www.crimejusticejournal.com IJCJ&SD 2013 **2**(3): 105-119 ISSN 2202–8005


# Global Policing and the Case of Kim Dotcom

**Darren Palmer**
Deakin University, Australia

**Ian J Warren**
Deakin University, Australia

**Abstract**

In early 2012, 76 heavily armed police conducted a raid on a house in Auckland, New Zealand. The targets were Kim Dotcom, a German national with a NZ residency visa, and several colleagues affiliated with Megaupload, an online subscription-based peer-to-peer (P2P) file sharing facility. The alleged offences involved facilitating unlawful file sharing and United States federal criminal copyright violations. Following the raid, several court cases provide valuable insights into emerging 'global policing' practices (Bowling and Sheptycki 2012) based on communications between sovereign enforcement agencies. This article uses these cases to explore the growth of 'extraterritorial' police powers that operate 'across borders' (Nadelmann 1993) as part of several broader transformations of global policing in the digital age.

**Keywords**

Global policing, extra territoriality, sovereignty, piracy, file sharing, surveillance.

## Introduction

On 20 January 2012, New Zealand (NZ) Police conducted a 'dramatic' raid dubbed 'Operation Debut' (Amsterdam and Rothken 2013: 7, 14) on a $30 million mansion in the Auckland suburb of Coatesville. Their target was the eponymously named Kim Dotcom, owner and developer of file sharing site Megaupload. Activities on this site were subject to extensive surveillance by United States (US) Federal Bureau of Investigation (FBI) officials, as well as NZ Police and the NZ Government Communications Security Bureau (GCSB). The raid involved 76 NZ Police officers, including members of the Armed Offender's Squad and Special Tactics Group equipped with rifles and semi-automatic weapons, several police dogs and two helicopters (Editorial 2012). Dotcom, Finn Batato, Bram van der Kolk and Mathias Ortmann were arrested at the house and imprisoned pending extradition to the US. Simultaneous raids were also conducted in Australia, the Philippines, Hong Kong, Germany, Canada, the Netherlands, Britain and the US. A NZ Police liaison officer in Washington indicated '(f)eedback on the New Zealand operation has

been extremely positive from our international law enforcement partners including the FBI and the US Department of Justice' (APNZ 2012).

Two suspects eventually spent seven months 'detained in a foreign country away from their families and ordinary places of residence' (United States of America v Dotcom #2 [2012] NZHC 1353 at para 23) before being granted bail. Dotcom was subject to several restrictive bail conditions including electronic monitoring (United States of America v Dotcom #1 [2012] NZHC 328 at para 41). Around $US175 million of Megaupload business assets was immediately frozen, $NZ200 million of Dotcom's personal assets including cash, several luxury cars, other property and $NZ10 million of government bonds were confiscated (Fisher 2012), and up to 150 terabytes of computer data located at the house were taken, cloned and conveyed to the FBI. US officials have made an extradition request supported by a 72-page federal indictment alleging several offences involving Dotcom and Megaupload related to 'breach of copyright, racketeering and money laundering' (Attorney-General in respect of the GCSB v Dotcom, Batato, Ortmann and van der Kolk (hereafter A-G re GCSB v Dotcom et al.) [2013] NZCA 43 at para 6; Amsterdam and Rothken 2013: 15).

Of itself, this considerable use of police resources and force against a person with no apparent involvement in violent behaviour warrants further scrutiny in light of the 'priorities, policies, practices and accountability' associated with transnational policing arrangements (Bowling and Sheptycki 2012: 1). However our purpose is to interrogate the enforcement processes in this case, as a measure of several key transformations in global policing (Bowling and Sheptycki 2012; Palmer et al. 2012). Specifically, concern over the extension of historical offences such as copyright breaches to regulate new forms of digital crime that transcend conventional sovereign borders has contributed to the extensive growth of 'extraterritorial' law enforcement (Nadelmann 1993). The Kim Dotcom saga reveals several accountability deficits associated with emerging international police cooperation, surveillance and extraterritorial law enforcement initiatives.

The initial identification of Megaupload as a potential site for US copyright piracy violations commenced in the US, where a Grand Jury hearing in the state of West Virginia confirmed there was sufficient evidence to issue US federal indictments against Dotcom. This compelled US authorities to seek the assistance of NZ enforcement agencies to gather additional evidence to assist with the extradition and prosecution of Dotcom and his associates. Any US prosecution depended on the mutual assistance of NZ Police and GCSB in conducting relevant surveillance, arrests and in seizing evidence under NZ law. However, the process has not been as seamless as either US nor NZ law enforcement agencies had hoped, and promises to take several years to formally resolve. This is partially due to the significant financial, legal and intellectual resources Dotcom has been able to employ to challenge these global policing practices. Before documenting the tensions to global policing revealed in this case, we situate Dotcom's activities within a broader movement towards the expansion of traditional notions of copyright to criminalise certain trans-sovereign online information flows.

## Internet piracy as global crime

An ongoing problem associated with global communication flows within the World Wide Web involves the ambiguous proprietary status of digital imagery. As far back as the early twentieth century, innovative uses of photographic and cinematographic technologies enabled the unlawful copying and smuggling of banned films across national borders (Warren 2005). The transnational reach of digital communications, often through subscription platforms specifically engineered to share personal information, magnifies the challenges for traditional notions of intellectual property law that sought to protect revenue derived from the production of books, artworks, moving pictures and photographs in hardcopy form. The capacity to copy and disseminate digital representations of original works enables contemporary forms of copyright

piracy to transcend established sovereign laws and enforcement processes (Yar 2005). The financial stakes are considerable, with estimates suggesting the net annual costs of illegally downloaded films, television and music content by Australian internet users is around $A900 million (McMahon 2011). These issues can only be reconciled by balancing:

> ... intellectual property rights and human rights (to privacy and freedom of expression) … [and] multiple challenges, modifications, exemptions and limitations to a universal and strong form of property rights in ideas, in principle and in enforcement (David 2010: 5).

Perhaps the most significant factor associated with online piracy is the development of subscription-based peer-to-peer (P2P) file sharing, social networking and cloud computing platforms enabling users to exchange and access the personal files of other registered users. In the current 'global intellectual property rights regime' (David 2010: 5) the scale of copyright violations that occur through P2P or cloud computing remains unknown. However, these platforms generate extensive concern amongst the entertainment industry. While some copyright holders have introduced technical measures – such as 'cyberlockers' – to prevent the illegal duplication, downloading or sharing of protected works, these measures are often easily subverted or have limited impact in curbing online piracy (Lauinger et al. 2013). The entertainment industry favours prohibition, heavy regulation or increased surveillance by law enforcement agencies and major film, television and music production companies, to prevent revenue losses to performers from the sharing of illegally duplicated files through multi-user P2P platforms.

Traditionally, alleged breaches of intellectual property law involved private claims initiated by artists or producers of original musical, film and television works (Marshall 2002; Mazzone 2011). However, the digital age has intensified criminalisation of online piracy and certain modes of P2P file sharing (David 2010). Law enforcement agencies in the UK (SOCA 2013), Australia (ACC 2011: 73-75) and the US identify intellectual property crime, online piracy and the production of counterfeit hardcopies of films and music, as significant organised crime problems with potential links to terrorist activity (David 2010: 97-100). Criminalisation of these behaviours is tied to the 'transformation of the language' (Bowling and Sheptycki 2013: 35) of transnational wrongdoing that has emerged in various global institutions and official United Nations reports since the 1970s. While initial forms of global criminalisation focused largely on the 'trans-boundary economic and social effects' of Western corporate business activities in developing nations, more recently the focus has shifted to protecting developed Western nations from the threats of transnational organised crime, drug trafficking and terrorist activities. These concerns are frequently 'scripted by transnational policing actors' through networks promoting highly selective national law enforcement interests (Bowling and Sheptycki 2013: 34-38; Deflem 2004) within a global regulatory framework increasingly sympathetic to governance through crime (Findlay 2008).

Regardless of the credibility of arguments linking piracy to organised crime and terrorism, they occur in a political climate that favours the expansion of criminal laws and enhanced global policing networks targeting individuals engaging in various activities that are potentially illegal in one jurisdiction regardless of their geographic location. The expansion of extraterritorial criminal laws and enforcement methods has arguably been most notable in the area of illegal drug trafficking (Andreas and Nadelman 2006; Costa 2004; Kontorovic 2009), and occurs either in conjunction with or independently of bi- and multi-lateral treaty requirements. In the financially lucrative and highly technical world of the internet, the extraterritorial enforcement of sovereign laws criminalising 'intellectual property piracy' (Wall and Yar 2010: 268) presents significant regulatory challenges in a borderless digital economy (Ku 2002). Technical measures enabling law enforcement agencies located in one nation to close down websites, confiscate any user's digital information or undertake online surveillance and data mining operations beyond

their own jurisdictional borders, raise numerous questions regarding extraterritorial policing activities that are seldom addressed by global criminal prohibitions on internet piracy. This case study allows us to explore these issues in detail via the extensive body of NZ court rulings examining the legal dimensions of local policing responses to US requests for investigative assistance into the allegedly criminal activities of Kim Dotcom and Megaupload.

**Kim Dotcom**

Kim 'Schmitz' Dotcom is a German national holding a residency visa in NZ. Dotcom developed and managed various businesses associated with Megaupload, a cloud computing platform allowing registered users to share digital photographs, music and films with other subscribed users. As with many social networking sites, the platform has significant potential to facilitate both intentional and innocent copyright breaches on a global scale.

The US FBI viewed Megaupload as a possible site for illegally sharing pirated films, music and television programs. After preliminary investigations, a Grand Jury in West Virginia determined there was sufficient evidence gathered in the US, including 10 million intercepted emails, 'voluminous financial records obtained from a number of different countries' and data contained in rented servers located in the US (United States of America v Dotcom #2 [2012] NZHC 1353 at paras 19-20), to support federal criminal indictments alleging 'breach of copyright, conspiracy to breach copyright, conspiracy to racketeer and money laundering' (Dotcom v Attorney-General #1 [2012] NZHC 1494 at para 10). This combination of charges targets the unlawful profits from site subscribers and other Megaupload revenue streams that were linked to alleged criminal copyright violations under US law. Therefore, even if Megaupload developers or site administrators committed no copyright violations *per se*, the platform could facilitate breaches of US federal law by other registered third-party users regardless of their geographic location (Amsterdam and Rothken 2013: 19-23).

Prior to the West Virginia Grand Jury ruling on 5 January 2012, FBI officials worked informally with NZ Police to gather preliminary evidence to support their allegations. These arrangements were formalised through a mutual assistance request from the FBI to the NZ Attorney-General once the indictments were approved in the US. Mutual assistance legislation is commonly enacted in most jurisdictions under international treaty requirements (Joutsen 2005) to facilitate transnational police investigations. The formal request sought the collection and transfer of any additional 'evidence, fruits, and instrumentalities of the crimes being investigated' (Dotcom v Attorney-General #1 [2012] NZHC 1494 at para 19), including physical property such as computers, hard drives and financial statements related to Dotcom or the Megaupload businesses, as well as statements from any witnesses located in NZ. On 19 January 2012, a NZ District Court Judge approved search warrants drafted in these general terms. On the same day the US Department of Justice closed down all Megaupload servers, which were physically located in Hong Kong.

The scale of this cross-national criminal investigation is matched by the flurry of proceedings in NZ courts challenging the legality of the raids, the seizure of computers, hard drives and personal property by NZ police, and the subsequent cloning and transfer of digital evidence to US authorities. Between 29 February 2012 and 9 April 2013, 13 major NZ court rulings examined whether Dotcom has the right to access details about any information transferred to the US to assist in preparing arguments for an extradition hearing and any subsequent US criminal proceedings. An additional series of legal claims challenged the validity of asset confiscation orders under proceeds of crime proceedings that commenced in an Eastern Virginia District Court, then were registered by the Commissioner of the NZ Police under a High Court ruling (Commissioner of Police v Dotcom #1 [2012] NZHC 634; Commissioner of Police v Dotcom #2 [2012] NZHC 2190). This allowed NZ authorities to sell any seized assets associated with Megaupload. The discussion below focuses on three sites of legal dispute relating to NZ

enforcement activities associated with the extraterritorial police investigation into Kim Dotcom: the legality of the search warrant; the disclosure of evidence seized in NZ and transferred to US authorities; and a related claim under the *NZ Bill of Rights Act 1990* seeking compensatory damages for unlawful NZ enforcement and surveillance activity.

**Challenging the NZ search warrant**

Legal challenges to the validity of the search warrants and Dotcom's claims for disclosure of evidence transferred to US authorities are interrelated. In a lengthy ruling, Chief Justice Winkelmann declared the warrants were legally invalid under NZ law because they did not mention the specific crimes or types of evidence that could be seized by NZ Police (Dotcom v Attorney-General #1 [2012] NZHC 1494). Although initially endorsed under NZ law and in line with the FBI's mutual assistance request, the broad drafting of the warrant did not require NZ Police to distinguish Dotcom's personal information from any specific evidence directly relevant to the US indictments. Evidence from a warrant later declared invalid is admissible in US criminal trials if police acted in 'good faith' during the enforcement operation (Dawson 1982: 525-30). A similar discretion exists under NZ law, even if a search related to a defective warrant is later declared 'unreasonable' (s. 21, *NZ Bill of Rights Act 1990*; New Zealand Law Commission 2007: 126). These vagaries in the rules of evidence may validate intrusive 'fishing' exercises in the execution of broad or imprecise warrants.

A further question involves the legality of the transfer of any data to US investigators by NZ Police under the terms of the *Mutual Assistance in Criminal Matters Act 1992 (NZ) (MACMA)* (A-G re GCSB v Dotcom et al. [2013] NZCA 43 para 58). All data from computers and hard drives seized during the raid were cloned by NZ Police, then transferred to the FBI. This was contrary to an express directive from the NZ Solicitor-General to retain the evidence pending a NZ court hearing to determine which specific items of evidence could be lawfully provided to US authorities (s. 49, *MACMA 1992*). This unlawful global policing practice was only discovered in judicial review proceedings. That the NZ Police could simply ignore the chief law officer of the country is itself stunning. That such behaviour was only discovered by subsequent judicial review highlights the lack of rigorous procedural scrutiny and accountability for global policing investigations short of extensive legal proceedings after the event.

Chief Justice Winkelmann ordered any clones of digital hard drives containing personal information irrelevant to the US indictments be returned to NZ in light of this breach and the invalidity of the search warrants (A-G re GCSB v Dotcom et al. [2013] NZCA 43 at para 11). A subsequent ruling has affirmed original and cloned data collected during the raid under the MACMA arrangement were unlawfully obtained. As a result, NZ Police must provide a full audit of all information seized and transferred to US officials, all material irrelevant to the indictments is to be returned to Dotcom, and any cloned information in the possession of US law enforcement agencies is to be destroyed (Dotcom v Attorney-General #4 [2013] NZHC 1269).

**Challenging extradition and the disclosure of US evidence**

Kim Dotcom has also sought the disclosure of specific evidence held by US enforcement authorities to assist his preparations for an extradition hearing in NZ and any subsequent US criminal proceedings. US authorities have resisted these requests due to fears disclosure will prejudice the prosecution case. A Record of the Case must summarise the allegations in the indictment and provide sufficient detail of evidence to sustain the extradition request. Dotcom argued the failure to allow sufficient disclosure compromises principles of fairness associated with criminal trials (ss. 24-25, *NZ Bill of Rights Act 1990*). This argument was rejected, as the procedural requirements for extradition hearings 'are not of a scale that would be afforded in a full hearing [trial] to determine whether a charge is proved' (United States of America v Dotcom #3 [2012] NZHC 2076 at para 119). However, extradition hearings are a judicial process requiring partial disclosure under a broad reading of section 27 of the *NZ Bill of Rights Act 1990*,

which applies to administrative processes. Unless some disclosure is permitted to enable preparations for the extradition hearing, an applicant:

> will be significantly constrained in his or her ability to participate in the hearing, and the requesting state will have a significant advantage in terms of access to information (United States of America v Dotcom #3 [2012] NZHC 2076 at para 119).

US law does not permit extensive pre-trial disclosure of prosecution evidence until domestic proceedings have commenced. This means Dotcom will only become fully aware of the details of US evidence if he is formally extradited from NZ. After almost a year of legal consideration, on 1 March 2013 the NZ High Court overturned a previous order for extensive pre-trial disclosure. This means Dotcom is only able to access summaries of evidence in the Record of the Case prepared by US authorities to establish the case for extradition, with additional evidence only to be disclosed if the NZ extradition hearing identifies 'specified items of inherently cogent evidence' warrant additional disclosure (United States of America v Dotcom #4 [2013] NZHC 38 at para 110).

The shift in legal standards associated with the disclosure of evidence under a defective warrant illustrates a broader shift in the law of extradition. Rather than the disclosure of compelling *prima facie* evidence that commonly supports criminal charges during a committal hearing, the NZ High Court ruling reinforces a growing trend towards 'relaxed' legal requirements associated with extradition proceedings (Nicholls et al. 2007). The demands of global policing and mutual assistance requests contribute to diluted legal standards relating to search and seizure, extradition and information disclosure, and highlights the potential for extraterritorial investigations to influence legal developments in other nations in favour of selective transnational law enforcement objectives (Bowling and Sheptycki 2012: 41-2). These processes have significant potential to compromise the preparation of any defence to extradition proceedings or an offshore criminal indictment, even though a disclosure order technically has no extraterritorial effect as the nation challenging the ruling will do so directly in a foreign court (United States of America v Dotcom #3 [2012] NZHC 2076 at para 119).

**Compensation under the *NZ Bill of Rights Act 1990***

After ruling the search warrants were invalid, Chief Justice Winkelmann suggested the unreasonable search and seizure (s. 21, *NZ Bill of Rights Act 1990*; Dotcom v Attorney-General #1 [2012] NZHC 1494 at paras 89 and 145) could be open to a common law claim for compensation (Smillie 1994). This issue was not raised by either party and only emerged after several teleconferences and the exchange of memoranda during proceedings. Dotcom and one co-accused were allowed to add this claim with qualified support from NZ Crown representatives. The claim seeks acknowledgement that the conduct of NZ Police during the raid warranted damages for:

> … emotional harm, the cost of reinstating electronic componentry at one of the properties searched, the cost of repairing damage to the properties and the costs incurred by the respondents in attempting to obtain access to the information stored on the computer equipment that had been seized (A-G re GCSB v Dotcom et al. [2013] NZCA 43 at para 17).

Common law remedies for violations of the *NZ Bill of Rights Act 1990* provide 'vindication … compensation and denunciation' for the unlawful actions of government agencies (A-G re GCSB v Dotcom et al. [2013] NZCA 43 at para 18 and note 21) not otherwise covered by express remedies clauses under enabling legislation or other administrative provisions (referred to as 'Baigent's compensation', see Simpson v Attorney-General (Baigent's case) [1994] 2 NZLR 667;

New Zealand Law Commission 1997). During hearings in August 2012 to determine the legality of the warrants, the GCSB admitted to conducting illegal surveillance on two co-defendants who held residency visas in NZ and were entitled to legal protection under the *NZ Bill of Rights Act 1990*. Once these admissions were made, the GCSB and NZ Attorney-General were listed as co-defendants in an amended Bill of Rights compensation claim endorsed by Chief Justice Winkelmann on 5 December 2012 (Dotcom v Attorney-General #3 [2012] NZHC 3268).

The Court of Appeal acknowledged the 'present case has been characterised by unforeseen disclosures of information' (A-G re GCSB v Dotcom et al. [2013] NZCA 43 at para 50), but allowed the GCSB to be included as co-defendants despite objections from the Crown regarding the availability of financial compensation for any procedural violations. Significantly, arguments during this case revealed breaches that generated public admissions from the GCSB relating to unlawful surveillance activity targeting Dotcom, his business associates and their respective families that was subsequently conveyed to NZ Police to assist their investigations. This has generated additional claims seeking disclosure of this information and details of any intelligence-sharing agreements between the NZ Police and GCSB, including the dates and times any unlawful surveillance was conducted. These claims extend to any information provided to 'other members of Echelon/"Five Eyes"', a signals intelligence sharing arrangement involving the 'five eyes' of the US, Canada, Australia, NZ and the UK, and surveillance data conveyed to 'any United States authority' (A-G re GCSB v Dotcom et al. [2013] NZCA 43 at para 53). The court accepted Crown submissions that disclosure of any information about relatives affiliated with Megaupload's business could compromise the integrity of lawfully intercepted intelligence and was unlikely to have been forwarded to NZ Police.

Both the NZ Police and the GCSB have accepted legal responsibility for the unlawful surveillance and Dotcom's entitlement to Baigent's compensation (A-G re GCSB v Dotcom et al. [2013] NZCA 43 at para 26). The amount of damages was to be determined prior to the commencement of extradition proceedings (Bayer 2013). The hearing was originally scheduled for August 2013, but at the time of writing had yet to commence due to unspecified delays. When ruling on the extradition request, the NZ High Court will consider the scale of the unlawful surveillance and information sharing between GCSB, NZ Police and other members of the 'Echelon group'. The outcome will be crucial to any subsequent US criminal proceedings against Megaupload and the related disclosure of information obtained by NZ authorities under the defective warrants that was transferred to US officials under the *MACMA 1992* agreement. This ruling will also have bearing on the disclosure or use of any communications relating to Dotcom or the other co-accused that are subject to legal professional privilege (Dotcom v Attorney-General #6 [2013] NZHC 697).

More broadly, the various court hearings, appeals, teleconferences and scrutiny of information flows within and between NZ and US enforcement authorities highlights the importance of judicial review as a meaningful forum to scrutinise global police investigations. The very active role of Chief Justice Winkelmann in 'calling out' the potential for Baigent's compensation has produced significant admissions from the GCSB and NZ Police about their involvement in unlawful surveillance and information transfer. This common law remedy has significant financial and symbolic deterrent effects that reinforce the importance of localised human rights requirements and legal standards that affect police agencies receiving mutual assistance requests on significant transnational criminal investigations. This is a poignant reminder that such requests and any related legal action commenced by requesting nations in other domestic legal systems can potentially cancel out any barriers relating to the extraterritorial application of law in offshore criminal investigations (United States of America v Dotcom #4 [2013] NZHC 38 (1 March 2013 at para 119). Under this logic, US authorities might not be able to hide behind the shield of sovereignty to avoid financial contributions for Baigent's damages payable by the NZ Police and GCSB as a direct result of any enforcement activity undertaken within the terms of the initial mutual assistance request.

**Kim Dotcom *cause célèbre***

Variously described as a 'big, jovial internet mogul' (Editorial 2012), a 'controversial internet tycoon' (Bennett 2013), 'one of the world's most "flamboyant" computer hackers' (Fisher 2011), a 'celebrity du jour' and a 'larger-than-life oddball' (Rudman 2013), Dotcom remains an enigma as one of the ten wealthiest people in NZ. The Megaupload indictments solidify his role as a prominent critic of proposed legislation to enhance the GCSB's surveillance capacity to combat terrorism, enhance cyber security, and legalise information sharing amongst NZ police, security and defence agencies (Young 2013b). The NZ Prime Minister dismisses Dotcom as a 'conspiracy theorist' (Young 2013a) who 'loves the limelight' (Protest marches against GCSB bill across NZ 2013) and fuels unnecessary public anxieties that challenge NZ's national security interests through unsubstantiated claims the GCSB operates as the compliant subsidiary of the US National Security Agency (NSA). These claims are considered part of Dotcom's long-term self-serving agenda to remain in NZ 'forever'.

The raids and their subsequent fallout generated considerable global interest in Dotcom's lavish and eccentric lifestyle. He has self-funded and produced two films, *Kimble Goes to Monaco* and *Kimble Goes to Monaco Part II*, which star leading German female centrefold models and document his penchant for fast cars, yachts and partying at the 2000 and 2001 Monaco Grand Prix (Pappademas 2012). Before Kimble officially changed his surname to Dotcom in 2005 when Megaupload was formally established in Hong Kong, he was convicted of insider trading and pleaded guilty to embezzlement under German law, which lead to two 20-month probation terms and fines totalling €100,000 (Gallagher 2012). After the NZ raids, he publicly warned members of the online protest group Anonymous to stop hacking the websites of NZ government ministers or risk strengthening claims for more expansive GCSB powers to combat cybercrime (Backhouse and Shuttleworth 2013). This warning coincided with extensive public consternation about the organisational culture of the GSBC and revelations of its surveillance of several NZ journalists (Edwards 2013). A short online 'mash up' of police video footage and CCTV images of the raid, accompanied by Dotcom's own original music and digital animations, is depicted as part of a broader 'publicity campaign' against the US indictments (Staff Writers/AAP 2013). The video is careful to conceal the identities of police officers in line with orders issued during court proceedings that prohibited the release of certain images and other strategic documents with the potential to cause 'danger to staff in future operations' (Dotcom v Attorney-General #2 [2012] NZHC 2000; Dotcom v Attorney-General #5 [2013] NZHC 695).

The theatrics of the NZ raid and its global depiction as news replicates other large-scale law enforcement and securitisation initiatives. The desire to assist the FBI with its MACMA request undoubtedly promoted the construction of an image of NZ policing as tough, uncompromising and pivotal to the success of a significant global criminal investigation. The displays of paramilitary and military force, extensive tactical coordination based on covert intelligence, and the selective distribution of graphic imagery and contentious factual descriptions of the raid to preferred media outlets, mirror the theatre of law enforcement activities at various major global political and cultural events, including the Olympic Games (Boyle and Haggerty 2009, 2012) and the annual G20 economic summits (Monaghan and Walby 2012). Speculation 'the raid made in Hollywood' (Amsterdam and Rothken 2013: 14-16) involved questionable force with lasting impacts on Dotcom, his pregnant wife and his three children, have been met by counterclaims that police misconduct was defensible, as police were forced to enter a secure 'panic room' while Dotcom's burly figure lunged towards a firearm. It was later reported the weapon remained inside a locked safe and was loaded with a single rubber bullet (Fisher 2012).

In May 2012, a 48-page whitepaper co-authored by two lawyers working for Dotcom systematically attacked the 'baseless' allegations and 'dubious legal principles' associated with 'the largest copyright case in history'. US concern over the criminal enterprise neglected various attempts by Megaupload to 'guard against copyright infringements' (Amsterdam and Rothken

2013: 2-5). However, the US Department of Justice claims that regular violations of a permissible daily threshold of 5,000 'copyright takedowns', largely detected through surveillance of file sharing activity in Megaupload by the US entertainment industry, justified criminal prosecution due to the evident failure of voluntary compliance with numerous directives issued by US law enforcement officials (Fisher 2012). The whitepaper challenges these justifications for such an 'overly expansive and unsupported legal theory of criminal liability' that tests the limits of conventional notions of US sovereignty and has been 'littered with due process violations' (Amsterdam and Rothken 2013: 5-11). Of specific concern is the confiscation of all Megaupload property and user data under US law via 'an ex parte hearing without prior notice, hearing, or opportunity for defence, and with no effective remedy afterward' (Amsterdam and Rothken 2013: 46). While this statement is only partly true as these issues have been subject to various review processes within the NZ court system, it reinforces the highly emotive underpinnings of this approach to extraterritorial policing, surveillance and prosecutorial decision-making.

These issues must be considered alongside news of the NSA's Prism surveillance program, which is likely to be the source of much online surveillance undertaken by US authorities to support the federal criminal indictments. Global revelations about Prism provided the opportunity for Dotcom to publicly affirm that his concerns about the role of 'the state as a potential threat to basic civil rights and liberties – may have been right all along' (Dotcom 2013). In an informed opinion piece for *The Guardian*, which was one of the major news outlets documenting leaks about the global implications of Prism's online surveillance activities along with the *Washington Post*, Dotcom reiterated key arguments in the whitepaper indicating this form of surveillance, and the highly selective US law enforcement and private corporate interests it promotes, affect the rights of all citizens under the Echelon/Five Eyes program.

> I have emphasised that I am being prosecuted not because the charges against me have some sound basis in US copyright law, but because the US justice department has been instrumentalised by certain private interests that have a financial stake in neutralising my business. That trend represents a danger not just to me, but to all of us (Dotcom 2013).

Once news of Prism emerged, the American Civil Liberties Union (ACLU) re-launched a significant case against the US federal government alleging the breach of several civil rights protections under the US Constitution. The ACLU uses Verizon, one of three major US telecommunications companies that allegedly supplies the NSA with 'metadata' revealing the identity of phone numbers and the time, length and location of incoming and outgoing calls throughout the US (American Civil Liberties Union v Clapper 2013 at para 31). The ACLU questions this surveillance practice. One reason is many telephone communications involve legally privileged discussions with clients regarding actual or prospective legal proceedings against US federal agencies (American Civil Liberties Union v Clapper 2013 at para 25). Proposed legislative reforms in NZ will allow the GCSB to access equivalent telecommunications metadata. Thus, Kim Dotcom's advocacy converges around several crucial political developments associated with state surveillance practices in NZ and the US, which are intertwined with the expanded transnational reach of US criminal laws, enforcement and mutual assistance initiatives associated with online piracy. The launch of MEGA, the cloud-based successor to Megaupload (Fletcher 2013a), might add further weight to intensified transnational criminal copyright enforcement (Fletcher 2013b), or could invoke more efficient data encryption (Barton 2013a) and digital blocking technology to prevent online piracy and protect information about registered users from questionable forms of surveillance and data exchange amongst law enforcement agencies within the Echelon/Five Eyes group.

**Conclusion: Global policing, information flows and sovereign authority**

The complexity of Kim Dotcom's case highlights several technicalities and regulatory gaps associated with the global consumption of digital media (David 2010) and commensurate deficits in the application of due process principles to transnational surveillance, intelligence gathering and law enforcement procedures. Principles of sovereignty that invoke territorial jurisdictional boundaries to constrain extraterritorial policing activity are significantly challenged by global information flows, and related commercial interests that favour enhanced transnational law enforcement capacities. The ability of private corporations and public police to engage in extensive online surveillance of suspect P2P and cloud services (David 2010: 5) has significant implications for notions of individual privacy (Drury 2012). These issues are magnified in transnational criminal investigations where traditional national due process constraints governing state surveillance do not adequately encapsulate informal requests for investigative assistance, which may or may not be formalised through recognised mutual assistance requirements. Extensive transnational flows of criminal intelligence and other surveillance activity through collaborative securitisation measures such as the Echelon/Five Eyes agreement appear to remain beyond critical public or regulatory scrutiny.

However, the cases documented in this paper challenge arguments that transnational policing is totally immune from regulatory control (Anderson 1989; Deflem 2004). In fact, the Dotcom case reveals several contradictions between US and NZ search warrant, information seizure, data transfer and judicial review procedures that are far from being fully 'harmonised' or aligned. Chief Justice Winkelmann's rulings declaring the NZ search warrants to be invalid might not have been able to prevent the initial unlawful transfer or destruction of sensitive personal information about registered users of Megaupload that has been unlawfully conveyed to US law enforcement authorities. However, these rulings allow for the qualified disclosure of this information for Kim Dotcom's extradition and any related proceedings associated with the US federal indictments. Despite the initially informal nature of the mutual assistance request, its subsequent formalisation and the related court rulings associated with the NZ raid, the seizure of evidence, its cloning and ultimate transfer to the FBI were subject to rigorous judicial scrutiny in line with the local contingencies of NZ criminal and human rights laws. These avenues temper claims about the 'Americanisation' of global policing via the regularisation, accommodation and homogenisation of highly selective US law enforcement interests in other nations (Nadelmann 1993).

Dotcom and his associates have been able to fund up to 10,000 hours of legal representation in NZ partly due to the release of $NZ2.7 million in funds from the various asset seizures. This sum does not cover legal advice relating to Megaupload's Hong Kong or US business activities (Fisher 2013). However, for a growing number of people enmeshed in transnational criminal investigations, such resources are unlikely to be available. Further, the overall costs of deploying resources and the potential for extensive legal challenges associated with transnational criminal investigations are a significant barrier to open and transparent justice, particularly due to the expenses associated with implementing mutual assistance requests, collecting and securely transferring evidence, and ensuring witness testimony can be presented and tested in court proceedings (Flynn and Fitz-Gibbon 2013). By April 2012, legal challenges in the Dotcom case cost NZ taxpayers an estimated $NZ1.12 million, independently of the undisclosed financial costs of resources provided to the investigation by NZ Police and the GCSB. Further estimates suggest these costs are likely to increase to $NZ4 or $NZ5 million by the time of Dotcom's extradition hearing (Barton 2013b). By contrast, reports suggest that since Megaupload was closed by the US Department of Justice, two major movie studios report increased revenues of between $US1.1 and $US1.9 million from online sales and rental arrangements (Collins 2013). Such figures add weight to the financial arguments supporting the more rigorous transnational enforcement of criminal copyright laws (McCourt and Burkart

2003), even though the main beneficiary is likely to be the private entertainment industry rather than the state.

Case studies such as this are an important means of understanding contemporary global policing developments. Legal case analysis does not replace the need for thick descriptions emanating from ethnographic research (Nadelmann 1993), nor does it seek to re-cloak global policing developments within narrow and restrictive 'rule-of-law' principles. Bowling and Sheptycki (2012: 130) caution that global policing should not be understood primarily through the rule-of-law. Rather, the analysis of written law should be seen as a resource to examine 'rule *with* law', by circumscribing global policing practices *through* law. The Dotcom case indicates tensions between US and NZ policing approaches and legal requirements have significant implications for any transnational prosecutions that reveal an extremely disjointed harmonisation of contemporary global enforcement and mutual assistance arrangements. While judicial review can address overt procedural gaps, and invoke awareness of arguments such as the existence of Baigent's compensation that might have significant effects in shaping desirable extraterritorial policing activities, they could equally validate and entrench problematic transnational enforcement arrangements in other cases. The cases documented in this paper demonstrate the importance of formal judicial rulings as evidence of 'rule *with* law' that reveal the relationship between external review and legal resistance towards the unchecked collection and distribution of criminal intelligence for transnational law enforcement purposes. These issues remain open to further and ongoing empirical analysis of mutual assistance arrangements, their implementation and their capacity to be subject to various modes of formal independent scrutiny under established sovereign legal processes.

Finally, intellectual property law was developed to protect commercial interests associated with burgeoning nineteenth century print industries (Mazzone 2011). Debate about the suitability of the criminal law in governing various forms of internet activity is ongoing and magnified by the difficulties of applying the logics of criminalisation to regulate any transnational or international behaviour (Findlay 2008). In the online world, competing claims to justice and procedural fairness involve the simultaneous normalisation of contentious surveillance, data mining, locational tracking and other digital assemblage technologies in the contemporary global policing armoury (Haggerty and Ericson 2006). These appear logical measures to combat copyfraud (Mazzone 2011) and other wrongful behaviour associated with digital information flows. However, the borderless nature of cyber culture places users of digital technology under increased surveillance and risk of exposure to complex prosecutions in offshore locations. One particularly disturbing legacy of the Kim Dotcom saga is that data containing the identities and locations of all Megaupload are likely to remain in the possession of US authorities, even though NZ law has later declared this information to have been obtained unlawfully. As such, we remain concerned that the rule-of-law must be incorporated as a central element of a broader suite of global policing accountability mechanisms that acknowledges the prospect for meaningful resistance to questionable extraterritorial law enforcement activity not only by individuals such as Dotcom, but also via activist civil libertarian groups and sovereign judicial review mechanisms. The cases documented and analysed above offer a pertinent site for the further examination of these issues, and their potential endorsement and contestation of questionable extraterritorial policing and surveillance arrangements in the contemporary digital age.

*Correspondence:* Associate Professor Darren Palmer, School of Humanities and Social Sciences, Faculty of Arts and Education, Deakin University, Waurn Ponds, Victoria, 3216. Email: darren.palmer@deakin.edu.au

**References**

Amsterdam RR and Rothken IP (2013) *Megaupload, the Copyright Lobby and the Future of Digital Rights: The United States vs You (and Kim Dotcom)* May. Available at http://kim.com/whitepaper.pdf (accessed 4 August 2013).

Anderson M (1989) *Policing the World*. Oxford, UK: Oxford University Press.

Andreas P and Nadelmann E (2006) *Policing the Globe: Criminalisation and Crime Control in International Relations*. New York, New York: Oxford University Press.

APNZ (2012) Dotcom raid gets positive feedback. *The New Zealand Herald*, 15 February. Available at http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10785599 (accessed 5 August 2013).

Australian Crime Commission (ACC) (2011) *Organised Crime in Australia*. Canberra, ACT: Commonwealth of Australia. Available at http://www.crimecommission.gov.au/sites/default/files/files/OCA/2011/oca2011.pdf (accessed 25 January 2013).

Backhouse M and Shuttleworth K (2013) Dotcom calls on National Party hackers to stop it. *The New Zealand Herald*, 30 July. Available at http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10905329 (accessed 5 August 2013).

Barton C (2013a) Kim Dotcom fights back with encryption. *The New Zealand Herald*, 5 February. Available at http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=10863313 (accessed 5 February 2013).

Barton C (2013b) Dotcom's costly battle continues. *The New Zealand Herald*, 5 March. Available at http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=10869106 (accessed 5 March 2013).

Bayer J (2013) Dotcom wins right to sue. *The New Zealand Herald*, 7 March. Available at http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10869764 (accessed 7 March 2013).

Bennett A (2013) Keys role upsets former spy chief. *The New Zealand Herald*, 4 April. Available at http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10875266 (accessed 5 August 2013).

Bowling B and Sheptycki J (2012) *Global Policing*. London, UK: Sage.

Boyle P and Haggerty K (2009) Spectacular security: Mega events and the security complex. *International Political Sociology* 3(3): 350-369.

Boyle P and Haggerty K (2012) Planning for the worst: Risk, uncertainty and the Olympic Games. *The British Journal of Sociology* 63(2): 241-259.

Collins S (2013) Dotcom's shutdown good for US studios. *The New Zealand Herald*, 9 March. Available at http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10870142 (accessed 9 March 2013).

Costa ME III (2004) Extraterritorial application of the Maritime Drug Law Enforcement Act in United States v Suerte. *Temple International and Comparative Law Journal* 18(1): 131-154.

David M (2010) *Peer to Peer and the Music Industry: The Criminalisation of Sharing*. London, UK: Sage.

Dawson JB (1982) The exclusion of unlawfully obtained evidence: A comparative study. *International and Comparative Law Quarterly* 31(3): 513-549.

Deflem M (2004) *Policing World Society: Historical Foundations of International Police Cooperation.* Oxford, UK: Oxford University Press.

Dotcom K (2013) Prism: Concerns over government tyranny are legitimate. *The Guardian*, 13 June. Available at http://www.theguardian.com/commentisfree/2013/jun/13/prism-utah-data-center-surveillance (accessed 13 June 2013).

Drury A (2012) How internet users' identities are being tracked and used. *Tulane Journal of Technology and Intellectual Property* 15: 219-241.

Editorial (2012) Kim Dotcom sets off year of fireworks for politicians. *The New Zealand Herald,* 27 December. Available at http://www.nzherald.co.nz/opinion/news/article.cfm?c_id=466&objectid=10856144 (accessed 25 January 2013).

Edwards B (2013) Democracy under attack, again. *The New Zealand Herald*, 30 July. Available at http://www.nzherald.co.nz/politics/news/article.cfm?c_id=280&objectid=10904950 (accessed 5 August 2013).

Findlay M (2008) *Governing Through Globalised Crime: Futures for International Criminal Justice.* Cullompton, UK: Willan.

Fisher D (2011) Flamboyant former hacker to settle in NZ. *The New Zealand Herald*, 12 June. Available at http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10731751 (accessed 5 August 2013).

Fisher D (2012) Kim Dotcommando: Life's no game. *The New Zealand Herald*, 29 January. Available at http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10781984 (accessed 5 August 2013).

Fisher D (2013) Legal costs mount in Dotcom case. *The New Zealand Herald*, 29 July. Available at http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10904690 (accessed 5 August 2013).

Fletcher H (2013a) Mega off to racing start. *The New Zealand Herald*, 25 January. Available at http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=10861263 (accessed 25 January 2013).

Fletcher H (2013b) Mega hit with 150 copyright warnings. *The New Zealand Herald*, 31 January. Available at http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=10862541 (accessed 31 January 2013).

Flynn A and Fitz-Gibbon K (2013) *A Second Chance for Justice: The Prosecution of Gabe Watson for the Death of Tina Thomas*. Newcastle Upon Tyne, UK: Cambridge Scholars Publishing.

Gallagher S (2012) The fast, fabulous, allegedly fraudulent life of Megaupload's Kim Dotcom. *Wired*, 26 January. Available at http://www.wired.com/threatlevel/2012/01/kim-dotcom/ (accessed 4 August 2013).

Haggerty KD and Ericson RV (eds) (2006) *The New Politics of Surveillance and Visibility*. Toronto, Canada: University of Toronto Press.

Joutsen M (2005) International instruments on cooperation in responding to transnational crime. In Reichel P (ed.) *Handbook of Transnational Crime and Justice*. Thousand Oaks, California: Sage.

Kontorovich E (2009) Beyond the Article 1 horizon: Congress's enumerated powers and universal jurisdiction over drug crimes. *Minnesota Law Review* 93(4): 1191-1252.

Ku RSR (2002) The creative destruction of copyright: Napster and the new economies of digital technology. *The University of Chicago Law Review* 69(1): 263-324.

Lauinger T, Szydlowski M, Onarlioglu K, Wondracek G, Kirda E and Kruegel C (2013) Clickonomics: Determining the effect of anti-piracy measures for one-click hosting. Paper presented at the *20th Annual Network and Distributed System Security Symposium*, San Diego, 26 February. Available at http://seclab.ccs.neu.edu/publications/ndss2013clickonomics.pdf (accessed 13 March 2013).

McCourt T and Burkart P (2003) When creators, corporations and consumers collide: Napster and the development of on-line music distribution. *Media, Culture and Society* 25(3): 333-350.

Marshall L (2002) Metallica and morality: The rhetorical battleground of the Napster wars. *Entertainment Law* 1(1): 1-19.

Mazzone J (2011) *Copyfraud and other Abuses of Intellectual Property Law*. Stanford, California: Stanford University Press.

McMahon N (2011) Nation of unrepentant pirates costs $900m. *Sydney Morning Herald*, 6 March. Available at http://www.smh.com.au/technology/technology-news/nation-of-unrepentant-pirates-costs-900m-20110305-1bix5.html (accessed 13 March 2013).

Monaghan J and Walby K (2012) 'They attacked the city': Security intelligence, the sociology of protest policing and the anarchist threat at the 2010 Toronto G20 Summit. *Current Sociology* 60(5): 653-671.

Nadelmann E (1993) *Cops Across Borders: The Internationalization of U.S. Criminal Law Enforcement*. University Park, Pennsylvania: Pennsylvania State University Press.

New Zealand Law Commission (1997) *Crown Liability and Judicial Immunity: A Response to* Baigent's Case *and* Harvey v Derrick. Wellington, NZ: The Law Commission. Available at: http://www.nzlii.org/nz/other/nzlc/report/R37/ (accessed 10 June 2013).

New Zealand Law Commission (2007) *Search and Surveillance Powers* Report 97. Wellington, NZ: The Law Commission. Available at http://www.lawcom.govt.nz/project/search-and-surveillance-powers (accessed 13 March 2013).

Nicholls C, Montgomery C and Knowles J (2007) *The Law of Extradition and Mutual Assistance*, 2nd edn. Oxford, UK: Oxford University Press.

Palmer D, Berlin M and Das D (eds) (2012) *The Global Environment of Policing*. Boca Raton, Florida: Taylor and Francis CRC Press.

Pappademas A (2012) Megaupload masterpiece theatre: 'Kim Schmitz goes to Monaco'. *Grantland*, 24 January. Available at http://www.grantland.com/blog/hollywood-prospectus/post/_/id/41834/megaupload-masterpiece-theater-kim-schmitz-goes-to-monaco (accessed 5 August 2013).

Protest marches against GCSB bill across NZ (2013) *The New Zealand Herald*, 27 July. Available at http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10904220 (accessed 5 August 2013).

Rudman B (2013) Dotcom's the man to get city noticed. *The New Zealand Herald*, 29 July. Available at http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10904695 (accessed 5 August 2013).

Serious Organised Crime Agency (SOCA) (2013) 'Threats' at *SOCA* homepage. Available at http://www.soca.gov.uk/threats (accessed 19 June 2013).

Smillie JA (1994) The allure of 'rights talk': Baigent's case in the Court of Appeal. *Otago Law Review* 8(2): 188-204.

Staff Writers / AAP (2013) Kim Dotcom mansion raid CCTV released. *news.com.au*, 14 June. Available at: http://www.news.com.au/world-news/kim-dotcom-mansion-raid-cctv-released/story-fndir2ev-1226663608878 (accessed 14 June 2013).

Wall DS and Yar M (2010) Intellectual property crime and the internet: Cyber-piracy and 'stealing' information intangibles. In Jewkes Y and Yar M (eds) *Handbook of Internet Crime*. Cullompton, UK: Willan.

Warren I (2005) 'Papa' Jack and US federal interventions. *Entertainment and Sports Law Journal* 3(1). Available at http://www2.warwick.ac.uk/fac/soc/law/elj/eslj/issues/volume3/number1/warren/ (accessed 10 June 2013).

Yar M (2005) The global 'epidemic' of movie 'piracy': Crime wave or social construction? *Media Culture Society* 27(5): 677-696.

Young A (2013a) Key, Dotcom clash over GCSB bill. *The New Zealand Herald*, 4 July. Available at http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10894618 (accessed 5 August 2013).

Young A (2013b) GCSB changes 'do not address flaws' – QC. *The New Zealand Herald*, 24 July. Available at http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10902099 (accessed 5 August 2013).

**Legislation**

Bill of Rights Act 1990 (NZ)

Mutual Assistance in Criminal Matters Act 1992 (NZ)

**Cases**

American Civil Liberties Union v Clapper (2013) United States District Court Southern District of New York (11 June 2013). Available at http://www.aclu.org/files/assets/nsa_phone_spying_complaint.pdf (accessed 19 June 2013).

Attorney-General in respect of Government Communications Security Bureau (GCSB) v Dotcom, Batato, Ortmann and van der Kolk [2013] NZCA 43 (7 March 2013)

Commissioner of Police v Dotcom #1 [2012] NZHC 634 (18 April 2012)

Commissioner of Police v Dotcom #2 [2012] NZHC 2190 (29 August 2012)

Dotcom v Attorney-General #1 [2012] NZHC 1494 (28 June 2012)

Dotcom v Attorney-General #2 [2012] NZHC 2000 (8 August 2012)

Dotcom v Attorney-General #3 [2012] NZHC 3268 (5 December 2012)

Dotcom v Attorney-General #4 [2013] NZHC 1269 (31 May 2013)

Dotcom v Attorney-General #5 [2013] NZHC 695 (9 April 2013)

Dotcom v Attorney-General #6 [2013] NZHC 697 (9 April 2013)

Simpson v Attorney-General (Baigent's case) [1994] 2 NZLR 667

United States of America v Dotcom #1 [2012] NZHC 328 (29 February 2012)

United States of America v Dotcom #2 [2012] NZHC 1353 (15 June 2012)

United States of America v Dotcom #3 [2012] NZHC 2076 (16 August 2012)

United States of America v Dotcom #4 [2013] NZHC 38 (1 March 2013)