively auditing individual computers to auditing the Shire Server Centres (Cth, 2010). A technical support help desk was also established for the 14-day compliance period. It appears that technical problems plagued the auditing process even when using the Pinpoint Auditor software. An ACC document from March 2011 to FaHCSIA points out that some (around 4%) of the audit files received were corrupted or not able to be opened for examination (ACC, 2011).

FaHCSIA also distributed 'audit packs' (Cth, 2010), and provided information on computer use policies and how to maintain user logs (FaHCSIA, 2009). It appears illegal material was found by both the June and December 2008 audits and although those instances were reported to police (ACC, 2009b), no persons were prosecuted (Cth, 2009a). The May 2010 audit also involved an education programme on the value of audits, including posters, mouse pads and other promotional material, which appear to have greatly improved compliance rates (see table 1). For the December 2010 audit, a process was developed to audit the Shire Citrix Server, which included 55 of the 60 shire sites, instead of individual computers (Cth, 2010).

From our assessment of the ACC documents, the number of computers found to have alleged illicit images was never higher than five per cent of all computers, with an average of 2.5 per cent across all audit rounds. As the documents we obtained through freedom of information were heavily redacted, this figure should be treated with caution. For most rounds, a significant portion of organisations did not respond or were not fully compliant (we found no evidence of penalties being applied for non-compliance). Although the alleged illicit material was only found on a small fraction of computers, it appears to have been spread across a number of organisations – as high as 30 per cent of organisations that submitted compliant reports in some rounds [6]. Further questions arise, including where the computers were located, how accessible they were to community members, and the proportion of total internet use within the prescribed areas that occurred on these computers. Although we cannot know the answer to these questions, an understanding of digital divide in the Northern Territory during this period provides important context for this surveillance regime and its operation.

REMOTE INDIGENOUS COMMUNITIES AND THE DIGITAL DIVIDE

Very few Indigenous people living in remote communities had access to the internet from home when the Intervention was launched in mid-2007. Statistics from the 2006 census revealed that only 13% of Indigenous households in remote and very remote NT (including the large township of Alice Springs, which was not a prescribed area) had access to the internet at home, compared with 70% of non-Indigenous households (Australian Bureau of Statistics [ABS], 2007, see also ABS, 2007a).

The Australian government had attempted to address the digital divide through various programmes, all of which were centred on the provision of public internet centres. *Networking*

the Nation funded 71 internet facilities in remote areas, most of which were in the Northern Territory between 1996 and 2003 (Department of Communications, Information Technology and the Arts [DCITA], 2005). In 2002, the *Telecommunications Action Plan for Remote Indigenous Communities Report* recommended that the government provide public internet access facilities rather than other programmes, as "Public access is more affordable and is well suited to the generally communal lifestyle of these remote communities. It also provides a central point for community support and training" (DCITA, 2002). The Plan received AUD $8.3 million over four years to improve telecommunications in remote communities, including funding for up to 170 public internet access facilities across remote Australia.

Analysis of the Community Housing Infrastructure Needs Survey data from 2006 found that 11% of Indigenous communities had some public internet access, with potential users of those centres accounting for approximately 50% of the population of remote Australia (Australian Communications and Media Authority, 2008). A study by Daly, using 2001 census data, found that residents of remote Indigenous communities were three times more likely than the general population to be using communal internet and computer facilities (Daly, 2005). Although these figures demonstrate the potential reach of community internet facilities during the Intervention, the on-the-ground reality was more complicated. A 2009 survey of the 34 larger remote communities in the central Australia region found that half had community internet access facilities (a total of 50 computers), but many of these were rarely or only occasionally in operation and available for use (Rennie et al., 2010).

By the time the *NTNER Act 2007* (Cth) was replaced by *Stronger Futures* in mid-2012, household internet access had more than doubled. At the time of the 2011 census, 33 per cent of Indigenous households in remote and very remote areas of the NT had access at home (compared with 85 per cent of non-Indigenous households, ABS, 2012). Although internet adoption in the NT rose during the period of the Intervention, significant disparities continued to exist between different localities. For instance, in 2011, only 16 per cent of Indigenous households had some form of internet connection in two of the three central Australia local government areas (Barkley and Central Desert Shires). Access from home was higher in the local government area, MacDonnell Shire, where 24 per cent of Indigenous households had access. In the large township of Alice Springs, 37 per cent of Indigenous households had an internet connection (ABS, 2012).

The regional differences are most likely explained by available ICT infrastructure, as well as cultural factors that influence consumer choices. Indigenous people living in remote communities mostly choose pre-paid billing systems, partly because it is simpler and partly to avoid bill shock, which is prevalent due to the way that resources (such as money or devices) are shared amongst family and friends, a practice known as 'demand sharing' (Rennie et al., 2013). Internet use is therefore likely to be much higher in communities with mobile coverage as mobile pre-paid billing is relatively straightforward for people compared to post-paid satellite or ADSL plans (Ewing et al., 2015).

Public internet access facilities also continued to be funded during the Intervention. Between 2009-2013, the *Indigenous Communications Program* funded public internet access facilities in 102 Indigenous communities, as well as training in internet and basic computer use, administered in the Northern Territory by the NT Library (under the *National Partnership Agreement on Remote Indigenous Public Internet Access 2009* (RIPIA, Council of Australian Governments, 2009, see below). The decision to legislate for the surveillance of these computers was therefore carried out with the knowledge that, for many people at that time, a public

computer was the only form of access. The laws would have had far more limited impact in mainstream Australia, where only a very small minority would be accessing public, rather than privately owned, computers.

THE END OF THE AUDIT REQUIREMENTS

As the *NTNER Act 2007* (Cth) transitioned into the *Stronger Futures in the Northern Territory Act 2012* (Cth), the statutory audit requirements expired. The stated intention then was to embed auditing obligations into funding agreements with organisations (Cth, 2011a). However, we have not found any information about auditing obligations in Commonwealth funding agreements or in our interviews with stakeholders. None of the secondary material for the *Stronger Futures* Act references the discontinuation of statutory auditing (Cth, 2009). [7]

No official policy analysis or rationale was provided for discontinuing the audit requirement, although the issues raised before and during its implementation offer some clues as to why it was abandoned. In parliamentary debate, the Greens party had argued that the obligations on computer centres were too onerous and unlikely to be effective (Senate Standing Committee on Legal and Constitutional Affairs, 2007a). The Senate Standing Committee on Legal and Constitutional Affairs considered that the requirement for computer centre administrators to have sufficient knowledge of the law to identify when computers were being used for various offences was unreasonable. [8] The substantial workload for FaHCSIA, and the problematic compliance rates may have also been factors in the reconfiguration of auditing responsibilities (FaHCSIA, 2009). There were even discussions about the legality of making the downloading of certain material illegal in one part of a jurisdiction but not elsewhere (Cth, 2007, 93).

Most community consultation indicated acceptance of the auditing, as part of the general restriction on pornography. In May 2009, the *Future Directions* discussion paper indicated the government intended to retain the auditing requirements as part of the suite of pornography controls. In response to questions about the auditing requirements, communities showed general support without identifying specific benefits (Cth, 2009; Cth, 2009a). It was acknowledged however, that not applying controls to private computers was problematic, and that the cost in maintaining the restrictions was significant. One community indicated they would prefer audits to be publicly funded (Cth, 2009a). Other accounts suggested that community attitudes towards pornography and computer restrictions were not clear or definitive. The November 2011 *Northern Territory Emergency Response* Report noted that 'The issue of access to 'sexy pictures' did not rate highly as a concern amongst communities when people were asked to rate the severity of this problem. Many people had no opinion about pornography restrictions' (Cth, 2011).

ASSESSING THE AUDITS

The end of the auditing appears to have been generally welcomed. The auditing process was widely seen as a confusing, poorly organised, unfunded, irrelevant and antiquated mode of deploying technology policy. Through discussions with a number of the actors and agencies concerned, some consistent themes emerged.

1. Operational complexity and confusion. There was substantial confusion amongst stakeholders and key actors as to the practical administrative process of the audits, and where

responsibility for these lay, whether in the computer centres, the shire offices, or the NT Library. This confusion was complicated by an 'in kind' administrative and logistical relationship between bodies such as shire councils and the NT Library, reflecting the broader complexity of service delivery in remote communities. For example, shires often provided an officer to assist maintenance of NT Library facilities for practical reasons (i.e. location). One shire officer indicated the shire did not perform audits in their locale because they did not deal with the relevant public access computers, which were on the NT Library network. Another shire officer indicated that because the shire paid NT Library for the internet (RIPIA) connection, it was the library's responsibility to administer and maintain the computers and networks. However, the shire had supplied employees to assist administering the computers in on the NT Library system for practical reasons. That said, the officer still assumed the responsibility for the audits belonged to NT Library. One shire officer even remarked with respect to audits, 'if they're [NT Library] not doing it, no one is'.

2. Lack of funding. The audit reports obtained indicated that neither ACC, nor the Australian Federal Police (AFP), had been provided any additional funding to perform their functions under the *NTNER Act 2007* (Cth) (ACC, 2008). One shire officer questioned the operability of the audit requirements without additional funding being provided to the shires. They noted no funding had been provided for 'the nuts and bolts' of the filtering or auditing processes, but there was an unwritten expectation that NT Library would cross-subsidise the audits. The issue of inadequate funding clearly led to a devolution of responsibility from relevant parties.

3. Non-compliance. The operational and funding difficulties were compounded by some resistance to the policy's administrative obligations. Some public servants saw these as an unwelcome burden, as unworkable or too onerous. We were informed that when the obligations were first introduced, library and knowledge centre employees attempted to keep a record of who came and used computers to comply with section 27. However, it was quickly found to be an unworkable system. We were told that a young woman who had the responsibility for maintaining the logs in one centre was unable to write down some names as it was forbidden under traditional law. The Northern Territory Library noted that it provides free internet connections to 40 locations around the Northern Territory, and 21 of those sites are operated through community good will and not managed by Northern Territory Library. There were no paid staff to manage the technology.

4. Audits and policy. From early in the process, the audit requirements were perceived as anachronistic. The spread of mobile technologies diminished the relevance of the desktop with internet connection. Shire officers questioned the point of auditing three unused computers in a library when smartphones were not subject to the same accountability measures, and were becoming increasingly available. The technology structure that the statutory requirements were attempting to regulate had been leap-frogged.

The audit records also show that there were no prosecutions, which brings into question the value of performing burdensome audits. When internet facilities were still being delivered through the library and knowledge centre model, the auditing provisions did impact on policy decisions because the Northern Territory Library needed to be able to reassure the Shires that they were capable of covering their filtering and auditing requirements. When a new model of service provision emerged based on Wi-Fi networks and the Open DNS filter, these issues ceased to be a concern. However, internet use in communities is still considered to be problematic by some residents, including many elders. Many of their concerns are better understood in terms of cyberbullying or cybersafety.

CONCLUSION

Altman and Hinkson write that during the Intervention prescribed communities were subjected to 'unprecedented levels of surveillance by an influx of transitory agents', including:

> police officers, tenancy officers, truancy officers, training officers, employment brokers, Centrelink officers, store licensers, and housing construction crews – but no badly needed dentists or mental health workers – all supposedly under the watchful gaze of the coordinating Government Business Manager, granted supreme statutory powers over those who come and go, displacing the authority of traditional owners under the abolished permit system (Altman & Hinkson, 2012/2013, p. 143).

The methods of surveillance described here were not covert but were carried out on the public stage, presented to mainstream media audiences as a 'state of emergency' that demanded tough and immediate action. The ICT surveillance avoided public scrutiny not because it was hidden, but because other, more overt tactics overshadowed it; the surveillance of 'publicly funded' computers and networks was less visible and immediate than the physical presence of military, police and bureaucratic officers in communities.

As we have explained, publicly funded computer facilities were the government's main strategy for addressing what was a significant digital divide at the time the intervention was launched. The decision to audit and monitor publicly funded computers therefore occurred in a paradigm where access through devices of this kind was likely to be the only viable form of internet and computer access for the target population. In the end, very little came of this exercise. Indecent material was handed over to police in two instances, the most serious of which appears to have been from a staff member rather than a public user, and no individuals or organisations were prosecuted.

The surveillance of computers under the Intervention, however flawed, was nevertheless a remarkable encroachment on internet freedom in Australia. It imposed criminal consequences for accessing content that was legal in other parts of the country, and imposed financial penalties for noncompliance on administrators as well as perpetrators. Measures that were justified on the grounds of stopping the flow of pornography into communities also became the vehicle through which criminal information of any kind could be detected and sent to policing entities.

The digital ecology in Indigenous communities has changed dramatically over the last decade, but questions relating to how these devices should properly be used in the Indigenous cultural and social context remain a serious concern for elders and other residents. Individuals and families are increasingly purchasing their own devices for use on publicly and commercially provided services. Most of these devices are not personal computers in their traditional form, but smartphones or tablets. As in the rest of Australia, there is a real need for users, parents, teachers, and community leaders to understand the positive and negative capabilities of these communication technologies. In particular, the sharing of devices appears to be leading to particular cybersafety issues, including inappropriate content, and privacy concerns. While some community-level programmes are attempting to teach people how to be 'cyber smart', the extent to which digital literacy can tackle these problems is debateable. For instance, the

response strategies of social media platforms (such as their uses of takedown notices) are not necessarily attuned to the particular communication practices and concerns of remote Aboriginal communities (Rennie, Hogan, & James, 2016).

The attempt to audit computers during the period of the Intervention was poorly designed. It was logistically complicated; its administrators were neither well supported nor committed to it; and the auditing technology was rudimentary. It contributed little to the wider objective of reducing family violence and abuse. In the wake of the Snowden revelations, the existence of far more sophisticated and comprehensive "bulk collection" systems for the surveillance of citizens is now well known. However, the technology of data collection is not its most important aspect. Indigenous communities remain particularly vulnerable to overreaching surveillance measures. The Intervention strategy was based upon communities' dependence on publicly funded computers. As low cost, mobile devices have been taken up, that dependence has substantially diminished, but the need for subsidised access to the internet remains for most communities.

It also remains the case that remote Indigenous communities have a great deal to gain from improved communications and online services in areas such as health, education and community services. The experience of the Intervention underlines the importance of transparency in how and for what purposes these new services collect and manage information. Without such clarity, the benefits of government initiatives to narrow the digital divide — and of course efforts in other sectors, from large corporates to civil society —will inevitably be compromised, and the programmes themselves may fail. [9]

REFERENCES

Altman, J. & Hinkson, M. (2012). Hope-less Futures. *Journal of Indigenous Policy*, *14*, 141-145.

Australia. Commonwealth Government. House of Representatives. (2007, August 7). *Parliamentary Debates*.

Australia. Commonwealth Government. (2009). *Policy Statement: Landmark Reform to the Welfare System, Reinstatement of the Racial Discrimination Act and Strengthening of the Northern Territory Emergency Response*.

Australia. Commonwealth Government. (2009a). *Future directions for the Northern Territory Emergency Response*.

Australia. Commonwealth Government. (2009b). *Report on the Northern Territory Emergency Response Redesign Consultations*.

Australia. Commonwealth Government. (2010). *Closing the Gap Monitoring Report July - December 2010 Part 2*.

Australia. Commonwealth Government. (2011). *Northern Territory Emergency Response: Evaluation Report*.

Australia. Commonwealth Government. (2011a). *Stronger Futures in the Northern Territory: Policy Statement*.

Australia. Department of Communications, Information Technology and the Arts. (2002). *Telecommunications Action Plan for Remote Communities: Report on the strategic study for improving telecommunications in remote communities*. Commonwealth of Australia, Canberra*.

Australia. Department of Communications, Information Technology and the Arts. (2005) *Networking the Nation: Evaluation of Outcomes and Impacts*. Commonwealth of Australia, Canberra.

Australia. Department of Families, Housing, Community Services and Indigenous Affairs & the Australian Crime Commission. (2007, July) *Memorandum of Understanding between the Commonwealth of Australia represented by the Department of Families, Community Services and Indigenous Affairs and the Australian Crime Commission*.

Australia. Department of Families, Housing, Community Services and Indigenous Affairs. (2009) *Northern Territory Emergency Response (NTER) Monitoring Report: Measuring Progress of NTER Activities July 2008 – December 2008 Part Two*.

Australia. Department of Families, Housing, Community Services and Indigenous Affairs (2009b), *Contract Number 45367033 between Commonwealth of Australia and Bridge Point Communications for The Provision of Contract Services in Relation to the Provision of PinPoint Auditor software and Information Technology services to support the audit of publicly funded computers*. FoI request number 12/13-048.

Australia. Parliament. Senate. Standing Committee on Legal and Constitutional Affairs (2007, August 10). *Official Hansard*.

Australia. Parliament. Senate. Standing Committee on Legal and Constitutional Affairs (2007a). *Social Security and Other Legislation Amendment (Welfare Payment Reform) Bill 2007 and four related bills concerning the Northern Territory National Emergency Response*. Retrieved from http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Completed%20inquiries/2004-07/nt_emergency/report/index

Australia. Parliament. Senate. Standing Committee on Legal and Constitutional Affairs (2008, February 18). *Australian Crime Commission: Question 2*. Retrieved from http://www.aph.gov.au/~/media/Estimates/Live/legcon_ctte/estimates/add_0708/ag/2.ashx

Australian Bureau of Statistics. (2007). File generated 1 September 2014 using 2006 Census of Population and Housing, Aboriginal and Torres Strait Islander Peoples (Indigenous) Profile, Based on Place of Usual Residence, by dwelling, Catalogue number 2002.0 – 2006 Community Profile Series

Australian Bureau of Statistics. (2007a). *Internet access by Indigenous people. Patterns of internet access in Australia, using 2006 Census data, Catalogue number 8146.0.55.001*, first issue.

Australian Bureau of Statistics. (2012). File generated 30 August 2012 using 2011 Census of Population and Housing, Aboriginal and Torres Strait Islander Peoples (Indigenous) Profile, Based on Place of Usual Residence, Catalogue number 2002.0 – 2011 Community Profile Series.

Australian Communications and Media Authority (2008). *Telecommunications in Remote Indigenous Communities*. Retrieved from http://www.acma.gov.au/theACMA/telecommunications-in-remote-indigenous-communities

Australian Crime Commission. (2008). *Letter from ACC to Dr Jeff Harmer, Secretary, Department of Families, Housing, Community Services and Indigenous Affairs, 'Forensic analysis of NTER Audit of publicly funded computers, June 2008'*. ACC Ref: 08/169847* FoI request number 12/13-048.

Australian Crime Commission. (2008a). *ACC analysis of NTNER audit of publicly funded computers, June 2008*. ACC Ref: 08/169847. FoI request number 12/13-048.

Australian Crime Commission. (2009). *ACC analysis of NTNER audit of publicly funded computers, December 2008*. ACC ref: 09/128526. FoI request number 12/13-048.

Australian Crime Commission. (2009a). *Letter from ACC to Dr Jeff Harmer, Secretary, Department of Families, Housing, Community Services and Indigenous Affairs, 'ACC Analysis of NTER Audit of Publicly funded computers, December 2008'*. ACC Ref 09/34999

Australian Crime Commission. (2009b). *ACC analysis of NTNER audit of publicly funded computers, December 2008 (additional information)*. ACC ref: 09/44106. FoI request number 12/13-048.

Australian Crime Commission. (2010). *Letter from ACC to Dr Jeff Harmer AO, Secretary, Department of Families, Housing, Community Services and Indigenous Affairs, 'ACC analysis of NTNER audit of publicly funded computers, December 2009 and June 2010'*. ACC Ref 10/111351. FoI request number 12/13-048.

Australian Crime Commission. (2010a). *ACC analysis of NTNER audit of publicly funded computers, December 2009 and June 2010*. FoI request number 12/13-048.

Australian Crime Commission. (2011). *Letter from ACC to Mr Finn Pratt PSM, Secretary, Department of Families, Housing, Community Services and Indigenous Affairs, 'ACC analysis of NTER audit of publicly funded computers – December 2011'*. ACC ref 11/79161. FoI request number 12/13-048.

Australian Crime Commission. (2011a). *ACC analysis of NTNER audit of publicly funded computers, December 2010*. FoI request number 12/13-048.

Australia. Government of the Northern Territory. (2007). *Ampe Akelyernemane Meke Mekarle "Little Children are Sacred": Report of the Northern Territory Board of Inquiry into the Protection of Aboriginal Children from Sexual Abuse*.

Bhatia, R. (2016, May 12). The inside story of Facebook's biggest setback, *The Guardian*. Retrieved from https://www.theguardian.com/technology/2016/may/12/facebook-free-basics-india-zuckerberg

Council of Australian Governments. (2009). *Closing the Gap: National Partnership Agreement on Remote Indigenous Public Internet Access*. Retrieved from http://www.federalfinancialrelations.gov.au/content/npa/other/closing_the_gap_remote_internet_access/national_partnership.pdf

Daly, A.E. (2005). Bridging the Digital Divide: The role of community online access centres in Indigenous communities. *Centre for Aboriginal Economic Policy Research Discussion Paper, No. 237/2005*. Canberra: Centre for Aboriginal Economic Policy Research.

Ewing S., Rennie E. & Thomas, J. (2014). Broadband Policy and Rural and Cultural Divides in Australia, in Kim Andreasson (Ed.) *Digital Divides: The New Challenges and Opportunities of e-Inclusion*. London: Taylor and Francis. (forthcoming).

Australia. Parliament. House of Representatives. (2007). *Explanatory Memorandum, Northern Territory National Emergency Response Act 2007* (Cth). Retrieved from http://www.austlii.edu.au/au/legis/cth/bill_em/ntnerb2007541/memo_0.html

Hinkson, M. & Altman J. (Eds.). (2010). *Culture Crisis: Anthropology and Politics in Aboriginal Australia*. Sydney: University of NSW Press.

Rennie, E., Crouch, A., Thomas, J. & Taylor, P. (2010). Beyond public access? Reconsidering broadband for remote Indigenous communities. *Communication, Politics and Culture*, *43*(1), 48-69.

Rennie, E., Hogan, E., Gregory, J., Crouch, A., Wright, A. & Thomas, J. (2016). *Internet on the Outstation: The digital divide and remote Aboriginal Communities*. Amsterdam: Institute of Network Cultures. Retrieved from http://networkcultures.org/blog/publication/no-19-internet-on-the-outstation-the-digital-divide-and-remote-aboriginal-communities/

Rennie, E., Hogan, E., & James, I. (2016). *Cyber-safety in remote Aboriginal Communities: First report*, Melbourne: Swinburne Institute for Social Research.

Stafford A. (2007, August 10). Howard Pitch for Family Vote with Internet Filter. *The Age*. Retrieved from http://www.theage.com.au/news/national/howard-pitch-for-family-vote-with-internet-filter/2007/08/10/1186530542829.html

FOOTNOTES

1. This is defined in section 4 of the NTNER 2007 (Cth). 'Prescribed areas' include any areas deemed so by a Commonwealth Minister, or any area covered by paragraph (a) of the definition of Aboriginal Land in subsection 3(1) of the Aboriginal Land Rights (Northern Territory) Act 1976 (NT) which includes any land held by a Land Trust for an estate in fee simple, or land the subject of a deed of grant held in escrow by a Land Council, as well as any areas that are expressly excluded under Schedule 1 of the Land Rights Act, as well as any land excluded for a grant for the purpose of a right of way (section 12(3)), or any Crown Land that is vested in the Northern Territory (section 3A).

2. The Families, Community Services and Indigenous Affairs and Other Legislation Amendment (Northern Territory National Emergency Response and Other Measures) Act 2007 (Cth) amended the Classification (Publications, Films and Computer Games) Act 1995 (NT) to include 'Part 10 – Material prohibited in prescribed areas'.

3. In the Northern Territory National Emergency Response Act 2007 (Cth).

4. The Families, Community Services and Indigenous Affairs and Other Legislation Amendment (Northern Territory National Emergency Response and Other Measures) Act 2007 (Cth) also amends the Australian Crime Commission Act 2002 (Cth) to include references to Indigenous violence or child abuse.

5. See Cth 2007b (Peter Webb), 93 where he suggests that the material in the relevant reports did not identify pornography on computers as a problem.

6. We cannot account for the differences between the number of computers audited as stated by FaHCSIA and the number of audit reports (presumably one per computer) as reported by the ACC and shown in table 1.

7. The Policy Statement (Cth, 2009) stated that although the auditing provisions would cease, continuing the measures would be preferred.

8. The penalties cited here were stated in the letter sent to organisations for the November 2011 audit, although it appears in retrospect that no civil penalties were ever levelled against responsible persons.

9. A recent instance in the corporate sector — Facebook's 'Free Basics' program in India — is a further, instructive example. For a detailed account, see Bhatia, 2016.