DATA PROTECTION MEETS WEB 2.0: TWO SHIPS PASSING IN THE NIGHT

PAUL ROTH*

I INTRODUCTION

Personal information placed on the internet by individuals, particularly information about other people, presents a serious challenge to privacy protection because of its sheer volume, the ease of bypassing any effective form of control, and the decentralised and cross border nature of the internet. As has recently been noted: '[p]rivate individuals now assume a central role in the collection, processing and distribution of data.'[1]

This article examines the extent to which individuals' web 2.0 activities are exempted from data protection regulation. 'Web 2.0' is a popular expression that refers to second generation internet use and applications, whereby people can interact and collaborate with each other and content providers online, sharing information and forming web communities. This is in contrast to the earlier, more passive use of non-interactive websites.[2]

'User generated content' that contains personal information about others and that has been placed online without the authorisation of the individual to whom the information relates is particularly problematic from a data protection perspective. Such information, which may consist of fact, opinion or even false information, may be posted on social networking sites, blogs, 'microblogs' such as Twitter, wikis (which are normally used to create collaborative and community websites), image and video sharing sites like Flickr and YouTube, and experience or information sharing sites. The information can be collected by

* Professor, Faculty of Law, University of Otago, New Zealand.

1 Rebecca Wong and Joseph Savirimuthu, 'All or Nothing: This Is the Question? The Application of Article 3(2) Data Protection Directive 95/46/EC to the Internet' (2008) 25(2) *John Marshall Journal of Computer & Information Law* 241, 242.

2 The expression 'web 2.0' is commonly credited to Tim O'Reilly, whose O'Reilly Media and MediaLive International has held annual conferences on the subject since 2004: see Tim O'Reilly, *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software* (30 September 2005) O'Reilly <oreilly.com/web2/archive/what-is-web-20.html>. Joe Firmage, however, has also been credited with coining the expression: see Paul Festa, *Newsmaker: Portals in Space* (28 July 2003) CNET News <news.cnet.com/2008-1082_3-5056441.html>.

a third party, including commercial entities, to build up profiles of individuals,[3] or it may be altered, used in another context, or be otherwise misused.

Individuals can suffer serious harm as a result of personal information being introduced into cyberspace. A few well known recent examples illustrate the point. In China, there is the phenomenon known as the 'human flesh search engine', which involves people linking up on the internet on blogs and forums in order to pool information, usually about particular individuals, so that some form of vigilante justice may be visited upon them.[4] In other jurisdictions, websites or social networking profiles created in the name of a real person in order to belittle or 'cyber-bully' the subject are not uncommon.[5] The 2008 case of *United States v Drew* arose from the suicide of a 13 year old girl who had been cyber-bullied.[6] The defendant was the mother of one of the victim's former friends. She used a MySpace account to pose as a young man. After initiating a flirtatious relationship with the victim, she then bullied the girl into committing suicide.[7] Another high profile case involved the internet circulation of nine grisly photographs of a young woman, Nikki Catsouras, who died in a 2006 car accident after taking her father's Porsche without permission.[8] The pictures were initially circulated by two Californian highway patrol officers. The parents tried, largely unsuccessfully, to stop the circulation of the pictures, which were being

---

3 For the practice of 'counter-Googling', whereby businesses use search engines like Google to collect information on individuals (as customers or potential customers), see, eg, WiseGeek, *What is Counter-Googling?* (10 September 2010) WiseGeek <www.wisegeek.com/what-is-counter-googling.htm>; Trendwatching.com, *Counter Googling* (2003) <trendwatching.com/trends/2003/09/COUNTER-GOOGLING.html>.

4 See Hannah Fletcher, *Human Flesh Search Engines: Chinese Vigilantes that Hunt Victims on the Web* (25 June 2008) TimesOnline <technology.timesonline.co.uk/tol/news/tech_and_web/article4213681.ece>; Tom Downey, 'China's Cyberposse' *The New York Times* (New York), 3 March 2010.

5 This has been called 'profile squatting': Giles Hogben (ed), 'Security Issues and Recommendations for Online Social Networks' (Position Paper No 1, European Network and Information Security Agency, October 2007) 14. See, eg, *Applause Store Productions Limited v Grant Raphael* [2008] EWHC 1781 (QB) (24 July 2008), discussed below. Curiously, in Hong Kong such sites would not qualify as 'personal information' for the purposes of data protection legislation because 'fabrication or lies' about an individual are not considered to be 'personal information' about the person: Office of the Privacy Commissioner for Personal Data (Hong Kong), *Notes on Complaint and Enquiry Cases Related to Jurisdiction of Personal Data (Privacy) Ordinance: Case Notes*, *Case No 2001009* (2001) <www.pcpd.org.hk/english/casenotes/case_complaint2.php?id=187&casetype=B&cid=27>. This decision was upheld on appeal by the Administrative Appeals Board. In Australia, however, 'personal information' is defined as including 'information or an opinion … whether true or not': *Privacy Act 1988* (Cth) s 6. This is the usual position elsewhere as well.

6 (CD Cal, 08-00582, 28 August 2009). For court documents and commentary on the case, see the Citizen Media Law Project, *United States v Drew* (16 September 2008) <www.citmedialaw.org/threats/united-states-v-drew>. The defendant was convicted but later acquitted of violations of the *Computer Fraud and Abuse Act 1986*, 18 USC § 1030.

7 After the defendant's subsequent acquittal, the law in over 20 US states was amended to cover online harassment and federal legislation was introduced into Congress.

8 See Jessica Bennett, *A Tragedy that won't Fade Away: When Grisly Images of Their Daughter's Death Went Viral on the Internet, the Catsouras Family Decided to Fight Back* (25 April 2009) Newsweek <www.newsweek.com/id/195073>. The body was in such a bad state that the coroner would not allow the victim's parents to identify it.

both sent via email and posted on websites. The pictures were also posted on a MySpace page that was set up in the victim's name.[9]

While remedies to these and other scenarios may or may not be found in existing law, data protection regimes do not normally figure in or provide a ready solution for such issues. Privacy officials around the world tend to find themselves unable to deal head on with such online phenomena, and instead have been largely limited to issuing cautions about the implications for privacy and offering advice to increase awareness and assist individuals in protecting their privacy.[10] It is seldom candidly admitted that user generated content seems to be immune from data protection regulation.

Regulation of web 2.0 activities would be difficult in any event, not least because of the impracticality of imposing the obligations of a data controller on private individuals, such as duties of notification, transparency, data subject participation, and the like. Moreover, the floodgates would be opened to potential complaints. To take as one example, it has been pointed out by one commentator[11] that the posting of photographs on social networking and image hosting websites such as Flickr[12] would involve the wholesale disclosure of personal data about others that is required by European Union law to be treated as 'sensitive'.[13] This is on the basis that photographs could reveal information about such protected interests as race, religion and health status (for example

9 Although the 2008 case against the California Highway Patrol failed at first instance because the dead do not enjoy privacy rights, the California Court of Appeal has now allowed it to proceed: see Dave Thompson, *California Court Vindicates Nicole Catsouras and Her Family Against California Highway Patrol* (1 February 2010), ReputationDefender <www.reputationdefenderblog.com/2010/02/01/california-court-vindicates-nicole-catsouras-and-her-family-against-california-highway-patrol/>.

10 See, eg, International Working Group on Data Protection in Telecommunications, 'Report and Guidance on Privacy in Social Network Services: "Rome Memorandum"' (Working Paper 675.36.5, 4 March 2008) <www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf>; 30th International Conference of Data Protection and Privacy Commissioners, *Resolution on Privacy Protection in Social Network Services* (17 October 2008) <www.lda.brandenburg.de/sixcms/media.php/3509/resolution_social_networks_en.pdf>. For particular jurisdictions, see eg, Australian Government Office of the Privacy Commissioner, *Your Privacy Rights FAQs: Social Networking* (2010) <www.privacy.gov.au/faq/individuals#social_networking>; Office of the Privacy Commissioner of Canada, *Fact Sheet: Social Networking and Privacy* (November 2007) <www.priv.gc.ca/fs-fi/02_05_d_35_sn_e.cfm>; Office of the Privacy Commissioner of Canada, *Fact Sheet: Social Networks Sites in the Workplace: An Introduction* (May 2009) <www.priv.gc.ca/fs-fi/02_05_d_40_sn_e.cfm>; Office of the Privacy Commissioner of Canada, *Fact Sheet: Privacy and Social Networking in the Workplace* (May 2009) <www.priv.gc.ca/fs-fi/02_05_d_41_sn_e.cfm>.

11 Rebecca Wong, 'Data Protection Online: Alternative Approaches to Sensitive Data?' (2007) 2 *Journal of International Commercial Law and Technology* 9, 9.

12 See Flickr (2010) <www.flickr.com>. See also Shutterfly (2010) <www.shutterfly.com>; Kodak Gallery (2010) <www.kodakgallery.com/gallery/welcome.jsp>; Snapfish (2010), <www.snapfish.com/snapfish/welcome>; Photobucket (2010) <www.photobucket.com>.

13 *European Parliament and Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* [1995] OJ L 281, art 8(1) ('*European Union Personal Data Directive*') provides that Member States 'shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.'

where the data subject is pictured in a hospital bed or with a cast).[14] The Article 29 Data Protection Working Party, established under article 29 of the *European Union Personal Data Directive*, however, has taken a purposive approach to the issue, commenting that it 'in general does not consider images on the Internet to be sensitive data, unless the images are clearly used to reveal sensitive data about individuals.'[15] The issue is yet to be legally tested.

This article examines three common exemptions to data protection regulation that apply, or could potentially apply, to web 2.0 activities, but which upon closer examination raise complex issues of definition and application, as is evident from a comparison of the law and practice in different jurisdictions. The focus will be on data protection regulation in Australia, New Zealand, Hong Kong and Britain, which are all common law jurisdictions. It will also consider the leading European cases. New Zealand in particular has a highly developed case law in the area of data protection, the result of an active and well reported Privacy Commissioner complaint system, as well as a specialist tribunal and appellate courts that have decided over 200 cases since 1994.[16]

The chief exemption that is applicable to the web 2.0 user context involves the disclosure of personal information in connection with 'domestic purposes'. However, this raises the issue of whether the dissemination of this information to the public, or even to a section of it, should truly be considered 'domestic'. Another exemption is the prior publication exemption that can sometimes apply when personal information has already been published or is otherwise in the public domain. Finally, there is the journalism exemption that relates to the traditional interest in 'freedom of the press', which is particularly relevant to blogs.

From a practical perspective, it is clear that data protection regulation is not in a position to deal with the myriad disclosures by individuals that take place on the internet. The wide application of the exemptions discussed in this paper mean that data protection regulation would have difficulty in getting to grips with online breaches of privacy in any event. Nevertheless, breaches of privacy on the internet remain a serious concern because the internet, by its nature, renders personal information highly vulnerable.

The answer seems to be only partly a legal one, with technical solutions having to assume an important role in dealing with the issue. Existing civil causes of action and criminal sanctions must continue to supply the necessary

---

14 See, eg, the obiter dictum observation of Patten J in relation to the *Data Protection Act 1998* (UK) c 29 in *Murray v Express Newspapers Plc* [2007] EWHC 1908 (Ch) (7 August 2007) [80]:

> if a photograph and the information it contains constitutes personal data then it is hard to escape from the conclusion that insofar as it indicates the racial or ethnic origin of the data subject it also consists of sensitive personal data.' In relation to health data, he opined that the photograph 'would have to be of someone with some clearly identifiable physical condition which was exposed by the photograph.

15 Article 29 Data Protection Working Party, *Opinion 5/2009 on Online Social Networking* [2009] 01189/09/EN WP 163, [3.4].

16 The tribunal was called the Complaints Review Tribunal until 2002 when it was renamed the Human Rights Review Tribunal. There are appellate rights to the New Zealand High Court, the Court of Appeal and the Supreme Court.

legal remedies, but privacy officials will continue to operate only along the fringes. If privacy officials are to play a larger role in this area, they will need wider jurisdiction, new powers and the capacity to aggressively pursue both legal and non-legal avenues. Private sector commercial agencies are already emerging to fill the gap.[17]

II THE 'DOMESTIC PURPOSES' EXEMPTION

Data protection regulatory regimes conventionally include an exemption for the private collection and use of personal information. Thus, the *European Union Personal Data Directive* does not apply to the processing of personal data 'by a natural person in the course of a purely personal or household activity'.[18] Users of social networking sites are generally regarded as falling under this exemption, except when they use such sites 'as a platform to advance commercial, political or charitable goals'.[19] Similarly, the *APEC Privacy Framework* excludes from its scope 'an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs'.[20]

---

17 See, eg, the technology company ReputationDefender, formed in 2006 'to defend your good name on the Internet': see ReputationDefender, *About Us* (2010) <www.reputationdefender.com/company>. Its self-described goal is:

> To SEARCH out all information about you and your family throughout the Internet and present it to you in a clear, easy-to-understand fashion. To provide DESTROY assistance, helping to remove, at your request, inaccurate, inappropriate, hurtful, and slanderous information about you and your family using our proprietary in-house methodology. This same mission extends to your personally identifiable information, like name, address, and phone number. To deliver CONTROL over how others are able to perceive you on the Internet.

The Catsouras family (above nn 8, 9) made use of this organisation's services: see above nn 8, 9.

18 *European Union Personal Data Directive* [1995] OJ L 281 31, art 3(2). See also Organisation for Economic Co-Operation and Development ('OECD'), *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (23 September 1980) <http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html>, which did not provide for an exception for domestic purposes. Article 2 states that the Guidelines apply, inter alia, to personal data that, 'because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.' Likewise, article 3(b) provides that the Guidelines 'should not be interpreted as preventing … the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties'. Information collected or held by an individual that relates to that individual's domestic or personal affairs could therefore be viewed as not posing a threat to 'privacy and individual liberties'. The OECD Expert Group that formulated the Guidelines did indeed foresee that there would be an increasing use of home computers in the future, but it thought that this would tend to be 'for private purposes that are both harmless and impossible to control': *Annex to the Recommendation of the Council of 23rd September 1980: Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data: Explanatory Memorandum* (23 September 1980) [35] <http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html>.

19 Article 29 Data Protection Working Party, above n 15.

20 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (APEC Secretariat, Singapore, 2005) Principle 10.

The domestic purposes exemption has been accurately described as 'a crucial exception' for social networking sites.[21] The scope of this type of exemption, however, is not always entirely evident, and there is some inconsistency in its application across jurisdictions. Where the line should be drawn between what is and is not exempted may not be a straightforward exercise because the intended dichotomy is not always apparent: is it between what is 'private' or 'personal' and what is 'public'? It has been suggested that with cyberspace, the distinction between the private and the public has become blurred.[22] Although this may be true, issues in drawing a distinction between the two have often arisen in a variety of contexts before the advent of the internet.

While it is possible to carve out 'private' spaces of various kinds online, cyberspace is inherently a public space where one can talk quietly, loudly, or any volume in between. At one extreme, one can maintain one's own webpage and restrict access to one's friends and immediate family, and at the other maintain a blog or profile on a social networking site that is entirely open to the general public. In a recent case, a blogger wanting to preserve his anonymity was unsuccessful in invoking a right to privacy on the basis that he did not have a reasonable expectation of privacy 'because blogging is essentially a public rather than a private activity'.[23] Accordingly, if the 'domestic purposes' exemption calls for a distinction between the private and the public spheres, it will be problematic to know precisely where the line can be drawn: one's close personal and family connections, the larger circle of one's acquaintances and contacts, a section of the public, or the public at large?

Another approach, which seems more straightforward to apply but tends to widen the scope of the exemption, is to distinguish domestic purposes from business, professional, or commercial purposes. This is the approach followed in Australian[24] and Canadian[25] data protection law. The Australian exemption

21 Gehan Gunasekara and Alan Toy, '"MySpace" or Public Space: The Relevance of Data Protection Laws to Online Social Networking' (2008) 23(2) *New Zealand Universities Law Review* 191, 213. The authors go on to remark that the exemption 'allows a vital "social" space within which individuals may conduct themselves without the fear of breaching the strictures of information privacy laws.': at 213.

22 For example, one scholar has commented: '[w]ithout the ability to easily conceptualize location, boundaries, or even norms in cyberspace, the traditional legal boundary between "public" and "private" have [sic] become blurred': Patricia Sànchez Abril, 'Recasting Privacy Torts in a Spaceless World' (2007) 21(1) *Harvard Journal of Law & Technology* 1, 5–6.

23 *The Author of a Blog v Times Newspapers Ltd* [2009] EWHC 1358 (QB), [11] (Eady J) (16 June 2009). The blogger was a serving detective who commented on matters relating to the police and justice. He applied for an interim injunction to preserve his anonymity on the basis of the traditional law of breach of confidence and the more recently evolved doctrine on invasion of privacy.

24 The National Privacy Principles in Australia's *Privacy Act 1988* (Cth) do not apply to '(a) the collection, holding, use, disclosure or transfer of personal information by an individual; or (b) personal information held by an individual; only for the purposes of, or in connection with, his or her personal, family or household affairs': s 16E. Conversely, the Act does not cover the collection, use, or disclosure of personal information by an individual 'other than in the course of a business carried on by the individual': s 7B(1).

applies simply whenever an individual acts in a 'personal capacity', such as 'an individual who posts personal information about others on a personal "blog"'.[26] The personal versus commercial dichotomy would be useful in making provision for the increasing use of web 2.0 activities for pursuing business or professional opportunities through such sites as LinkedIn and Spoke.[27]

A Case Law and Practice

1 *Europe*

The European approach to the application of the domestic purposes exemption to web 2.0 activities is currently dominated by the decision in *Lindqvist*, a case referred from Sweden, where the European Court of Justice held:

> [This] exception must … be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.[28]

Lindqvist involved the publication by Mrs Lindqvist of personal information on an internet website she had set up on her home computer as part of a data processing course. She was a catechist in her parish church and had added pages to her website to allow parishioners preparing for their confirmation to obtain information. The website included information about Mrs Lindqvist and 18 colleagues. She had not informed them of the website, nor had she notified the Swedish data supervisory authority of her activity. She removed the material from her site once she realised that some of her colleagues did not appreciate the material.

As examples of activities that fell under the *European Union Personal Data Directive* article 3(2) exemption for the processing of data 'in the course of a purely personal or household activity', the European Court of Justice cited the sort of activities mentioned in the 12th recital to that Directive, namely, 'the processing of data carried out by a natural person in the exercise of activities

---

25 Part 1 of the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, which covers personal information in the private sector, does not apply to 'any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose': s 4(2)(b). Conversely, Part 1 applies to organisations that collect, use, or disclose personal information 'in the course of commercial activities': s 4(1)(a). The coverage of commercial activities is also reflected by section 4(1)(b), which relates to personal information about employees in connection with the operation of an undertaking or business.

26 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) vol 1, 453 [11.1]. See also Australian Government Office of the Privacy Commissioner, *Your Privacy Rights FAQs: Social Networking* (2010) <www.privacy.gov.au/faq/individuals#social_networking>.

27 See Wade Roush, *Social Networking 3.0: The Third Generation of Social-Networking Technology Has Hit the Web, and It's about Content as Much as Contacts* (18 November 2005) Technology Review <www.technologyreview.com/web/15908/?a=f>.

28 *Lindqvist v Aklagarhammaren I Jonhoping* (C-101/01) [2003] ECR I-12971('*Lindqvist*'); see also *Tietsusuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia* (C−73/07) [2008] ECR I-9831, [44].

which are exclusively personal or domestic, such as correspondence and the holding of records of addresses'.[29] In making this finding, the Court accepted the submission of the Swedish government that the exemption should not apply to the publication of personal information on the internet in such a way that it would be accessible to the public at large.

This decision takes a narrow approach to the scope of the exemption. It implies that the exemption will not apply to information that is accessible to everyone, or at least a large audience, on the internet. The decision does not indicate, however, where one may draw the line between private and public purposes. One could posit that the exemption would cover situations where information is accessible only to one's family and friends. However, mere acquaintances or like minded contacts (such as within a group that shares recreational or social concerns) would seem to fall within a grey area, not to mention 'friends' on social networking sites who may not, in fact, be 'real' friends or even acquaintances. The Article 29 Data Protection Working Party has suggested that '[a] high number of contacts could be an indication that the household exception does not apply'.[30]

2 *Britain*

In Britain, the domestic purposes exemption applies if an individual is holding personal information for their 'personal, family or household affairs (including recreational[)] purposes'.[31] Examples given by the Information Commissioner's Office include personal address lists, Christmas card lists and information held in connection with a hobby,[32] as well as lists of birthdays of friends and relatives, address labels and recordings of images or videos of people met while on holiday.[33]

One interesting scenario that arose, but was not played out, involved a woman who surreptitiously filmed a meeting with a social worker who threatened to take her baby away from her once it was born and place it with foster parents. The mother published the film on the video sharing website YouTube. The local authority objected to this on the ground that it breached the *Data Protection Act 1998* (UK), since the film was made without the knowledge or consent of the social worker.[34]

---

29 *Lindqvist* [2004] QB 1014, 1035 [46].

30 Article 29 Data Protection Working Party, [2008] ECR I-12971, above n 15.

31 *Data Protection Act 1998* (UK) c 29, s 36.

32 Information Commissioner's Office, *Notification Exemptions: A Self-Assessment Guide* (September 2007) 5 <www.ico.gov.uk/upload/documents/library/data_protection/forms/notification_exemptions_-_self-assessment_guide.pdf>.

33 Information Commissioner's Office, *Exemptions: In Brief – Are There Any Exemptions from the Data Protection Act?* <www.ico.gov.uk/for_organisations/data_protection_guide/exemptions.aspx>.

34 Ben Leapman, YouTube Row over Social Services Baby Threat, *Sunday Telegraph* (UK) 19 August 2007 <http://www.telegraph.co.uk/news/uknews/1560701/YouTube-row-over-social-services-baby-threat.html>. See also Camilla Cavendish, *Guilty of Child Abuse! (Well, Our Version)* 23 (August 2007) *The Times* <www.timesonline.co.uk/tol/comment/columnists/camilla_cavendish/article2310550.ece> described the video as follows:

A legal commentator opined that this online publication fell outside the domestic purposes exemption on the basis of the *Lindqvist* decision, since the video was 'made accessible to an indefinite number of people'.[35] While the video was widely published, it undoubtedly dealt with the woman's personal and family affairs. It seems unsatisfactory, however, to base the determination that publication is for domestic purposes on the identity or extent of the audience. For example, if an individual is by nature an exhibitionist or desires the attention or support of others, why should the size of the audience take the information out of the personal affairs sphere? The *Lindqvist* approach here presents a somewhat blunt instrument.

On the other hand, the identity of the person disclosing personal information and the subject matter of the information should make some kind of difference. In the above scenario, the information was squarely about the domestic or family affairs of the individual who processed it. If the processing had been undertaken by the social worker, on the other hand, it would have been done in the course of employment and therefore would not fall under the domestic affairs exemption. Moreover, it would infringe the privacy of the woman by intruding into her personal or family affairs. Put another way, when the woman concerned did the processing, it empowered her by enhancing her control over her own personal and family affairs in a situation where that was being affected by a state agency. It also seems a little far fetched that the social worker's privacy could be infringed upon in the course of going about his job. It assumes that one has a right to privacy when at work, which is by no means a universally accepted proposition.

3 *New Zealand*

Section 56 of New Zealand's *Privacy Act 1993* (NZ) provides that its principles do not apply to the collection or holding by an individual of personal information 'where that personal information is collected or held by that individual solely or principally for the purposes of, or in connection with, that individual's personal, family, or household affairs'.

It is somewhat confusing that the provision refers to personal information that is 'collected'[36] and 'held'[37] by individuals, since this raises the issue whether the provision also covers personal information of one individual that is used or disclosed by another. On a narrow interpretation, the term 'held' in this provision may be relevant only to the application of those principles that apply information

---

> Had it been staged, critics would have called it a caricature. A robotic official orders the sobbing mother to stay in the hospital until his colleagues come to remove her new baby. He refuses her desperate pleas to be monitored with the baby at home. He explains in the tones of a traffic warden the inconvenience of delivering her breast milk. He then lets drop an astonishing admission: that Calderdale Council is pursuing a court order despite there being "no immediate risk to your child from yourselves."

35 OUT-LAW News, *Baby Battle Woman Can't Claim Data Protection Exemption for YouTube Video, Warns Expert* (22 August 2007) OUT-LAW News <www.out-law.com/page-8401>. In the event, the video was taken down within the week: Cavendish, above n 34.

36 *Privacy Act 1993* (NZ) s 56(a).

37 *Privacy Act 1993* (NZ) s 56(b).

while it is in a state of being held, that is, the principles that relate to security, access, correction and retention of personal information.[38] The application of those principles to information relating to one's domestic affairs would otherwise raise absurdities. Moreover, the marginal note to the provision indicates that section 56 was based on section 33(1) of the *Data Protection Act 1984* (UK),[39] which dealt only with the exemption from the legislation's data registration and subject access provisions. New Zealand case law, however, adopts a wider approach to section 56, so as to cover not only the collection and holding of personal information, but use and disclosure as well.[40]

One case investigated by the Privacy Commissioner dealt with a complaint against a woman by the man who was harassing her.[41] Although the facts did not involve the internet, it did deal with the breadth of the domestic purposes exemption. The woman concerned had disclosed the fact of the harassment and the man's criminal convictions to the man's employer. The Privacy Commissioner found that this disclosure fell under the domestic purposes exemption. This conclusion was debatable, as the man had originally contacted her in order to pursue a business proposition after she appeared on television. The woman subsequently complained to the police and hired a private investigator to make inquiries about him. It could be argued that these elements took the matter outside the bounds of the domestic affairs exemption. Moreover, the approach adopted in the case would confer immunity under the *Privacy Act 1993* (NZ) on anyone who chooses to make disclosures to another person's employer, so long as there is no business or employment related connection with the employer. The approach in this case seemed to owe more to sifting out the complaint because of disapproval of the man's conduct than it did to a principled application of the domestic purposes exemption.

In another case investigated by the Privacy Commissioner, the complainant claimed that his former wife had disclosed information about his income and expenditure to the Inland Revenue Department.[42] This disclosure was found to fall under the domestic purposes exemption. One wonders if the same finding would be made if the disclosure was made to the world at large. Another case arose as a result of a neighbour setting up a video camera aimed directly into the complainant's living area.[43] No action was taken on the complaint because the camera was found to be inoperable, but the Privacy Commissioner commented

---

38 *Privacy Act 1993* (NZ) ss 6(5) – (7), (9).

39 Now repealed and re-enacted in altered form as section 36 of the *Data Protection Act 1998*.

40 See, eg, the Complaints Review Tribunal decision in *S v P* [1998] 3 NZCRT 1 (12 March 1998) [15]. The Tribunal reasoned that:

> The *protection*, *use* or *disclosure* of information concern obligations that can only arise if an agency *holds* information. There is therefore no need for s 56 to specifically refer to those obligations because they are covered by the use of the word *hold* in s 56(b). Section 56, therefore also covers the disclosure of information (emphasis in original).

41 *Case Note 52405* [2003] NZPrivCmr 3 (1 February 2003).

42 *Case Note 10115* [1999] NZPrivCmr 8 (1 August 1999).

43 *Case Note 1635* [1994] NZPrivCmr 23 (1 May 1994).

that one issue would have been whether the domestic purposes exemption applied.

4 *Hong Kong*

The *Personal Data (Privacy) Ordinance* (Hong Kong) chapter 486 exempts '[p]ersonal data held by an individual and (a) concerned only with the management of his personal, family or household affairs; or (b) so held only for recreational purposes'.[44] As in Britain, this provision is intended to cover 'the holding of an address and telephone list of friends and relatives by an individual for communication purposes and social or recreational activities, such as the sending of Christmas cards'.[45] The reference to 'management' of one's personal, family or household affairs would tend to make it inapplicable to most web 2.0 applications, except for 'cloud computing' activities that assist individuals in managing and sharing their information.[46] However, the 'recreational purposes' limb of the definition could encompass blogs and the use of social networking services.[47]

The Hong Kong exemption is related to article 14 of the *Hong Kong Bill of Rights Ordinance* (Hong Kong) chapter 383, which aims to prevent interference with a person's 'privacy, family, home or correspondence'.[48] It has been noted that:

> Provided such data are used solely for the stipulated purposes, they have little potential to harm the interests of data subjects. Further, to impose, for example, the access requirements of the Ordinance on such data would not only be cumbersome, but would also unduly intrude on the individual's personal and family life. Should the individual transfer or disclose such data to a data user in administrative or commercial spheres contrary to the limitations of the exemption, however, then the exemption would terminate.[49]

In one case, the Privacy Commissioner dealt with the issue whether a data user contravened the *Personal Data (Privacy) Ordinance* (Hong Kong) chapter 486 by posting an individual's name and photograph publicly on a website without obtaining prior consent.[50] The Privacy Commissioner advised that personal data may not be used for any purpose other than that for which the data were to be used at the time of collection of the data, unless it is a directly related

---

44 *Personal Data (Privacy) Ordinance* (Hong Kong) cap 486, s 52. For the inclusion of 'recreational purposes'; see also *Data Protection Act 1984* (UK) c 29, s 33(1) carried over into the *Data Protection Act 1998* (UK) s 36.

45 Office of the Privacy Commissioner for Personal Data (Hong Kong), *Data Protection Principles in the Personal Data (Privacy) Ordinance – from the Privacy Commissioner's Perspective* (Hong Kong, 2nd ed, 2010) 107 [12.3].

46 Flickr is an example of an image and video management site.

47 See also the similarly worded section 1(4)(c) of the *Data Protection Act 1988* (Ireland) Number 25/1988, which exempts 'personal data kept by an individual and concerned only with the management of his personal, family or household affairs or kept by an individual only for recreational purposes'.

48 *Hong Kong Bill of Rights Ordinance* (Hong Kong) cap 383, s 8.

49 Office of the Privacy Commissioner for Personal Data (Hong Kong), *Data Protection Principles*, above n 45.

50 Office of the Privacy Commissioner for Personal Data (Hong Kong), *Notes on Complaints*, above n 5.

purpose.[51] If the disclosure was inconsistent with the purpose, then the individual's prescribed consent was necessary. The Privacy Commissioner went on to note, however, that the use may fall under the domestic or recreational purposes exemption, in which case the Ordinance may not have been contravened.

5 *Canada*

As noted earlier, Canada takes a capacity based approach to the domestic purposes exemption: the individual must be processing information in a personal, as opposed to a business or professional, capacity.[52] The domestic purposes exemption has been found to apply to:

- personal information relating to a complaint lodged with an agency by an individual and in the individual's possession, as in a case where an employee was unwilling to grant access to the record of a complaint that had been lodged earlier with the employer who no longer retained the records relating to the complaint;[53]
- photographs taken for personal reasons, as in a case where an airline pilot had taken the complainant passenger's photograph as a personal memento during a flight without the passenger's consent. The pilot wished to record his last flight in the particular type of aircraft and took the photographs for personal reasons;[54]
- information collected for use in litigation by an individual, as in a case where a doctor was being sued for professional negligence and hired a private detective to collect information about the plaintiff. The Ontario Supreme Court of Justice commented by way of obiter dicta that being a party in a lawsuit was a personal and not a commercial activity;[55]

---

51 *Personal Data (Privacy) Ordinance* (Hong Kong) cap 486, sch 1 (3).

52 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 4(2)(b) ('PIPEDA').

53 Office of the Privacy Commissioner of Canada, *PIPEDA Case Summary #2002-60: Airport Employee Demands Access to Personal Information from Airline* (19 July 2002) <http://www.priv.gc.ca/cf-dc/2002/cf-dc_020719_e.cfm>.

54 Office of the Privacy Commissioner of Canada, *PIPEDA Case Summary #2002-89: Passenger Objects to Photograph Taken by Airline Employee During a Flight* (12 November 2002) <http://www.priv.gc.ca/cf-dc/2002/cf-dc_021112_1_e.cfm>.

55 *Ferenczy v MCI Medical Clinics* (2004) 70 OR (3d) 277 (SCJ). This finding seems somewhat incongruous in the context of a lawsuit alleging professional negligence. Although the private investigator was undertaking a commercial activity, it was as the agent of the plaintiff, who was collecting information for the purpose of defending himself against the lawsuit: at [30]. This was distinguished on the basis that the private investigator who took photographs in that case was working for an insurance company rather than an individual. The exemption applies only to individuals, not bodies corporate, which cannot have 'personal or domestic purposes': Office of the Privacy Commissioner of Canada, *PIPEDA Case Summary #2008-392:Individual Objects to Being Photographed by Private Investigation Firm* (27 February 2008) Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/cf-dc/2008/392_20080227_e.cfm>.

- Facebook users posting personal information about non users to their profiles, 'Walls' and 'News Feeds'.[56]

On the other hand, the exemption did not apply to an individual who sought to collect information for personal reasons for his sister, but did so at work in his capacity as company vice president.[57] The executive, whose sister was representing the complainant's ex-wife in a court dispute with the complainant, circulated an in-house email requesting information about the complainant's employer. The Assistant Privacy Commissioner found that the domestic purposes exemption applied only to 'individuals' and 'is not intended to absolve an organization of responsibility for an employee who uses their position within the organization to collect, use or disclose personal information for their own purposes'. It was noted that although the executive 'may have had personal reasons for sending the e-mail, he did not act as an *individual* in doing so. His actions had every appearance of being conducted on behalf of the company, for business-related purposes.'

III THE PRIOR PUBLICATION EXEMPTION

A Publicly Available Publications

Information published on the internet that has its source in a prior publication may be exempted from data protection laws in some jurisdictions based on the prior public availability of the information concerned. The rationale behind this exemption is problematic. On the one hand, it is arguable that if information is already published or in the public domain, the strict requirements of data protection regulation should not apply since the information is no longer private and it would be otiose to impose those requirements. On the other hand, using such information for secondary purposes that are unrelated to the original reason for their collection would be inappropriate if it undermines individuals' rights in respect of their personal information. Thus, the European Court of Justice has remarked that:

> a general derogation from the application of the [European Union personal data] directive in respect of published information would largely deprive the directive of its effect. It would be sufficient for the Member States to publish data in order for those data to cease to enjoy the protection afforded by the directive.[58]

---

56 Elizabeth Denham, Assistant Privacy Commissioner of Canada, *PIPEDA Case Summary #2009-008: Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc under the* Personal Information Protection and Electronic Documents Act (16 July 2009) [306] <www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm>.

57 Office of the Privacy Commissioner of Canada, *PIPEDA Case Summary #2006-346: E-Mail Message Raises Questions about Purposes, Credibility and Accountability* (15 June 2006) Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/cf-dc/2006/346_20060615_e.cfm>.

58 *Satakunnan Markkinapörssi Oy and Satamedia* (C-73/07) [2008] ECR I-9831, [48]. This was a reference from a Finnish data protection case in which the government published an individuals' tax and income information, which was then commercially re-published.

For similar reasons, a recent Hong Kong proposal[59] to exempt personal data available in the public domain[60] from the data collection principle was not pursued.[61] The Privacy Commissioner for Personal Data explained that:

> If the test for exemption is simply whether the data are in the public domain, it would provide data users with the opportunity to subvert the law by publicizing the data. The proposal could result in abuse in the use of information available in the public domain, such as improper use of personal data available on the Internet arising from data leakage incidents.[62]

The prior publication exemption can take various forms. Firstly, it can be limited to government information that the law allows or requires to be publicly available. The publication of the information can be strictly circumscribed by particular conditions, such as a legislative requirement that the information be made available to the public,[63] or that the information be specified in regulations.[64] A second type of exemption arises when the data subject makes information about him or herself publicly available.[65] A third form of exemption is broader. It can cover the first and second forms, and includes information that has been published in generally available publications such as books, newspapers and magazines. The *APEC Privacy Framework*, for example, recognises such an exemption.[66]

New Zealand has an exceptionally broad exemption for 'publicly available information', which is defined as 'personal information that is contained in a publicly available publication'.[67] The expression 'publicly available publication' is defined in turn as 'a magazine, book, newspaper, or other publication that is or

---

59 Office of the Privacy Commissioner for Personal Data (Hong Kong), *PCPD's Information Paper on Review of the Personal Data (Privacy) Ordinance* (9 September 2009), 106–8 <www.pcpd.org.hk/english/review_ordinance/files/Odnreview_Information_Paper_e.pdf>.

60 Ibid 106 [2]. The ambit of the 'public domain' was explained as follows:

> Personal data can be made known in the public domain by various means, such as by being contained in public records and obtainable through public search or inspection, e.g. court documents filed, records kept by public registries, etc. Another means is by way of publication in the media, such as a journalistic report or a public announcement.

61 Office of the Privacy Commissioner for Personal Data (Hong Kong), *Consultation Document on Review of the Personal Data (Privacy) Ordinance* (August 2009) Annex 2, B.2 Public Domain Exemption, 75–6 <www.cmab.gov.hk/doc/issues/PDPO_Consultation_Document_en.pdf >.

62 Ibid 75–6 [19]. See also Office of the Privacy Commissioner for Personal Data (Hong Kong), *PCPD's Information Paper*, above n 59, 107 [8].

63 See *Data Protection Act 1998* (UK) c 29, s 34.

64 See *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, ss 7(1)(d), (2)(c.1).

65 See, eg, *European Union Personal Data Directive* [1995] OJ L 281 31, art 8(e), which contains an exemption to the prohibition of the processing of 'sensitive' data (ie data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life) where the data 'are manifestly made public by the data subject'.

66 Asia-Pacific Economic Cooperation, above n 20, 7 [11] defines the expression 'publicly available information' as

> personal information about an individual that the individual knowingly makes or permits to be made available to the public, or is legally obtained and accessed from:
>
> (a) government records that are available to the public;
>
> (b) journalistic reports; or
>
> (c) information required by law to be made available to the public.

67 *Privacy Act 1993* (NZ) s 6(2)(a).

will be generally available to members of the public; and includes a public register'.[68] The exemption applies to the data protection principles dealing with the collection, use and disclosure of personal information.[69]

Information available on the internet falls into the category of 'publicly available publication' if it can be accessed by the general public.[70] Where information is subject to some form of restricted online access, then there could be a question as to whether the information is 'generally available to members of the public'. Where a restriction to access that limits availability to the general public is merely monetary or requires the performance of some simple task like online registration, this would arguably not take the publication out of the publicly available realm, since the obtaining of publicly available newspapers and magazines in hard copy also commonly involves the payment of money or the registration of a subscription. Moreover, the expression 'members of the public' might well cover a particular section of the public, as it does in human rights law.[71]

In one case, the Privacy Commissioner found that online databases of legal cases made available by government or commercial agencies (whether gratis or for payment) fell under the 'publicly available publication' exemption.[72] Accordingly, personal information obtained from a case accessed from such a database fell under the exemption when it was published on a law firm's website. In another case, a polytechnic language course used the photograph of a woman that had been obtained from an overseas news website. The woman's complaint was not upheld, on the basis that the news website was a publicly available publication. The Privacy Commissioner observed:

> Information on the internet can usually be accessed, and copied, by anyone, anywhere, with an internet connection. Any personal information that is posted on a open website is therefore publicly available.[73]

In a New Zealand Human Rights Review Tribunal case, the scope of the 'publicly available publication' exemption was pushed further, somewhat implausibly, to cover personal information that had been disclosed (or 'published') at a local public meeting concerning health care issues, and was

68 *Privacy Act 1993* (NZ) s 2.

69 See the Information Protection Principle 2(2)(a), 10(a) and 11(b) exceptions: *Privacy Act 1993* (NZ) s 6.

70 This interpretation is supported by the fact that there are many online editions of newspapers and periodicals. See also *Case Note 100413* [2007] NZPrivCmr 20 (1 December 2007), discussed below.

71 Under New Zealand human rights legislation, a well-defined group may be treated as a section of the public: see *Coburn v Human Rights Commission* [1994] 3 NZLR 323, where the High Court held that the employees of a company, together with their families, should be treated as a section of the public for the purposes of the *Human Rights Act 1993* (NZ).

72 *Case Note 100413* [2007] NZPrivCmr 20 (1 December 2007). The complainant had done a Google search of his name on the internet and was surprised to find a reference to himself on the law firm's website. The information related to a case in which he was a party.

73 *Case Note 212156* [2010] NZPrivCmr 8 (1 May 2010).

therefore to be regarded as being in the public domain.[74] The Tribunal's approach, however, failed to take into account the qualification that the publication 'is or will be generally available to members of the public'. Words said and behaviour observed in a local public meeting arguably do not fit this description. It is difficult to see how the general public, or a section of it, could access what transpired at a public meeting unless the information is itself made available in a newspaper, internet news site, or blog. The decision did, however, accept that information on the internet can be a 'publicly available publication':

> if a person places a video piece about themselves on the internet, or keeps a blog, we would have thought that qualifies as a 'publication' of such personal information about the person in question as is contained in the video piece or the blog. It is therefore made 'publicly available'. We see no reason to read the definition of 'a publicly available publication' as excluding that kind of information simply because it is not in magazine, book or other printed form.[75]

Similarly, under the Australian *Privacy Act 1988* (Cth), personal information may be collected or used when it is held in a 'generally available publication',[76] which can include a publicly available website.[77] The difference, however, is that where the information is collected for inclusion in a 'record'[78] or another publicly available publication,[79] then there must be compliance with the collection, notification and data quality privacy principles.[80] These requirements would not apply to an individual making personal use of the internet, but this would be by virtue of the domestic purposes exemption, not a publicly available information exemption.

B Prior Disclosure

A variant of the prior publication exemption can arise where information has been previously disclosed. Here, the issue is whether there has actually been a 'disclosure' if the same information has already been disclosed. This issue has arisen on several occasions in New Zealand case law, where it has been held that there is no disclosure if the personal information concerned has already been disclosed by someone else, or if the information is already known. Disclosure thus entails informing someone else of something that was not previously known.

---

74 *Coates v Springlands Health Ltd* [2008] NZHRRT 17 (11 August 2008) [78]. The Tribunal declined to interpret the phrase 'or other publication' in the definition of 'publicly available information' in a way that followed on from 'magazine, book, newspaper'. The context plainly called for the application of the *ejusdem generis* principle of statutory interpretation.

75 Ibid [79].

76 *Privacy Act 1988* (Cth) s 6(1): 'generally available publication' is defined as 'a magazine, book, newspaper or other publication (however published) that is or will be generally available to members of the public'.

77 Australian Law Reform Commission, above n 26, [11.1], [11.30].

78 Defined as a 'document', or a 'database', or 'a photograph or other pictorial representation of a person': *Privacy Act 1988* (Cth) s 6.

79 *Privacy Act 1988* (Cth) s 16B. See generally Australian Government Office of the Privacy Commissioner, *Information Sheet (Private Sector) 17–2003: Privacy and Personal Information that Is Publicly Available* (February 2003) <www.privacy.gov.au/materials/types/infosheets/view/6549>.

80 *Privacy Act 1988* (Cth) ss 14(1) – (3), (80).

In one New Zealand case investigated by the Privacy Commissioner,[81] no disclosure was found where the personal information concerned had already been disclosed by the person to whom the information related. The individual was complaining about how had been treated by a public sector agency and she provided information about herself to a newspaper reporter. When the agency wished to defend itself, the individual did not agree to the agency's disclosure of her personal information. The agency subsequently responded to the journalist's questions, generally confining itself to the material the individual had raised. In so far as the agency's disclosure of information related to material that the individual had already supplied to the news media, the information was found not to have been disclosed by the agency, as the individual had already supplied it to the reporter.

A subsequent New Zealand Human Rights Review Tribunal decision upheld the Privacy Commissioner's approach,[82] finding support in both British[83] and Australian[84] case law (though these were not dealing with data protection issues). The Tribunal held that 'implicit in the term *disclose* … is the requirement that the information at issue has not already been disclosed by someone else'.[85] A later Tribunal case reiterated that a disclosure of information normally means that its communication is being made to someone who does not already know it.[86] There are additional Tribunal decisions and Privacy Commissioner case notes that follow this line of authority. The basic position is that '[f]or there to be a disclosure under principle 11 it is necessary to show that a third party received information of which it was previously unaware.'[87]

In some situations, however, the mere repetition of information that has already been disclosed can amount to confirmation of the earlier information, and

81 *Case Note 8649* [1997] NZPrivCmr 3 (1 July 1997).

82 *A v G* [1999] NZCRT 18 (13 July 1999).

83 *Bank of Credit and Commerce International (Overseas) Ltd (in liq) v Price Waterhouse* [1998] Ch 84, 101–2, which dealt with the meaning of the term 'disclose' in section 82(1) of the *Banking Act 1987* (UK). The Court noted that 'to disclose information normally entails communicating information to someone who does not know it already. It means to bring to light or reveal something of which the third party was previously unaware.' The Court followed *A-G v Associated Newspapers Ltd* [1994] 2 AC 238, where the House of Lords commented that there was a distinction between 'disclosure' and the 'mere republication of already known facts': at 255.

84 *King v South Australian Psychological Board* [1998] SASC 6621 (9 April 1998). This case concerned the issue of whether a disclosure had been made under the *Whistleblowers Protection Act 1993* (SA).

85 *A v G* [1999] NZCRT 18 (13 July 1999) [35] (emphasis in original).

86 *H v Chief Executive of Work and Income* [2000] NZCRT 40 (19 December 2000).

87 *Case Note 13518* [1999] NZPrivCmr 11 (1 August 1999). See also *Williams v Department of Corrections* [2004] NZHRRT 4 (9 March 2004); *Clearwater v Accident Compensation Corporation* [2004] NZHRRT 2 (23 February 2004); *Director of Human Rights Proceedings v Commissioner of Police* [2007] NZHRRT 23 (13 November 2007), affd on appeal by the High Court: *Director of Human Rights Proceedings v Commissioner of Police* [2008] NZHC 1286 (14 August 2008); *Case Note 51765* [2003] NZPrivCmr 13 (1 June 2003); *Case Note* 67516 [2006] NZPrivCmr 2 (1 March, 2006); *Case Note 94991* [2007] NZ PrivCmr 15 (1 August 2007).

so contribute an additional element to information that was previously known.[88] One Tribunal case conceded that '[t]here may well be circumstances in which confirmation of information constitutes a disclosure because there is fresh information included in the confirmation'.[89]

Naturally, there will be no 'disclosure' in terms of the New Zealand legislation if no-one actually receives the disclosure. The corollary of this, however, is that if a disclosure is made, the fact that it has been received may need to be proved.[90] How this can be technically proved in relation to a disclosure in cyberspace is indicated in an English case that involved the calculation of damages for defamation and misuse of private information where the defendant had set up a false Facebook profile in the name of the plaintiff, as well as a group called 'Has [the plaintiff] lied to you?' that was linked to the plaintiff's profile.[91] The plaintiff was awarded £15,000 for libel and £2,000 for breach of privacy on the basis that the profile and group had been on the internet for 16 days before they were taken down. The Court found that although it was not possible to show how many Facebook users had merely viewed the profile, it was possible to establish the number of users who had performed some online activity in relation to it, which in this particular case was three.[92] The false profile and group were placed on the London network, which at the time had over 850,000 members. The information would have been visible to any of them. In measuring the quantum of damages, the judge stated that:

> I bear in mind … the limited extent of proved publication, but I accept that Facebook is a medium in which users do regularly search for the names of others whom they know, and anyone who searched for the name Mathew Firsht during those few days will have found the false group without difficulty. In my view, a not insubstantial number of people is likely to have done so. By that I have in mind a substantial two-figure, rather than a three-figure, number.[93]

88 See *Case Note 20545* [2003] NZPrivCmr 15 (1 June 2003), where the Privacy Commissioner found that 'confirming facts could constitute a disclosure if that confirmation provided information not previously known to the recipient'.

89 *J v New Zealand Police* [2000] NZCRT 2 (3 March 2000) [20].

90 See, eg, *J v New Zealand Police* [2000] NZCRT2 (3 March 2000), which involved an alleged police disclosure within the hearing of an unknown member of the public who was not called as a witness in the case. The Tribunal commented that 'we would have to have heard from her because we think that in order to show that a disclosure has occurred there must be some evidence of receipt of that which is alleged to have been disclosed'. On appeal*: J v Commissioner of Police* [2001] AP 64 (14 March 2001), the High Court did not disturb the Tribunal's decision. See also *Case Note 35433* [2003] NZPrivCmr 17 (1 September 2003), which involved the issue whether personal information had been 'disclosed' by a return address on an envelope ('Community Probation Service'). The Privacy Commissioner found that although there had been a disclosure, it could only be assumed that a postal worker saw this information.

91 *Applause Store Productions Limited v Grant Raphael* [2008] EWHC 1781 (QB) (24 July 2008). The case established no new principles of liability, but it is an interesting illustration of how the identity of the person posting a false profile on Facebook can be established, as well as how the extent of publication can be measured.

92 Ibid [70].

93 Ibid [78].

IV THE JOURNALISM AND NEWS ACTIVITIES EXEMPTION

An exemption is conventionally made for journalism and associated news media activities in data protection legislation.[94] While dissemination to the general public can tell against the application of the domestic purposes exemption, it is an element that normally goes hand in hand with the journalism exemption.

The journalism exemption has its basis in the right to freedom of expression and the right to receive and impart information, a human right that receives protection in both national[95] and international instruments. Article 19(2) of the *International Covenant on Civil and Political Rights*, for example, provides that:

> Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.[96]

Recognition of this human rights interest is exemplified in the data protection context by recital 37 of the Preamble to the *European Union Personal Data Directive*, which provides:

> Whereas the processing of personal data for purposes of journalism or for purposes of literary of [sic] artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority.[97]

There is also a practical rationale underlying the journalism exemption: it would be unreasonably burdensome in many instances to impose conditions on the collection and disclosure of personal information in the journalistic context. For example, it may be impractical to collect information directly from the individual concerned if information can be independently confirmed, or the publishing of news in a timely manner may be compromised.

The scope of the journalism exemption, however, is neither universally agreed nor entirely clear in some jurisdictions. Some take a restrictive approach

---

94 See, eg, *European Union Personal Data Directive* [1995] OJ L 281 31, art 9; *Privacy Act 1988* (Cth) s 7B(4); *Data Protection Act 1998* (UK) c 29, s 32; *Personal Data (Privacy) Ordinance* (Hong Kong) cap 486, s 61; *Privacy Act 1993* (NZ) s 2(1); *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, ss 4(2)(c), 7(1)(c).

95 See, eg, *New Zealand Bill of Rights Act 1990* (UK) s 14; *Canada Act 1982* (UK) c 11, sch B pt 1 ('*Canadian Charter of Rights and Freedoms*'), pt 1, s 2(b).

96 *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976). Article 19(2), para (3)(a) goes on to qualify this right by providing that it 'carries with it special duties and responsibilities', with the result that it can be subject to legal restrictions that are necessary '[f]or respect of the rights or reputations of others'.

97 *European Union Personal Data Directive* [1995] OJ L 281 31.

and apply the exemption only to 'genuine' or 'serious' news, others tread a more expansive path. The former approach involves the balancing of competing public interests, but the difficulties in defining what is 'real' news tends to end up being resolved in a more expansive approach towards defining what is 'news'. The more expansive approach is more often adopted in the case law, which is beginning to deal with internet based sources of information, and other new media such as SMS (short message service) text messaging.

While the journalism exemption is centred around news and current affairs activities, the scope of subject matter can be quite wide and may include information of an entertainment and educational nature. Some argue that the exemption should be confined to information that is published in the public interest, as opposed to matter in which the public might simply be interested.[98]

Moreover, the broader the interpretation of what constitutes a news activity, the more likely the agencies covered can include non-media agencies.[99] This may mean the exemption could cover material that is of a marketing, advertising, promotional or public relations nature.[100] For example, there are websites where products may be reviewed by consumers.[101] Such material has its parallels in the conventional media, where news stories may actually be a form of disguised advertising or public relations. It can be difficult to draw a line between the two, but it certainly should not depend simply on the criterion of where or in what context such material appears.

One characteristic of the journalism exemption is that the information must be made available to the public. Such case law as exists indicates that this is not a particularly restrictive requirement. It can be satisfied if only a section of the public can access the information. In a New Zealand case,[102] the subscribers to *The New Zealand Beekeeper* magazine constituted a section of the public for the purposes of the exemption, since a 'news activity' under the *Privacy Act 1993* (NZ) meant an activity involving the dissemination of news 'to the public or any section of the public'. Although the magazine was only available to financial members of the National Beekeepers Association of New Zealand, the Tribunal found that the exemption applied because it was available to anyone in the public who wanted to subscribe to it or read it in a public library.[103] The journalism exemption does not require that material be available to the public at large, as

98 See Carmen Vietri, 'The Media Exemption under Information Privacy Legislation: In the Public Interest?' (2003) 8 *Media & Arts Law Review* 191, arguing that the media exemption in data protection legislation tends to be wider than necessary for protecting the policy goals underlying the exemption.

99 Elizabeth Paton-Simpson, 'The News Activity Exemption in the Privacy Act 1993' (2000) 6 *New Zealand Business Law Quarterly* 269, 281.

100 Ibid 284–5.

101 See, eg, Amazon (2010) <www.amazon.com>; Target.com (2010) <www.target.com>; Productreview.com.au: Australia's No1 Product Review Site (2010) <www.productreview.com.au>.

102 *Wallingford v National Beekeepers Association of NZ* [2001] NZCRT 32 (17 November 2000) 251.

103 Moreover, even if dissemination of the magazine were limited to members of an association, there was a binding High Court precedent that had held that a well-defined group sufficed as a section of the public for the purposes of human rights type legislation: *Coburn v Human Rights Commission* [1994] 3 NZLR 323.

this is an issue of circulation, which often involves some limitation on availability to the general public, such as payment or subscription.

A Case Law and Practice

1 *Sweden*

A Swedish case is directly on point in applying the journalism exemption to an individual's internet activities. The Swedish Supreme Court found that a website engaged in a campaign about alleged malpractice in the Swedish banking industry, which included derogatory comments about individuals, fell under the journalistic purposes exemption of the *Personal Data Act 1998* (Sweden).[104] Section 7 of the legislation, which is based on article 9 of the *European Union Personal Data Directive*, makes provision for an exemption for 'such processing of personal data as occurs exclusively for journalistic purposes or artistic or literary expression.'[105]

The case was successfully appealed from the lower courts, which had held that the exemption did not apply because the processing was intended in part to spread derogatory information about the individuals concerned. The Swedish Supreme Court, however, placed emphasis on article 10 of the *European Convention on Human Rights*,[106] which provides that 'everyone' has the right to freedom of expression. European cases routinely attempt to balance article 10 with article 8, which protects the right to privacy,[107] in their domestic case law.[108] While the lower courts had emphasised the fact that the publication denigrated the reputations of individuals in the banking industry, the Supreme Court, referring to the case law of the European Court of Human Rights, noted that the right to freedom of expression included the right to communicate information

---

104 *Case B 293-00* (12 June 2001) (in Swedish) <www.bankrattsforengen.org.se/hddomslut.html>. For an English account and analysis of the judgment, see Lee Bygrave, 'Balancing Data Protection and Freedom of Expression in the Context of Publishing – Recent Swedish Case Law' (2001) 8 *Privacy Law and Policy Reporter* 40.

105 Bygrave, above n 104, 40.

106 *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953) ('*European Convention on Human Rights*').

107 *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953), art 8 provides:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

108 See, eg, one of the leading British privacy cases: *Campbell v MGN Ltd* [2004] 2 AC 457, 465 [16]–[17]:

> The European Convention on Human Rights, and the Strasbourg jurisprudence, have undoubtedly had a significant influence in this area of the common law for some years. The provisions of article 8, concerning respect for private and family life, and article 10, concerning freedom of expression, and the interaction of these two articles, have prompted the courts of this country to identify more clearly the different factors involved in cases where one or other of these two interests is present. Where both are present the courts are increasingly explicit in evaluating the competing considerations involved. … The time has come to recognise that the values enshrined in articles 8 and 10 are now part of the cause of action for breach of confidence.

and opinions that 'mortify, shock or disturb'.[109] While such communications might be exempt from data protection law, they could still involve legal liability under the law of defamation.

The Supreme Court found that the journalism exemption was intended to extend beyond the established mass media and people who were not professional journalists. The Court noted that a basic purpose of journalistic activity was 'to inform, exercise criticism and provoke debate about societal questions that are of larger significance for the general public',[110] and the website satisfied this purpose.

The Court indicated that publications that were of a 'purely private character' would not fall under the journalism exemption, but even if the information published was for mixed journalistic and private purposes, that could still bring the information under the journalism exemption.[111] That said, as discussed earlier, if a publication is of a private nature, it could still fall under the domestic purposes exemption.

2 *Finland*

In a reference for a preliminary ruling on the interpretation of the *European Union Personal Data Directive* in relation to the activities of two Finnish news media organisations, the European Court of Justice held that it is up to Member States to reconcile the right to privacy and right to freedom of expression in their national laws.[112] Under Finnish law, information about the income and tax liability of individuals (as well as date of birth) was in the public domain and national law provided that the right to public access to this information prevailed over the law on personal data.

A media organisation collected public data from the Finnish tax authorities and published extracts in regional editions of a newspaper each year relating to individuals whose income exceeded certain levels. While the newspaper also contained articles and advertisements, its main purpose was to publish personal tax information. Some of this information was transferred to another branch of its organisation, Satamedia, so that the information could be published by a text messaging service. This allowed mobile phone users to receive the information published in the newspaper for a charge. One of the issues in the reference to the European Court of Justice was whether the information in question that was processed for the text messaging service could be regarded as being processed solely for journalistic purposes within the meaning of the *European Union Personal Data Directive*.

The Court held that the journalism exemption applies not only to media undertakings, 'but also to every person engaged in journalism',[113] and that where

109 Bygrave, above n 104, 41

110 Ibid.

111 Ibid.

112 *Satakunnan Markkinapörssi Oy and Satamedia* (C-73/07) [2008] ECR I-9831, [52]–[55].

113 Ibid [58].

documents that are in the public domain under national legislation and where the sole object of processing the personal data is to disclose to the public information, opinion or ideas, then such activities must be considered as being carried out for journalistic activities.[114] The Court's approach to the ambit of the journalism exemption was as follows:

> In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary, first, to interpret notions relating to that freedom, such as journalism, broadly. Secondly, and in order to achieve a balance between the two fundamental rights, the protection of the fundamental right to privacy requires that the derogations and limitations in relation to the protection of data provided for in the chapters of the directive referred to above must apply only in so far as is strictly necessary.[115]

The Court went on to note that the particular medium used for the dissemination of information, 'whether it be classic in nature, such as paper or radio waves, or electronic, such as the internet, is not determinative as to whether an activity is undertaken "solely for journalistic purposes"'.[116]

3 *New Zealand*

New Zealand case law on the news media exemption takes a broad approach to the ambit of the exemption. This could be argued to be in line with the right to freedom of expression, which is protected by section 14 of the *New Zealand Bill of Rights Act 1990*. The *New Zealand Bill of Rights Act 1990* requires that other statutes (such as the *Privacy Act 1993* (NZ)) should be interpreted in a way that is consistent with the rights in the *New Zealand Bill of Rights Act 1990*.[117] Accordingly, the right to freedom of expression is a value that must be considered when any other statute purports to limit it, with any limitation required to be narrowly interpreted in light of the *New Zealand Bill of Rights Act 1990*.

The New Zealand definition of 'news medium' refers to 'any agency whose business, or part of whose business, consists of a news activity',[118] including publications on the internet.[119] The term 'business' is somewhat ambiguous. It could have a commercial connotation, but it is can also be used in a neutral sense denoting 'a pursuit or occupation demanding time or attention'.[120]

'News activity', in turn, while defined in the legislation as focusing on news or current affairs,[121] has been subject to broad interpretation in the case law. In its

---

114 Ibid [61]–[62].

115 Ibid [56].

116 Ibid [60].

117 *New Zealand Bill of Rights Act 1990* (NZ) s 6 provides that '[w]herever an enactment can be given a meaning that is consistent with the rights and freedoms contained in this Bill of Rights, that meaning shall be preferred to any other meaning'.

118 *Privacy Act 1993* (NZ) s 2.

119 *Coates v Springlands Health Ltd* [2008] NZHRRT 17 (11 August 2008) [79].

120 *Oxford English Dictionary* (Oxford University Press, 2nd ed, 1989). For discussion of this aspect of the definition, see Paton-Simpson, above n 99, 281–2.

121 *Privacy Act 1993* (NZ) s 2 defines 'news activity' as

> (a) The gathering of news, or the preparation or compiling of articles or programmes of or concerning news,

recent review of the *Privacy Act 1993* (NZ), the New Zealand Law Commission queried 'whether it would be possible to define "news activity" with any greater precision', and went on to observe that '[g]iven the increasingly unclear line between news and entertainment, and the uncertain boundaries of even the term "news" itself, that would be a very difficult undertaking'. [122]

New Zealand case law illustrates the wide scope of what falls under the rubric 'news'. The publication of a list of the wealthiest New Zealanders ('The Rich List') by a business periodical, for example, was found to be a 'news activity'.[123] The Tribunal identified two possible approaches to the issue: a narrow, one focusing on the particular contents of the item in question; and a broad one focusing on the publication as a whole. The Tribunal found that The Rich List satisfied both tests. The latter approach was favoured by both the defendant publisher and the Privacy Commissioner because it avoided having to deal with subjective judgments about what was or was not news or current affairs, or what was in the public interest.

Another New Zealand case concerned the publication of correspondence in the letters to the editor column of a periodical aimed at a specialist audience, *The New Zealand Beekeeper*.[124] The complainant alleged that he had been anonymously maligned in several letters to the editor and he requested the identity of the author.[125] The issue therefore was whether or not the agency could withhold the information on the basis that it fell under the news activities exemption. The Tribunal applied the exemption to include letters to the editor on the basis that these should not be severed from the surrounding publication when determining whether or not a particular activity is a 'news activity'. The Tribunal commented that '[t]he important point is that it is the publication as a whole (e.g. the journal or the newspaper or the magazine) which is under scrutiny, not the individual pieces which are contained within that publication'.[126]

Also illustrating New Zealand's wide approach was the Privacy Commissioner's view in one case that a consumer television program, in which

---

observations on news, or current affairs, for the purposes of dissemination to the public or any section of the public;

(b) The dissemination, to the public or any section of the public, of any article or programme of or concerning –
  (i) news;
  (ii) observations on news;
  (iii) current affairs.

122 New Zealand Law Reform Commission, *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4*, Law Commission Issues Paper No 17 (2010) 131 [5.30]. The Australian Law Reform Commission, however, has recommended that the *Privacy Act 1988* (Cth) be amended to define 'journalism' and 'media organisation', and that such organisations be required to be committed to adequate privacy standards: see Australian Law Reform Commission, above n 26, 54–5, (Recommendation 42.1, 42.2, 42.3). This lack of definition was criticised in submissions as effectively allowing anyone to benefit from the exemption by simply setting up a publishing enterprise: vol 2 1446 [42.26].

123 *Talley Family v NBR* (1997) 4 HRNZ 72.

124 *Wallingford v National Beekeepers Association of NZ* [2001] NZCRT 32 (17 November 2000) 251.

125 Under New Zealand privacy and freedom of information law, information about oneself includes the source or author of information or opinion material about the individual concerned.

126 *Wallingford v National Beekeepers Association of NZ* [2001] NZCRT 32 (17 November 2000) 251, 255.

tradesmen were surreptitiously filmed while performing their tasks for actors pretending to be householders, constituted a 'news activity'.[127] This was on the basis that tradesmen's activities in private homes were a matter of public interest and related to current affairs.

Where the disclosure of information on the internet is not covered by a news media or news activity exemption, its collection for use in journalistic activities may nevertheless be covered by the exemption, or alternatively by the 'publicly available publication' exemption discussed earlier. For example, the news media exemption extends to the collection of information by way of background research that feeds into journalistic activities. In one case, the Privacy Commissioner found that the making of unauthorised personal credit checks with a credit reporter came within the news medium exemption on the basis that the information was being collected by a business publication in order to test the accuracy of information it had received for a story on a couple who were shareholders and directors of a small publishing company.[128] Accordingly, the collection or checking of background information via social networking or other internet sites for publication purposes may also fall under the journalism exemption by a similar extension.

4 *Hong Kong*

The 'news activity' exemption in section 61 of Hong Kong's *Personal Data (Privacy) Ordinance* (Hong Kong) chapter 486 is defined along similar lines to New Zealand's, but it seems to have been interpreted more restrictively.[129] The Privacy Commissioner has noted that the natural meaning of 'news' is 'information about recent events or happenings, especially as reported by newspapers, periodicals, radio or television'.[130] In the one case, for example, the Privacy Commissioner found that a feature on dress sense and individual taste in clothes did not amount to a news activity, since it 'was based on the random thoughts of the reporter rather than a report on fashion trends', and that 'the

127 *Case Note 38197* [2003] NZPrivCmr 24 (1 September 2003).

128 *Case No 48423* [2002] NZPrivCmr 6 (1 May 2002).

129 *Personal Data (Privacy) Ordinance* (Hong Kong) cap 486, s 61: 'news activity' is defined as

(a) the –

(i) gathering of news;

(ii) preparation or compiling of articles or programmes concerning news; or

(iii) observations on news or current affairs, for the purpose of dissemination to the public; or

(b) the dissemination to the public of

(i) any article or programme of or concerning news; or

(ii) observations on news or current affairs.' For New Zealand's definition, see *Privacy Act 1993* (NZ) s 2.

130 Office of the Privacy Commissioner for Personal Data (Hong Kong), *Data Protection Principles*, above n 45, 122 [12.59].

taking of the complainant's photograph to illustrate such an article, did not amount to news gathering'.[131]

The exemption is mainly for the protection of news sources,[132] but only where it is reasonably believed to be in the public interest.[133] The expression 'public interest' is not defined in the legislation, but the Privacy Commissioner has noted that a 'fine distinction may need to be drawn between what the public is interested in knowing and what public interest there exists in disclosing the information'.[134] One case dealing with the concept concerned the disclosure to media reporters of information relating to a college staff member by the principal of the college.[135] The information concerned was contained in an accident investigation report relating to an employee compensation claim. The complainant's wife was alleging that the college was procrastinating in paying compensation to the complainant. The principal, confronted by reporters, sought to rebut this allegation, and disclosed information contained in the investigation report. In dealing with the staff member's complaint to the Privacy Commissioner, the college raised the news activity exemption as a defence. The principal had reasonable grounds for believing that disclosure was in the public interest, since it was to defend the college's image and enable journalists to present a balanced news report. The Commissioner was satisfied that the exemption applied to this situation, and this view was upheld on appeal to the Administrative Appeals Board.[136]

The Privacy Commissioner has written that he 'is inclined to take a broad view of what constitutes the 'public interest',[137] and that having access to public information and a free press in itself constitutes a public interest. When information is disclosed to the media for 'serious' news reporting, the public interest argument will be even more compelling.

B The Democratisation of Journalism

The advent of the internet has enabled nearly anyone to become a 'journalist' of one sort or another. Individuals can post 'news' (however broadly defined) on their own websites, or can contribute or share news in web 2.0 communities. Accordingly, it may be overly artificial nowadays to distinguish journalists from

131 *Eastweek Publisher Limited v Privacy Commissioner for Personal Data* [2000] 2 HKLRD 83; Office of the Privacy Commissioner for Personal Data (Hong Kong), *Data Protection Principles*, above n 45, 122 [12.59]. Justice Keith, the judge at first instance, however, did not make any ruling on the nature of the reporting activities, but simply noted that it was open for the Privacy Commissioner to come to such a view.

132 Office of the Privacy Commissioner for Personal Data (Hong Kong), *Data Protection Principles*, above n 45, 122 [12.57], [12.59].

133 *Personal Data (Privacy) Ordinance* (Hong Kong) cap 486, s 61(2).

134 Office of the Privacy Commissioner for Personal Data (Hong Kong), *Data Protection Principles*, above n 45,124 [12.65].

135 Ibid 123 [12.63].

136 Ibid 124 [12.64]. The Board, however, did not further elucidate the meaning of 'public interest', and remarked that each case needed to be decided on its own facts.

137 Ibid 124 [12.65].

others who are conveying 'news' or news related matters within a framework oriented to providing people with information.

One point of distinction might be whether or not the individual or agency undertaking news activities is run as a commercial enterprise. Some media, however, are non-profit. As one commentator has noted:

> The alternative press plays an important role in the marketplace of ideas, providing an outlet for radical and dissenting thought. Any interpretation denying coverage under the [news medium] exemption to non-commercial media would undermine the purpose of the exemption of protecting press freedom.[138]

Another point of distinction might be whether the individual or agency is bound by a code of ethics or some regulatory scheme, whether statutory or self-regulatory. All sources of information, however, whether the conventional media or not, are subject to limits imposed by the general law, which includes sanctions for defamation, invasion of privacy (in so far as recognised by the criminal and civil law), and contempt of court (in cases where suppression orders have been breached).

One might query whether it is necessary for journalistic activities to satisfy particular professional standards in order to benefit from the exemption if the underlying reason for it is freedom of expression and freedom of the press and freedom of expression, since 'the press' can take a variety of forms and has essentially been 'democratised' by the internet. Moreover, internet sources of news and analysis can, at least in some instances, be more accurate and less susceptible to latent editorial or commercial influence than the conventional news media, or may publish information that is not published elsewhere.[139]

While it would be drawing an impossibly long bow to assert that all or most web 2.0 publications ought to fall under a news media exemption, there are some activities to which the exemption really ought apply. The European Union Article 29 Working Party has suggested that if the domestic purposes exemption does not apply to social networking services, 'the SNS user may benefit from other exemptions such as the exemption for journalistic purposes, artistic or literary expression', in which case 'a balance needs to be struck between freedom of expression and the right to privacy'.[140]

The strongest case could be made for the inclusion of at least some blogs under the news media exemption, though there would be inevitable problems in definition as to what qualifies as journalism or a news activity across the range of legislation found from jurisdiction to jurisdiction, as noted above. There are many bloggers with specialist knowledge or expertise, so that there is now often

---

138 Paton-Simpson, above n 99, 282.

139 See, eg, WikiLeaks (2010) <www.wikileaks.org> and Cryptome (2010) <www.cryptome.org>, which publish anonymously submitted sensitive or controversial documents from governments and other organisations. For an example of personal information that has been published on WikiLeaks, see *Deborah Jeane Palfrey Washington DC Prostituion Service Phone Records* [sic] (11 May 2008) WikiLeaks <wikileaks.org/wiki/Deborah_Jeane_Palfrey_Washington_DC_prostituion_service_phone_records>. The publication of material on these sites sometimes leads to conventional press coverage of a story.

140 Article 29 Data Protection Working Party, above n 15 [3.1.2].

a symbiotic relationship between the mainstream media and the 'blogosphere', with each consulting or quoting the other in the course of their activities. Reporters are now as likely to use Google to hunt relevant information from blogs in their research, as bloggers are in using mainstream media reports as the basis of their discussions.

The issue whether bloggers should be treated on the same basis as the conventional media is a subject of much online discussion,[141] but the principal difference that is of significance is that conventional media are subject to various accountability mechanisms, such as codes of ethics and, in many instances, complaints processes, whereas bloggers are not. While some blogs have quite high journalistic standards,[142] or present expert views and reviews of a variety of matters,[143] others may be purveyors of misinformation, public relations guff, prejudice, or are simply cyberspace soapboxes for venting the author's pet peeves. Blogs associated with established online and non-online newspapers and magazines do not pose a problem. There would, however, be issues concerning the ambit of the journalism exemption for blogs that do not enjoy such an association, given that blogs range so widely in quality.

In some jurisdictions and contexts, there is an emerging recognition that some blogs should be treated as bona fide media activities. In the US, for example, two political blogs have been found to be media rather than political entities for the purposes of the *Federal Election Campaign Act of 1971*,[144] and thus enjoy an exemption from federal campaign finance regulation.[145] This exemption gives bloggers the right to free speech on the same basis as the media, rather than subjecting them to the limits imposed by electoral law. Another recent example is the offer by the Mayor of New York City to treat bloggers on the same basis as journalists by offering two year press passes to those who can produce clips to prove they attended six media only events.[146]

V CONCLUSION

This article has attempted to show that data protection regulation is not an effective means for dealing with privacy issues arising from individuals' web 2.0

141 See, eg, Ira Brodsky, *Blogosphere vs. Mainstream Media* (14 February 2005) Network World <www.networkworld.com/columnists/2005/021405brodsky.html>.

142 See, eg, The Huffington Post (2010) <www.huffingtonpost.com>.

143 See, eg, TechCrunch (2010) <techcrunch.com>.

144 2 USC § 431 (1972).

145 Federal Electoral Commission, 'FEC Resolved Two Matters Involving Internet Activity; Applies Media Exemption to Political Blogs' (Press Release, 4 September 2007) <www.fec.gov/press/press2007/20070904murs.shtml>.

146 This was in response to a federal suit filed by two bloggers against New York City's press-credentials policy, whereby only press journalists were able to attend official news conferences: see Emily Laermer, *City Hall Set to Admit Bloggers to Media Events* (19 March 2010) Crain's New York Business <www.crainsnewyork.com/article/20100319/SMALLBIZ/100319860>. This policy, however, would only assist bloggers like those who had brought the federal suit, since they were journalists who lost their press credentials after leaving their print media positions.

activities, not least because there are difficulties in determining the ambit of the various exemptions, which can vary from jurisdiction to jurisdiction. This conclusion is reinforced by the actual dearth of data protection cases that deal with web 2.0 issues.

Data protection regulation is an inappropriate way of dealing with web 2.0 activities mainly because of their cross border nature and their sheer extent. If existing exemptions were removed or relaxed, complaints systems would be likely to be swamped. Whether data protection regulation should, in principle, even apply to web 2.0 activities is also debatable. While individuals should be protected from misuse of their personal information that could seriously harm their interests, freedom of expression and communication with others are also important values that need to be protected. The remedies for misuse of individuals' personal information in the web 2.0 context lies better in a combination of measures, which include reforming the law in small but effective ways, and introducing engineered solutions to web design.

The online environment is probably best left to be governed by existing conventional causes of action and criminal offences, rather than data protection law. These would include actions for defamation, the invasion of privacy tort (where recognised), and computer misuse offences in the criminal law. Such remedies tend to winnow out the frivolous or *de minimis* cases, of which there would no doubt be many if the floodgates were opened to a more easily invoked remedy. There is probably also a need, however, for new remedies in respect of internet activities, such as 'take down' orders, 'internet trespass' orders, and the legal imposition of time limits after which information must be removed from web pages at the option of the data subject.

Reliance on legal solutions, however, is not sufficient for protecting peoples' privacy interests, as it will only tend to cover the more serious situations, usually after harm has already been done. Privacy interests in the online environment should also be protected through innovations in web design. Building in privacy protection could involve, for example, the sending of automated 'red ears'[147] warnings or the seeking of authorisation when another individual is being tagged in a photograph or mentioned on a website.[148] With the further development of facial recognition and content based image retrieval technologies,[149] such warnings might also be generated upon the posting of an individual's image or other images associated with a particular individual. Measures might also be

147 So-called after the superstition that a person's ears turn red when someone is talking about them.

148 See, eg, Hogben (ed), above n 5, 21 (Recommendation SN 12). See also the reference to tagging management tools in Article 29 Data Protection Working Party, above n 15, 7 fn 13. Office of the Privacy Commissioner of Canada, *PIPEDA Case Summary: E-Mail Message*, above n 57, 75–6 [310]–[313]: it was found that Facebook was not legally responsible for ensuring that tagged non-users gave their consent to use of their personal information, but rather, the onus was on the user to obtain consent. Facebook, however, needed to exercise due diligence to see that users obtained such consent from third parties.

149 Hogben (ed), above n 5, 9–10. Content based Image Retrieval would be able to match particular location-specific features in images (such as furniture, paintings, or fixtures in a room) in a large database of images.

introduced to prevent 'spidering' by bots or web crawlers, and the wholesale harvesting of personal information on the internet.[150]

Individuals could also be given the option of choosing the self-destruction of obsolete information, or enabling their destruction, after the lapse of a certain period of time.[151] This would, for example, prevent future prospective employers from using social networking and other websites for vetting purposes when personal information is out of date or simply embarrassing. The Royal Academy of Engineering has suggested that Digital Rights Management technology, currently used for the sale of music over the internet, might also be able to be harnessed to protect individuals' personal information:

> Applying this technology to information posted on the Web could allow information to be posted for limited amounts of time, or could allow information to be publicly available on the Web but not copied by others – meaning that the author of the information had control over the amount of time for which it was available, and could also rule out the possibility of the information being altered. Thus it could be used to protect the authors of blogs and the users of social networking sites.[152]

No doubt further ideas for designing solutions to enhance individuals' privacy will emerge in the coming years. The law, however, is unlikely to play a very large role, except along the fringes.

150 See Bing Liu, *Web Data Mining: Exploring Hyperlinks, Contents, and Usage Data* (Springer, corrected 2nd printing, 2007) 273–317.

151 Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (March 2007) 40 [7.2.1] <www.raeng.org.uk/policy/reports/default.htm>: 'For example postings to websites might be automatically destroyed after a certain period of time, unless the end user confirmed they wished to have the material retained.'

152 Ibid.