International Journal of Communication 6 (2012), 127–143 1932–8036/20120127

The Internet, the Law, and Privacy in New Zealand: Dignity with Liberty?

JONATHAN BARRETT
LUKE STRONGMAN
Open Polytechnic of New Zealand

Early participants in the Internet experienced very little legal or social pressure with respect to either data privacy or regulation. However, the innovations of Web 2.0 are symptomatic of a re-creation of cyberspace from an original "free for all," in which websites had no normative constraints, toward a significant shift to website management that addresses privacy concerns. If the laws of the non-virtual world are difficult to apply to the online world, must the non-virtual world create new laws to control the online world? Should a balance be made between laws of the non-virtual and virtual worlds, or should a new set of laws be created specifically to govern the Internet? Concordant with this dilemma is the issue that although precedent may create new laws, when the law changes with the possibilities for uses and abuses of new online technologies, to what extent can it be said to either perpetuate or create to any internally consistent system?

Introduction

For many of its early participants, the Internet presented the opportunity for a benignly anarchic and anomic space for freedom of expression that, in principle and practice, should be liberated from established legal traditions and social pressures. Its debt to the military notwithstanding (see Morozov, 2011b), Web 1.0 was typically conceived as a virtual realm that could be created, grown, and governed—or non-governed—by its participants. Because web-based communication usually features cooperative production and use (see, for example, Benkler, 2006; Boyle, 2008; Lessig, 2004), "the web grows organically as a reflection of the collective activity of the users" (Mason & Rennie, 2008, p. 2). Indeed, the Internet may be seen as an "autopoietic system"—a network of processes that, through their interactions, regenerate and instantiate the processes from which they are produced (Varela et al., 1974). The ease of technological transfer to the electronic medium may have allowed the traditional print-based community, with its network of values in relation to writing and interpersonal exchanges, to have moderated behavior

Jonathan Barrett: Jonathan.Barrett@OpenPolytechnic.ac.nz
Luke Strongman: Luke.Strongman@OpenPolytechnic.ac.nz
Date submitted: 2011–02–13

to some extent, but any norms, such as those relating to privacy, that did emerge in the context of Web 1.0 were greatly determined by online users and commercial websites (Hetcher, 2004).

Web 2.0 is distinguished by an unprecedented proliferation of self-expression. (See O'Reilly, 2005, for a discussion of the distinctions between Web 1.0 and Web 2.0.) Technology that is "global, social, ubiquitous and cheap" (Shirky, 2009) has enabled individuals to become producers of outputs historically the preserve of state or public media corporations. This development intimates a remarkable potential for emancipation. Thus, for Fitzgerald (2003, p. 184), Web 2.0 "software is not just code. It is discourse." Best argues "the Internet is a fundamental human right in and of itself" (2004, p. 30). Since individuals involved in Web 2.0 media production and social networks tend not to engage in commercial activity (Hocking, 2009), they are subject neither to the pressures exercised on commercial media by advertisers or consumers, nor the moderating discipline of editorial control. As a consequence, typical Web 2.0 language is, at best, candid and robust; commonly, discourteous; and at worst, cruel and hurtful. Grayling (2009, p. 184) describes the blogosphere as "the biggest lavatory wall in the universe, a palimpsest of graffiti and excretion." Furthermore, verifiable fact is not a concern for many new media producers. Thus Manley describes the Internet as "one of the biggest wellsprings of misinformation ever developed" (1998, p. 136) .

For a utopian moment, a self-regulating, virtual world seemed to have been created by and for Web 1.0 users (see Barlow 1996). Indeed, certain commentators argued the Internet was separated from territorial jurisdictional doctrine altogether and subject only to new rules for cyberspace (Johnson and Post, 1996). However, to borrow from Dworkin (1988) and Kershner (1980), in the face of the excesses of Web 2.0, Law's Empire has struck back. Normative expectations have shifted away from "a wild-west world in which websites did almost whatever they wanted with impunity to a world in which a significant percentage of websites are explicitly addressing privacy concerns" (Hetcher, 2004, p. 243). Authoritarian regimes have become adept in quashing online dissent, and in liberal democracies, governments have sought to reestablish conservative values, such as orderly public discourse. Furthermore, the ubiquity of CCTV and other surveillance technology may have changed the relationship between the citizen and government. Police states have always relied on family and neighbors to act as spies on potential dissidents, but the state's contemporary surveillance capacity allows everyone, even in liberal democracies, to be treated as, say, a potential terrorist (Grayling, 2009). Nevertheless, privacy has become an important consideration for lawmakers. For example, in a way that has been likened to King Canute's attempt to repel the tide (Chesterman, 1997), common law courts in Australia and New Zealand have sought to close off judicial processes from new media and to reassert a pragmatic balance between freedom of expression (the right to utter and apprehend information) and respect for human dignity, manifest in the principles of fair trial and privacy.

Article Overview

In this article, we seek to illuminate these developments using some unusual recent judicial decisions as illustrations. First, a discussion of the territorialization of the Internet is given because, once Internet law is patriated, distinctive norms may develop in different jurisdictions. Second, we demonstrate how this fractured normativity may be developing with regard to privacy. Different conceptions of privacy

derived from human dignity and liberty are sketched, and particular issues for privacy arising from the Internet are identified. We discuss conflicts of rights and expectations, making specific reference to recent New Zealand case law in this field. We conclude that, despite common problems for all jurisdictions, online privacy norms are likely to evolve differently, perhaps idiosyncratically.

Territorialization

Early jurisprudential comment proposed that because of its ubiquity and transnational character, jurisdiction over the online world could be considered the equivalent of Antarctic space or the high seas. Menthe, for example, proposed that, for jurisdictional analysis, cyberspace could be treated as a "fourth international space" (1998, p. 70). This view now appears quaint. Questions of jurisdiction in relation to the Internet are problematic, but tricky as they may be, they are predicated on the acceptance that one or other jurisdiction may decide a dispute or prosecute a crime. Harvey (2011) identifies the following challenges to jurisdictional claims raised by the global computer network: first, the authority of local or national governments to assert control over online activity; second, the effects of online behavior on individuals or things; third, the question of the legitimacy of the local sovereign state to formulate or apply local rules to global phenomena; and, fourth, the ability to state which rules apply to a physical location. However challenging the hurdles may be for establishing jurisdictional claims, they are not bars to it. As Kohl concludes, "national law has survived, and can survive, however uncomfortably, the online challenge" (2007, p. 253).

If early commentators commonly argued that no terrestrial law applied to the Internet, an equally utopian but converse idea held that a unified law should apply to cyberspace. However, the fact is that the components of the Internet are located in a multiplicity of jurisdictions. The Internet comprises a physical outer layer that includes operating equipment, such as the connection between phones, modems, and routers, and other communicating technology; a technology layer, which determines access capability among systems; a content layer; and arguably a cognitive layer in the user's application of semantic content and operability to and of the web. Each of those components is likely to be subject to jurisdictional claims. No international treaty, single regulatory framework, or organization governs the Internet, although International Internet Law is a developing area of study (Uerpmann-Wittzack, 2010). In New Zealand, more than 60 statutes refer to online activity, but there is no specific Internet law (New Zealand Human Rights Commission, 2010). Legal engagement with the Internet is impeded by the characteristics that make the system such a powerful publication and communication medium: geopolitical fracture, asynchronous remote operation, and universal access. Conversely, the global reach of web-based publication has massively expanded the scope for online wrongdoing, such as perpetrating libels. As Harvey (observes, it does not "lie within the competence of the [Internet] publisher to restrict the reach of publication" (except by price or encryption) (2011, p. 52). Thus, the potential readership of libelous statements has increased exponentially (Rolph, 2002), and when dissemination "goes viral," millions have become privy to violations of individuals' intimacy.

Given the myriad ways in which the Internet enables breaches of privacy and other assaults on dignity, government action is inevitable. Hieratic elites have traditionally held control over communication systems, and in the past 20 years, media corporations have tended to consolidate (Doyle, 2002), thereby

concentrating economic power still further. This development may help regulatory focus. However, for Web 2.0 media, despite anomalies, such as the *Huffington Post*, production and power is generally diffused, rendering regulation and control problematic. Furthermore, ascription of normative values to cyberspace is inherently difficult because of national differences. Countries may be readily willing to trade and cooperate with one another, but they are less willing to cede elements of sovereignty for the sake of unified law.

Because websites often lack an identifiable location, conflict of laws is inherent in online commerce and other interactions that have legal consequences. Traditional concepts, such as *lex fori* (the place a case is tried), *lex loci contractus* (the law of the place a contract is made), *lex situs* (the law of the place a thing is situated), and *lex loci solutionis* (the law of the place where an obligation is to be satisfied), become further problematized, but not beyond resolution. For example, development of targeting tests, which consider intention, rather than effect (Geist 2001) as part of a broad country-of-destination approach (Kohl 2007), may contribute significantly to settling issues of jurisdictional conflicts.

Summation

Given the broad scope of issues we have sought to identify and sketch so far, it is useful to provisionally sum up. We have argued that the extra-legal nature of the early Internet, actual or optative, has yielded to comprehensive normativity, including rules imposed by website managers and jurisdictional claims by sovereign states. Territorialization of the Internet is problematic, but real. When authoritarian regimes can filter or shut down access to online social media, claims for supra-territoriality are bluntly disproved. Likewise, if the online version of a subscriber access only magazine published in the United States can be sued for libel in Australia (see Rolph 2002), we can conclude that Law's Empire really has struck back. Despite these developments, online discourse is, to a great extent, practically uncontrollable. License in speech, rather than freedom of expression, typifies Web 2.0 discourse. Hoaxes, lies, slander, and breaches of confidence and intimacy have become normal features of the new media. Only occasionally can the law take action, but when it does, an intimation is given of what is important to the law and how territorialized Internet rules might develop differently across jurisdictions. In the following parts, we look at how certain low level, common law courts have engaged with the fundamental human rights of freedom of expression and privacy. We do not suggest these cases establish principles that can be extrapolated beyond the relatively obscure forums in which they were decided; they may indicate there are no metanarratives to be discerned here beyond territorialization.

Privacy

Privacy Crisis

Hetcher argues

> There is a burgeoning privacy crisis caused in large part to [sic] the explosive growth of the Internet. In large measure, this crisis has emerged in a legal vacuum, as there is little positive law that directly regulates the private collection of personal data. Because of this legal vacuum, informal social norms have the potential to play an especially important role in the regulation of data collection online. (2004, p. 243)

Generally, a degree of self-governance of sectors of cyberspace is possible, provided there is minimal spill over and terrestrial norms are not challenged. Online communities, commercial or not-for-profit, may regulate themselves, based on explicit rules or convention. Extra-legal methods of enforcing norms in cyberspace, such as criticism, negative tweets, or forms of outing may be potent (see, for example, GuttenPlag Wiki, 2011), but not necessarily proportionate. Consequently, no society governed by the rule of law will be prepared to allow nontrivial issues to be settled by the unpredictable discipline of an online hue and cry, such as the Chinese "human flesh search" (see Downey, 2010). For Morozov (2011b), "[w]e are careening towards a future where privacy becomes a very expensive commodity." Emerging technology can offer some protection in the face of this privacy crisis. Various tools that enable preservation of anonymity and thereby privacy include *Freenet*, *anonymisers* (Forder and Svantesson, 2008), and *Tor* (Morozov, 2011a), but technological developments, such as cloud computing, generally challenge privacy. A "cloud" is a network of data centers, composed of thousands of interconnected computers that perform software functions on business or personal computers. Cloud computing potentially makes locating target text or data packets much more difficult, given that data is not accessible in the cloud itself. However, the cloud provider may not be legally responsible for ensuring privacy integrity (New Zealand Law Commission, 2010). Thus with almost instantaneous and potentially world wide transborder flows, it is even more difficult to establish the "target information" of data transfer in cloud computing and to prevent "degradation of consumer privacy" (Hetcher, 2004, p. 245).

Privacy: Dignity vs. Liberty?

The *Universal Declaration of Human Rights* provides: "No one shall be subjected to arbitrary interference with his privacy" (1948, art. 12). Privacy is a fundamental human right, which for Grayling (2009, p. 115) is "a necessity, a constitutive aspect for well-being," and "an indispensible adjunct of the minimum that individuals require for a chance to build good lives" (2009, p. 110).

Burrows and Cheer (2010) identify three axioms of privacy as secrecy (our accessibility to others), solitude (the extent to which we are known to others and the extent to which others have physical access to us), and anonymity (the extent to which we are the subject of others attention). Some sphere of individual privacy is essential to the preservation of human dignity, and contemporary technology challenges that basic expectation.

Legal protection of privacy in Western legal systems is derived from conceptions of either human dignity or liberty. Whitman observes "[c]ontinental privacy protections are, at their core, a form of protection of a right to respect and personal dignity," whereas American law "is much more oriented toward values of liberty, and especially liberty against the state. . . . It is the right to freedom from intrusions by the state, especially in one's own home" (2003, p. 1161). However, the values of democracy are preeminent. As Fish suggests in the context of the First Amendment to the United States Constitution:

> Despite what they say, courts are never in the business of protecting speech per se, "mere" speech (a nonexistent animal); rather, they are in the business of classifying speech (as protectable or regulatable) in relation to a value— the health of the republic,

> the vigor of the economy, the maintenance of the status quo, the undoing of the status quo—that is the true, if acknowledged, object of their protection. (1994, p. 106)

(Assuming that readers are familiar with negative liberty, we will outline a generic continental conception of privacy, exemplified by German law.)

German law does not recognise a specific right of privacy, instead the Basic Law (*Grundgesetz)* (art. 1) imposes a duty on all state authorities to respect and protect human dignity. In terms of article 2, everyone has the right to the free development of his or her personality, insofar as it does not infringe upon the rights of others or offend against the constitutional order or the moral code (Coors, 2010). Based on these provisions and the Civil Code (*Bürgerliches Gesetzbuch*) (arts. 823 and 826), the German Federal Court has developed a "general right of personality" (*Allgemeines Persönlichkeitsrecht*) (Coors, 2010, p. 592). The South African Constitution, which like the German Basic Law is explicitly dignity-based, guarantees that "[e]veryone has the right to privacy" (Constitution of the Republic of South Africa Act 1996, s. 14). While this guarantee contemplates specific examples of breaches of privacy, such as searches of the person or someone's home, the list is not exhaustive, and it is generally accepted that the right "extends to any other method of obtaining information or making unauthorized disclosures" (McQuoid-Mason, 1998, pp. 11-18).

The adaptability of the common law presents the prospect for judge-made privacy protections in the field of tort. Thus Justices Warren and Brandeis writing ex-judicially, said:

> That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define a new the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. (1890, p. 193)

However, according to Whitman these protections will need to be derived from the principles of negative liberty or, conversely, dignity; he says:

> We have to identify the fundamental values that are at stake in the "privacy" question as it is understood in a given society. The task is not to realize the true universal values of "privacy" in every society. The law puts more limits on us than that: The law will not work as law unless it seems to people to embody the basic commitments of their society. In practice, this means that the real choice, in the Atlantic world at least, is between social traditions strongly oriented toward liberty and social traditions strongly oriented toward dignity. (2003, p. 1220)

Despite these different originating principles, hybridization is both possible and necessary for common law jurisdictions that have adopted dignity-based bills of rights. Thus, in the United Kingdom, the Human Rights Act 1998 incorporates the European Convention on Human Rights into the English common law, notably its continental conception of privacy (art. 8).

New Zealand's Approach to Privacy

Internet use is normal among New Zealand's roughly 4.5 million people for business, socialization, and self-expression. In 2009, 75% of New Zealand homes had access to the Internet, and 80% of individuals over the age of 15 had gone online in the previous 12 months (Statistics New Zealand, 2009). Furthermore, Bell et al. (2008) report that one in ten New Zealand Internet users keeps a blog. Despite New Zealand's markedly laissez-faire governance (Kelsey, 1993), the country's approach to privacy lies somewhere between the American and German positions. A crossover is discernible between common law protections of reputation (*dignitas*) and continental-style assertions of human dignity (*dignatio*) as the noncontingent basis of all human rights. (See Barrett [2005] on the distinction, but also see Post (1986) on human rights-style dignity as a basis for defamation law in the United States.) As Hammond observes:

> The common law has long protected dignity interests through the law of tort. The various torts which protect against . . . invasion of privacy . . . all recognise in greater or lesser measure an affront to personality, and in some respects, dignity. But in modern regimes, the concept of "dignity" is increasingly invoked in the human rights context. (2007, p. 6)

Traditional negative freedoms from interference are affirmed in the New Zealand Bill of Rights Act 1990 (BORA) (s. 21), but the Privacy Act 1993 follows Organisation of Economic Cooperation and Development (OECD) guidelines (Privacy Act 1993; OECD, 1980a), which seem to combine dignity and liberty considerations.[1] (Because the Privacy Act, unlike BORA, only applies to individuals, it is can be seen as primarily dignity-based.) OECD (1980b) identifies "violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data" as a justification for privacy legislation. However, the OECD's motives are not purely concerned with protecting such human rights, and it cautions:

> . . . there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance. (ibid)

Conflict of Rights and Expectations

Privacy is important from a rights perspective, but must be considered with other rights and reasonable expectations. In this regard, Uerpmann-Wittzack argues:

[1] In New Zealand, the Privacy (Cross-border Information) Amendment Act 2010 amended the Privacy Act 1993 to prevent the country being used as a conduit through which personal information can be transferred and received without adequate privacy protection.

> It would be wrong, however, to focus exclusively on privacy. In the cases at hand, protection of privacy comes into conflict with internet freedom . . . Whereas freedom of expression may be restricted in favor of the rights of others and in particular the right to privacy, any restriction must be proportionate to the aim pursued. States have to strike a fair balance between privacy on the one hand and internet freedom on the other hand. (2010, p. 1253)

In a similar vein, New Zealand's independent privacy commissioner is required to take into account:

> [T]he protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way. (Privacy Act 1993, s. 14[a])

Freedom of Expression

The maxims of tort—*volenti non fit injuria* (no injury is done to a willing person) and you take your victim as you find him—seem eminently apposite to web-based discourse. These discourses are context-dependent and will apply differently in the varied, web-based discursive communities. In loosely moderated spaces of the Internet, such as the comments section of YouTube, a person posting an opinion about a video can expect contrary views to be expressed in a way unmitigated by the courtesies normal in face-to-face discussions between strangers. In contrast, in strictly moderated areas, participants may be expected to adhere to varying degrees of "netiquette." For example, in a discussion forum for a college course, a high degree of civility would be expected. Participation in these different discursive communities entails consent to exposure to different kinds of discourse. A problem arises when the conversational style of, say, Twitter—truncated, urgent, and often sarcastic—is received by people outside the particular discursive community for which it is intended. The *Chambers* case, heard in the United Kingdom, highlights the problems of this linguistic and behavioral spill over from particular areas of the Internet to the outside world. The decision also indicates the limited extent to which the law might tolerate expression of web-style speech license in the public sphere.

Chambers

When Paul Chambers' travel plans were affected by severe weather, he tweeted his frustration in the following terms:

> Crap! Robin Hood airport is closed. You've got a week and a bit to get your shit together, otherwise I'm blowing the airport sky high!

The tweet was seen by a duty manager at the airport in Yorkshire, who was using Google to survey references to the airport; he notified the Police. Chambers was arrested under antiterrorism laws on suspicion of creating a bomb hoax. Police confiscated his iPhone, laptop, and personal computer. He

subsequently lost his job and was charged with sending a menacing message via a public telecommunications network—the first person in the United Kingdom to be charged in connection with Twitter. A district judge found him guilty of the offence on May 10, 2010, and Chambers was fined a total of £1,000. Having lost his appeal, Chambers became liable for the £1,000 fine and costs from his original conviction, as well as an additional £2,600 in prosecution costs. (This account is based on Davis, 2010.)

The *Index on Censorship* describes Chambers' lost appeal as "a devastating blow for free speech" (Davis, 2010) and compares the tweet in its jocular innocuousness with John Betjeman's 1937 poem "Slough," which starts

> Come, friendly bombs, and fall on Slough
> It isn't fit for humans now,
> There isn't grass to graze a cow
> Swarm over, Death! (Betjeman, 1970, p. 22)

Literary merit aside, the texts of Betjeman and Chambers are ostensibly similar, but the pertinent issue appears to be context and how a communication might be received by its audience. In the context of the Spanish Civil War and the looming possibility of a wider war, Betjeman's invocation may appear somewhat tasteless, but unlikely to cause alarm. The poem was included in a printed collection, *Continual Dew: A Little Book of Bourgeois Verse*, and Betjeman's select readership would no doubt have been aware of the poet's ironic observations on modern life. In contrast, Chambers' threat, taken in the context of a country in a state of constant alertness for terrorist attacks, could be read by anyone with Internet access and might be taken seriously by those charged with ensuring an airport's security. It appears to be a speech act in the "shouting 'fire!' in a crowded theater" category, which is generally considered unworthy of freedom of expression protection. Tweeters and other Web 2.0 publishers may claim an expectation of absolute freedom of speech, and within a closed community of discourse that may be reasonable, but when the potential audience is the whole world, they must either self-censor or face the consequences, legal or otherwise.[2]

Whale Oil

In broad brushstroke, unlike United States' courts, which tend to ensure fair trials by controlling juries once sequestered, Australasian courts tend to seek to control the flow of information to potential jurors (Chesterman, 1997). This is principally done by imposing information suppression orders about accused persons in controversial cases. However, when the accused is well known or the crime attracts special public opprobrium, suppression of information is challenging in a Web 2.0 context.

[2] On self-censorship, the iconoclastic comedienne Sarah Silverman says: "Why didn't I choose to have Muhammad having sex? The answer is simple: I don't want to get blown up with explosives." Cited by Lynskey (2010, p. 101).

In the *Whale Oil* case,[3] which involved the breach of numerous suppression orders by Cameron Slater, who blogs under the pseudonym "Whale Oil," Justice Harvey observed, "The real essence of the case is about human behaviour. It is a case about the law speaking in the light of changing technologies" (para. [2]). The decision implies there is nothing exceptional about the communications technology associated with the Internet that might save bloggers from being charged with breaches of suppression orders. (Slater could, for example, have broken the law by handing out leaflets outside the court.) Certainly, a local newspaper breaching a suppression order would be open to prosecution, and according to this logic, so should a blogger who is physically present in the relevant jurisdiction. Although name suppression orders originate from the courts' power to administer justice, they commonly protect the privacy of victims (particularly children and victims of sexual assaults) and even for the most obnoxious of crimes, can be linked to respect for the accused's inherent human dignity.

The *Chambers* and *Whale Oil* decisions were largely predictable. Liberal democracies tend to exalt freedom of expression, but not to the extent of endangering lives or jeopardizing fair trials. The fact that new technology was used to abuse the right to free speech presented no problems for the courts, nor should it have. The same outcome would have resulted from older forms of communication technology, such as the printing press, if used to issue threats or breach court orders. However, the decisions that are outlined next are less obvious inasmuch as the technology used seems to have been important in itself. The cases also indicate the emergence of a strong, if ill-defined, conception of dignity-based privacy in a common law jurisdiction.

Ashby

On November 12, 2010, Joshua Ashby was found guilty in the Wellington District Court of distributing an "indecent model or object" to the public (Crimes Act 1961, s. 124(1)[a]) after posting a photo of his naked ex-girlfriend on the public area of Facebook (Anon, 2010). The *Dominion Post* reported:

> Judge Becroft said he was adapting an old print law for the Internet age. "Technology can't be used in this way," he warned. "You would do incalculable harm to someone's reputation." . . . The victim felt degraded. "She was embarrassed, felt exposed and ridiculed and couldn't sleep afterwards." (*The Dominion Post*, Nov 13, 2010, p. A1)

Without access to Web 2.0, it would have been implausible that a young man of modest means could have exposed his victim to such widespread degradation. Presuming the act performed constituted the distribution of a model or object, as the crime requires, the model or object would need to be "indecent," a term not defined in the Crimes Act. Based on the well-established test of "deprave and corrupt" (Cooke, 1993, para. [213]), it is not obvious that Facebook users being exposed to the victim's photo would be affected in that way. Indeed, the hyper-sexualization of the Internet is likely to have inured users to such an image. Responses might range from sympathy to *Schadenfreude*, but depravity and corruption seem unlikely. The real issue—and one the criminal law does not appear to provide an

[3] *Police v Cameron John Slater* DC CRN 004028329-9833 (District Court at Auckland, New Zealand, September 14, 2010).

adequate resolution for—is that Ashby used Web 2.0 technology to disseminate images (potentially to millions of people) that were likely to seriously impinge on the dignity of another person. This case indicates that, rather than focusing on paternalistic ideas, such as public decency, regulation should emphasize the preservation of human dignity. Grayling (2009, pp. 110–111) notes: "Even lovers require a degree of privacy from each other, for to lack a reserve of selfhood is almost the same as not having a self at all." Ashby's case indicates this sentiment has much stronger resonance for ex-lovers, whose dignity may be especially prone to violation.[4]

X

In a significantly misguided attempt to save his failing marriage, X, whose name and the name of his business are suppressed, took to surreptitiously filming his wife in various intimate contexts (Leaman, 2010). When she discovered a hidden camera, X not only lost his wife, but was also successfully prosecuted under the Crimes Act 1961 (s. 216H), which prohibits the making of nonconsensual intimate visual recordings. The court noted that X had not shown the videos to anyone, but the implications were serious, since recordings of this nature tend "to end up on the internet for everyone to see" (Leaman, 2010). X was convicted not because he had disseminated intimate images of his wife, but because the capacity for online publication to humiliate is so great; the simple threat to her dignity was sufficient to warrant legal intervention. The Crimes Act 1961 (ss. 216G–216N) were introduced by the Crimes (Intimate Covert Filming) Amendment Act 2006. The general policy statement in the explanatory note to the bill stated:

> Intimate covert filming . . . robs individuals of the freedom to choose how they present themselves to others. Because they do not know they are being filmed they cannot adjust their behaviour to minimise the intrusion and control how they are viewed. Surreptitious filming reduces people to the objects of another's gaze and if the images are distributed, particularly on the Internet, the subjects become the objects of many people's gaze. Often the filming involves parts of the body only, which intensifies the objectification of human beings for others' gratification.

This statement explicitly links the provisions to freedom of choice, but it is fundamentally about the preservation of human dignity—and that is an appropriate place for any discussion of freedom of expression and privacy to start.

[4] With a particular view to the malicious ex-lover, New Zealand Law Commission (2011) has recommended that the Privacy Act 1993 be amended so that a person posting intimate photographs online cannot enjoy protections designed for families under that Act.

Conclusion

Attempts to find coherence and recount metanarratives about a phenomenon as protean as the Internet invite failure. Alert to this possibility, we have in broad brushstroke sought to identify how the aspiration, if not realization, of benign anarchy and anomy for Web 1.0 has been succeeded by comprehensive regulation, both private, through website managers, and legal at a state level for Web 2.0. Once this territorialization occurs, it becomes appropriate to look locally. To this end, we have sought to show how a particular jurisdiction, which is in many regards an Anglo-liberal, free market paragon, has increasingly turned to the principle of respect for human dignity for guidance. The appropriate balance between dignity and freedom of expression is perennially elusive; it is a tension that requires continuous recalibration. Nevertheless, in New Zealand, a country noted for its eschewing of theory, a pragmatic preference for continental-style dignity is both interesting and welcomed.

References

Anonymous. (2010, November 13). Naked photo sends jilted lover to jail. *The Dominion Post* (Wellington, New Zealand), p. A2.

Barlow, J. (1996). A declaration of the independence of cyberspace. *Electronic Frontier Foundation*. Retrieved from https://projects.eff.org/~barlow/Declaration-Final.html

Barrett, J. (2005). Dignatio and the human body. *South African Journal on Human Rights, 21*, 525–546.

Bell, A., Billot, J., Crothers, C., Gibson, A., Goodwin, I., Sherman, K., Smith, N., Smith, P. (2008). *The Internet in New Zealand 2007 Final Report*. Auckland, New Zealand: The Institute of Culture, Discourse and Communication, AUT University.

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven, CT: Yale University Press.

Best, M. (2004). Can the Internet be a human right? *Human Rights & Human Welfare*, *4*, 23–31.

Betjeman, J. (1970) *John Betjeman's collected poems*. London, England: John Murray.

Boyle, J. (2008). *The public domain: Enclosing the commons of the mind*. New Haven, CT: Yale University Press.

Burrows, J., & Cheer, U. (2010.). *Media law in New Zealand* (6th ed). Wellington, New Zealand: LexisNexis NZ.

Chesterman, M. (1997). OJ and the dingo: How media publicity relating to criminal cases tried by jury is dealt with in Australia and America. *American Journal of Comparative Law*, *45*(1), 109–147.

Cooke, R. (Ed.). (1993). Criminal law. *Laws of New Zealand*. Wellington, New Zealand: Butterworths.

Coors, C. (2010). Headwind from Europe: The new position of the German courts on personality rights after the judgment of the European Court of Human Rights. *German Law Journal*, *11*, 527–538.

Davis, L. (2010). Paul Chambers loses appeal in Twitter joke trial. *Index on Censorship* Retrieved from http://www.indexoncensorship.org/2010/11/paul-chambers-lose-appeal-in-twitter-joke-trial

Downey, T. (2010, July 3). China's cyberposse. *The New York Times*, p. MM38.

Doyle, G. (2002). *Media ownership: The economics and politics of convergence and concentration in the UK and European Media*. London, England: SAGE Publications.

Dworkin, R. (1988). *Law's empire*. Cambridge, MA: Belknap Press of Harvard University Press.

Fish, S. (1994). *There's no such thing as free speech: And it's a good thing, too*. New York, NY: Oxford University Press.

Fitzgerald, B. (2003). Theoretical underpinning of intellectual property: "I am a pragmatist but theory is my rhetoric." *Canadian Journal of Law and Jurisprudence, 16*(2), 179–189.

Forder, J., & Svantesson, D. (2008). *Internet and e-commerce law.* Melbourne, Australia: Oxford University Press.

Geist, M. (2001). Is there a there there? Towards greater certainty for Internet jurisdiction. *Berkeley Technology Law Journal, 16*, 1345–1406.

Grayling, A. C. (2009). *Liberty in the age of terror: A defence of civil liberties and enlightenment values.* London, England: Bloomsbury.

GuttenPlag Wiki. (2011). Retrieved from http://de.guttenplag.wikia.com/wiki/GuttenPlag_Wiki/English

Hammond, G. (2007). Beyond dignity? Courts of New Zealand. Retrieved from http://www.google.co.nz/url?q=http://www.courtsofnz.govt.nz/speechpapers/Speech16-11-07-000.pdf/at_download/file&sa=U&ei=WuYyT7v6CMmbiQe36NWaBQ&ved=0CBMQFjAB&usg=AFQjCNFXHUzIcoPNgK5CEFIPKO_8qDMFxw

Harvey, D. (2011). *Internet.law.nz*: *Selected issues* (3rd ed.). Wellington, New Zealand: LexisNexis.

Hetcher, S. (Ed.). (2004). *Norms in a wired world.* Cambridge, England: Cambridge University Press.

Hocking, A. (2009). Selected liability issues: Social networks and blogs. *The Computer & Internet Lawyer*, *26*(1), 12–19.

Johnson, D., & Post, D. (1996). Law and borders—the rise of law in cyberspace. *Stanford Law Review*, *48*, 1367–1402.

Kelsey, J. (1993). *Rolling back the State: Privatisation of power in Aotearoa/New Zealand*. Wellington, New Zealand: Bridget Williams Books.

Kershner, I. (Director). (1980). *Star Wars: Episode V—The Empire Strikes Back*. San Francisco, CA: Lucasfilm.

Kohl, U. (2007). *Jurisdiction and the Internet: Regulatory competence over online activity.* Cambridge, England: Cambridge University Press.

Leaman, A. (2010, December 4). Sex tape with unaware wife backfires. *Waikato Times*. Retrieved from http://www.stuff.co.nz/waikato-times/news/4422681/Sex-tape-with-unaware-wife-backfires

Lessig, L. (2004). *Free culture: How big media uses technology and the law to lock down culture and control content.* London, England: Penguin Press.

Lynskey, D. (2010, September). The damp patch. *The Word*, p. 101.

Manley, W. (1998, January). The Worldwide Vanity Press. *American Libraries,* p. 136.

Mason, R., & Rennie, F. (2008). *E-Learning and social networking handbook: Resources for higher education.* London, England: Routledge.

McQuoid-Mason, D. (1998). Privacy. In M. Chaskalson et al. (Eds.), *Constitutional law of South Africa* (pp. 18-1–18-19). Cape Town, South Africa: Juta.

Menthe, D. C (1998). Jurisdiction in cyberspace: A theory of international spaces, *Michigan Telecommunications and Technology Law Review*, *4*, 69–103. Also available at http://mttlr.org/volfour/menthe.pdf

Morozov, E. (2011a). *Net delusion: The dark side of internet freedom*. New York, NY: PublicAffairs.

Morozov, E. (2011b). Two decades of the web: A utopia no longer. *Prospect*, *184*. Retrieved from http://www.prospectmagazine.co.uk/2011/06/morozov-web-no-utopia-twenty-years-short-history-internet

Naked photo sends jilted lover to jail Keeping Safe. (2010, November 13) *The Dominion Post*, p. A1.

New Zealand Human Rights Commission. (2010). *The right to freedom of opinion and expression* (Draft for discussion). Retrieved from http://www.hrc.co.nz/hrc_new/hrc/cms/files/documents/26-Oct-2010_10-04-12_Right_to-freedom_opin_and_express_draft.html#_ednref33

New Zealand Law Commission. (2010). *Review of the Privacy Act 1993* (NZLC IP17). Wellington, New Zealand: New Zealand Law Commission.

New Zealand Law Commission. (2011). *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4* (NZLC R123). Wellington, New Zealand: New Zealand Law Commission.

OECD. (1980a). *Recommendation of the Council of the Organisation for Economic Co-operation and Development Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. Retrieved from http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#recommendation

OECD. (1980b). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Retrieved from http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#part1

O'Reilly, T. (2005). *What is Web 2.0*. O'Reilly Media. Retrieved from http://oreilly.com/web2/archive/what-is-web-20.html

Post, R. (1986). The social foundations of defamation law: Reputation and the Constitution. *California Law Review, 74*, 691–742.

Rolph, D. (2002). The message, not the medium: Defamation, publication and the Internet. In *Dow Jones & Co. Inc. v. Gutnick, Sydney Law Review*, *24*(2), 263–280.

Shirky, C. (2009). How social media can make history. *Technology, Entertainment, Design*. Retrieved from http://www.ted.com/talks/clay_shirky_how_cellphones_twitter_facebook_can_make_history.html

Statistics New Zealand. (2009). *Household use of information and communication technology*. Retrieved from http://www.stats.govt.nz/browse_for_stats/people_and_communities/households/householduseofict_hotp2009.aspx

Uerpmann–Wittzack, R. (2010). Principles of international internet law. *German Law Journal*, *11*, 1245–1263.

United Nations. (1948). *The Universal Declaration of Human Rights.* Retrieved from http://www.un.org/en/documents/udhr/

Varela, F., Maturana, H., & Uribe, R. (1974). Autopoiesis: The organization of living systems, its characterization and a model. *BioSystems*, *5*, 187–196.

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.

Whitman, J. (2003). The two Western cultures of privacy: Dignity versus liberty. *Yale Law Journal*, *113*, 1152–1221.

Legislation

Germany

- Bürgerliches Gesetzbuch 1900.
- Grundgesetz für die Bundesrepublik Deutschland 1949.

New Zealand

- Crimes Act 1961.
- Crimes (Intimate Covert Filming) Amendment Act 2006.
- New Zealand Bill of Rights Act 1990.
- Privacy Act 1993.
- Privacy (Cross-border Information) Amendment Act 2010.

South Africa

- Constitution of the Republic of South Africa Act 1996.

United Kingdom

- The Human Rights Act 1998.