MEDIANZ • VOL 14 NO 2 • 2014
DOI: http://dx.doi.org/10.11157/medianz-vol14iss2id118

- EDITORIAL -

Special Issue: Surveillance, Copyright, Privacy

John Farnsworth, Kevin Fisher, Erika Pearson

Introduction

In December 2014, the New Zealand Government introduced legislation that strengthened the powers of its spy services, the Government Communications Security Bureau (GCSB), reduced civil liberties, and threatened to render some of its citizens stateless. These actions echo those in several Western jurisdictions, notably the US. Taken together, they point to the continued international intensification of state control over citizens through legislation and surveillance. These actions have been commonly legitimated by provoking moral panics. Since 9/11, it has been routinely accomplished by pointing to sometimes illusory global terrorist threats, most recently to the presence of Islamic State (IS) in New Zealand. What remains hidden behind these alarms, as the revelations from Wikileaks and Edward Snowden repeatedly demonstrate, is the expansion of state and corporate incursions into private lives using sophisticated digital techniques.

The Surveillance, Copyright, Privacy Conference

In New Zealand, these developments have largely gone uninvestigated. This prompted the first International conference on surveillance, copyright and privacy issues, held at the University of Otago in January 2014. The papers for this special issue are largely taken from its proceedings, although some have undergone considerable revision since then. The conference itself was lively, cross-disciplinary and well-attended. Yet its

John Farnsworth is associated with the Media, Film and Communications Department at the University of Otago. He is also a registered psychotherapist in private practice. Recent papers include work on new technologies, mobile devices, psychoanalysis, ethnography and methodology.
Kevin Fisher is a Senior Lecturer in the Department of Media, Film & Communication at the University of Otago. His research interests include phenomenology, intermediality, indigenous theory, and documentary.
Erika Pearson is a Senior Lecturer in the Department of Media, Film & Communication at the University of Otago. Her research interests cover several aspects of Internet culture, including virtual communities, fan culture, trust networks, hacktivism and political activism online, complexity in virtual social networks, and notions of social capital in cyberspace.

vibrancy was offset by two factors: new revelations since the event regarding the depth of the problem, and the clear recognition that online surveillance, like rust, never sleeps. This was one of the gloomiest themes to emerge, with widespread agreement that many ordinary rights have been muted or removed by governments and big corporations.

Three days of intensive discussion amongst forty-one participants, swelling to a hundred for each of the four public keynote sessions. Each session strung together surveillance, privacy and copyright issues; and saw hacktivists engaged with academics, policy analysts debating cryptographers, and former spies questioning legal experts.

The conference threw into sharp relief the inequities and injustices of recent Internet legislation. As journalist Nicky Hager demonstrated, New Zealand is as complicit as anywhere. This has been not just through the Search and Surveillance Act 2012, or subsequent legislation, but also in its role as long-standing accomplice of the US Government through the long-running Five Eyes programme and the Waihopa Echelon base.

Privacy was a second prominent theme. A significant issue, often lost in public debate, is the difference between privacy and anonymity. Vikram Kumar, the ex-CEO of Mega clarified the distinction by describing how his company uses encrypted cloud storage to ensure privacy but not anonymity. Mega, he insisted, responds to reasonable requests to investigate illegal activity by site users who have violated privacy to gain anonymity.

Graham Murdock's keynote address highlighted the dense entanglement of state and corporate interests. As he and many presenters emphasised, data-mining lies at the heart of this issue: Big Data's use in predicting often invisible patterns of behaviour. Such data-mining compounds staggering amounts of digital traffic, sifting it through keywords and tags for markers of significance. But this ceaseless activity remains both largely ungoverned and highly obscure.

Hager emphasised that, nonetheless, any single individual has little chance of interception; but Judge Harvey also raised important civil liberties implications of state 'fishing expeditions'. He reminded his audience that in earlier days phone tapping carried tough legal restrictions and penalties, a dramatic difference to the open season for mass monitoring now in place.

In the private sphere, the conference learnt how Big Data allows corporations, from casinos to online video companies, to anticipate behaviour before consumers know it themselves. This facilitates the shaping of spending patterns and consumer behaviour without any consumer awareness. Big Data forecasts when employees may quit their job or enables airlines to change online prices instantly, based on closely forecasting seat demand.

In the sessions, Labour MP Clare Curran highlighted the growing lack of protection against state or private intrusion. She proposed a new digital Bill of Rights to address this, though Labour's election defeat makes its development problematic.

Similar debates circulated around copyright, where, it was argued, the better protection it affords corporations than creators they represent lies at the heart of online piracy wars. These tensions have produced alternative strategies of Copyleft and the Creative Commons.

Underlying all these discussions was the question of an open Internet. Hager suggested it may remain open, though it has never been secure; other speakers reminded delegates that, open or not, it runs in parallel to other, inaccessible Internets such as Darknet. Either way, conference discussion suggested the open Internet may well crumble. Individual states, such as China, have reacted to the Edward Snowden revelations, by continually seeking to limit or manage the Internet.

The Current Environment

In some ways, the conference acted as a lens for events that have continued to unfold. In New Zealand, the general election debates were dominated by discussions of privacy, data sovereignty, free trade agreements and copyright. Much of this was in direct response to the release of Nicky Hager's book, *Dirty Politics*, which had received its gestation through the conference. It was also in response to the extraordinary online conference in Auckland, also known as the 'Moment of Truth', attended by Glen Greenwald, Julian Assange and Edward Snowden. The political fallout of domestic spying allegations claimed cabinet figures, bloggers and others, though December 2014 reports on the New Zealand Security and Intelligence Service (NZSIS) hardly suggest this will lead to more stringent oversight of state spying or surveillance activity.

It was not just government and state institutions that had a busy year. In the commercial sphere, questions were raised over privacy of users when major social media networks let slip that they had been studying social media use, commercializing user data, and even conducting experiments on user 'social graphs', manipulating the information they saw and studying how it affected users behaviour and even mood. Algorithmic approaches to social data saw data mining techniques dig ever deeper. The boundaries of privacy and anonymity spent the year in flux, being redrawn as much by commercial interests as by shifting social and cultural practices.

Even the Darknet was not immune to these changes, with major underground sites like Silk Road and Utopia being targeted by international law enforcement, using the same tools as the users of those sites to gather evidence and target suspects. It is still to be seen whether these arrests raise the profile of the Darknets with more and more users, or whether such sites are driven deeper, further out of reach of users who perhaps do not have the skills or knowledge to access them and the hidden spaces they represent.

Copyright continued to be a contentious issue, with all the players, creator/consumers and corporations working both with and against each other to forge new practices of creation that made sense in the digital age. Throughout 2014, copyright and 'copyleft' debates highlighted the tensions produced by new technologies, and the trend seemed to be to move away from containers of content (protected by things like DRM systems) towards copyright and licensing practices on the content itself, with significant questions as to how to protect the value of increasingly ephemeral content while also adapting to a digital ecosystem. This has played out in music (for example with major artists leaving Spotify over questions of payment), television and movies (represented by Netflix's continually increasing market share), and even publishing with the growing movement towards open access in books and publishing as well as coding and infrastructure development.

The digital media infrastructure itself has also been shaken, with bugs in the code revealing just how widespread the code has become, and just how reliant we are on increasingly hidden and unremarked-upon systems maintained by a relatively tiny number of individuals, mostly volunteers. As the recent New Zealand elections and other activities around the world have forced us to face, most users do not think about the systems, codes, laws, commercial imperatives and political decisions that shape our digital environment. This makes the ideas and issues raised in this special edition of *MEDIANZ* that much more important as we make decisions that will shape the digital world around us for years to come.

Contributions

The themes of the conference were surveillance, copyright and privacy but, in this issue, these are cross-cut by several others. Two in particular stand out: one is a consistent emphasis on a sustained critical scrutiny of surveillance, copyright and privacy concerns. It is worked out differently across each paper, but is common to most. A second theme highlights the pragmatics of the response to such concerns: how the processes and modes of engagement with state and corporate surveillance actually take place. This runs across Hager's opening paper detailing state mass surveillance, Murdock on the erosion of citizenship, Taffel on anti-surveillance software, Farnsworth on digital mimicry, McGuire on Creative Commons, and Harvey's closing paper on legislative responses to surveillance challenges.

The special issue begins with essays by two keynote speakers, Nicky Hager and Professor Graham Murdock. Hager traces the history of New Zealand's involvement with Anglo-American electronic surveillance systems since WWII and the rapid development of its national intelligence agency: the GCSB within the global Five Eyes Network. Murdock takes a longer historical view and focuses more on the Anglo-American context. He locates the historical precursors of global systems in pre-modern practices of census taking and the formalisation of state citizenship.

Both Hager and Murdock describe a transition between two eras of surveillance. The first justified itself as a necessary response to exigent global threats (such as WWII). In the second, surveillance becomes legitimated as a permanent, proactive tool of government. In this new era, states claim the need to manage internal and external threats—targeting not just enemy states but also 'friendly' trading partners, foreign and domestic citizens, as well as private corporations. The correlative shift from 'human intelligence' to 'signals intelligence' has also, crucially, changed the focus from targeted surveillance to mass monitoring of entire populations, as the Snowden revelations confirm.

Hager details how these systems function, leading the reader through diagrams released by Snowden and others. He details how surveillance works around state sovereignty, commonly by nominating a state intelligence agency to spy on its own citizens. This, Hager claims, was the case with Kim Dotcom. Whilst Hager insists most citizens need not worry about individual intrusion, his main concern is how active political participation is deterred by the public awareness of such systems and the fear of being targeted. Murdock expresses similar concerns. He reflects on the semantic games that state agencies employ in subjecting their own citizenry to otherwise illegal forms of monitoring. He further argues that 'saturation surveillance' is doing more than simply deterring political participation: its ambient presence threatens to install a new social order, one bearing a greater resemblance to neo-feudalism than participatory democracy. In short, he raises the spectre of an emerging digital serfdom.

Murdock situates the political effects of surveillance within late capitalism: the 20th Century convergence of intelligence and marketing methodologies, and the resulting conflation of citizen and consumer. He traces a series of widespread transformations from implicit surveillance within public institutions to explicit tracking of consumer behaviours, all of this made possible by the state and corporate harvesting of metadata. In terms of social justice, Murdock explores how for the citizen, like the consumer, the focus becomes not just upon what people have done but on what they might do. The implications, argues Murdock, are already evident in the changing legislation around 'terror' and copyright and how these terms are constructed.

The articles by Sy Taffel and Simon Ryan work through the theories of Bernard Stiegler to stage their critiques of surveillance practices. Both draw on his concepts of a libidinal economy and technicity: the primacy of technology in constituting what it means to be human. The Internet, and the surveillance software that monitors it, act as emerging forms of this technicity; together, they exemplify Stiegler's concept of technology as pharmakon, by which he means technology as both poison and remedy. From here, they explore the ambivalence of the Internet—holding out the possibility of developing collaborative 'cures' in the form of 'associative milieus' and 'economies of contribution', which nevertheless always remain vulnerable to the 'poison' of capture by state and corporate interests.

This enables Taffel, reading through Stiegler, to critique the celebration of Internet 'open-ness' as naïve, given its neglect of how essential privacy and anonymity are for effective political action and dissent. Echoing Hager, he reminds us that temporary anonymity was critical for the activities of Snowden and Manning. He further points out that the flipside of 'openness' is a type of coerced, simulated transparency intrinsic to the 'societies of control' critiqued by Deleuze. Openness, he argues, is not a default setting that guarantees privacy; on the contrary, the right to privacy must be constantly won on a plane of shifting conflicts. To this end, Taffel provides detailed analyses of several software applications developed to preserve anonymity and the collectives these sustain.

Ryan touches on many of Taffel's concerns but outlines Stiegler's thought in more detail. In particular, he focuses on the possibility of developing what Stiegler describes as a 'politics of care'. This is the 'cure' dimension of the pharmakon: the issue of how to engage with an increasingly 'addictogenic' society where consciousness itself becomes a commodity through the capacity of digital, online technologies to persistently harness attention. This 'always-on', pervasive software threatens to disindividuate humans as political beings and to create new, readily surveilled subjects and social formations. The dilemma, for Ryan, is whether an alternate economy of contribution can still grow. Such a possibility is both within and against what he describes, following Stiegler, as the contemporary hypercapitalist economy of consumption. Like Hager, his key concern involves the power of mass surveillance to discourage cultural and political participation.

John Farnsworth takes up the ambivalence of the Internet explored by Taffel and Ryan in yet another way. He investigates the dual role of digital mimicry. As he demonstrates, mimicry has a complex relationship with power, an insight he elaborates by drawing on Homi Bhaba's account of the relationship between coloniser and colonized. In the digital arena, Farnsworth describes how sophisticated practices of camouflage, and shifts between simulation and deception, colonise digital technologies in just the same way as Babha describes domination in postcolonial societies. Yet, like Taffel and Ryan, mimicry can be both poison and cure, and Farnsworth illustrates this through detailed examples. They range from collective innovations in algorithmic swarming and new robotic technologies to the way text mining and predictive analytics allow microscopic tracking of individual and collective behaviours. Such tracking and predicting extends to simulating and reproducing even unconscious human gestural communication; deployed across mobile devices, from predictive text to targeted ads, they generate both emancipatory and exploitative possibilities.

Mark McGuire's essay is the only one to focus specifically on copyright issues. He concentrates on Creative Commons licensing in New Zealand, and focuses on the tensions surrounding property rights and the right to share new work experienced by a variety of institutions and practitioners. Drawing on the work of Lessig, McGuire describes how, within the virtual commons, the digitization of cultural artefacts poses a challenge to copyright by making the content layer distinct from the physical and code layers of any medium. Yet, the digital era has witnessed redoubled attempts at control, principally through a tightening of US copyright laws, and compliance pressure applied to US trading partners such as New Zealand. McGuire details the *ad hoc* and unworkable legislation that has resulted, but he also describes innovative New Zealand responses to copyright challenges through the use of Creative Commons licencing. As with earlier contributors, McGuire's essay highlights the ambivalent, constantly contested nature of emerging digital developments.

The final essay, by Internet law expert Judge David Harvey highlights legislative issues around electronic surveillance in New Zealand. Harvey analyses, in particular, the Search and Surveillance Act 2012 and how this has been applied specifically to 'cyber-searches'. In a wide-ranging, but intricately detailed discussion, he demonstrates how new digital technologies challenge prevailing legal assumptions about the objects and processes of search and seizure. He demonstrates how electronic information differs fundamentally to 'hard copy' using illustrations such as the 'filing cabinet analogy'. He also shows how legal definitions have fallen behind in recognizing this. Calling on McLuhan's concept of 'rear view mirror' thinking, he describes the bleak irony of authorities able to elude practical and legal obstacles more easily now than they could before by treating electronic communications as if they were hard copy. In this way, he also laments the fact that technology seems to determining search and seizure practice rather than the law.

Harvey's essay highlights the two themes common across the papers. First, they offer a persistent critical inquiry into the implications of digital technologies and surveillance: how these affect ordinary citizens and also rework civil and subjective life. Second, each essay describes in detail how these transformations are effected in the overlapping spheres of surveillance, copyright and privacy. Each, in its own way, also addresses the ongoing ambiguities of digital communications within network societies. Taken together, they emphasise the ongoing centrality, for the public good, of contesting state and corporate surveillance, and of creating alternative domains for collective practice and innovation.