PRIVACY IN THE DIGITAL ERA: HUMAN RIGHTS ONLINE?

DANIEL JOYCE*

This commentary focuses on the United Nations General Assembly's Resolution 68/167 *on the right to privacy in the digital age and continuing developments in this area. The key questions I explore are whether such developments are welcome, and whether human rights law is being used in a meaningful way in the face of complex technological change and our fears regarding the reality of mass surveillance and big data analytics. To do so I offer commentary and critique of the present articulation of a right to privacy in the digital age and consider broader theoretical and doctrinal difficulties associated with privacy. The idea of digital privacy connects with a broader project — the digital rights movement — and engages questions regarding the translation of human rights into digital contexts. The commentary moves to consider the work of Marko Milanovic and Fleur Johns to illuminate the tensions and possibilities in this developing field. A right to digital privacy is one strategy to address concerns in the aftermath of the National Security Agency surveillance scandal, but ultimately a much larger question regarding liberty and collective political resistance is involved.*

CONTENTS

I INTRODUCTION

In the wake of revelations that the United States and the United Kingdom had conducted mass surveillance programs of their own and others' citizens, and shared much of the data with select allies and cooperating intelligence agencies ('the Snowden revelations'),[1] it was reported that sales of George Orwell's classic examination of the surveillance state, *1984*, had surged.[2] The Big Brother of science fiction had taken contemporary form and significance. Along with this literary revival, the response to the National Security Agency ('NSA') surveillance scandal has been accompanied by a renewal of interest in privacy as

* Lecturer, UNSW Law; Project Director, Digital Media and Human Rights, Australian Human Rights Centre; Affiliated Research Fellow, Erik Castrén Institute of International Law and Human Rights, University of Helsinki. The author would like to thank the Editors of this journal, Fleur Johns, Lyria Bennett Moses, Kirsty Hughes and participants in the UNSW Law 2015 writing retreat where this article was conceived and commenced.

1 See generally Ewen Macaskill and Gabriel Dance, 'NSA Files: Decoded', *The Guardian* (online), 1 November 2013 <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>; Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* (Hamish Hamilton, 2014).

2 Danielle Kucera, 'Sales of Orwell's *1984* Skyrocket amid US Spying Scandal', *The Age* (Melbourne), 13 June 2013.

a human right. This prompts the question whether a right to privacy can help us analyse and regulate against the incursions on liberty which have been increasingly routinised in our daily ritual usage of information and communications technologies and in the harvesting, accumulation and analysis of big data by our governments, communities, corporate actors and employers. We used to think that Big Brother would always take the form of the state in Orwellian terms. Then slowly commentators pointed to the dangers posed by transnational actors and companies: why were we worried about our governments when our local supermarket or our internet service or phone provider held incredibly sensitive personal information about us? The Snowden revelations point to yet another variation on this theme: that public and private actors now both act in ways which are potentially invasive and detrimental to our liberty, and often do so together.

This commentary focuses on the United Nations General Assembly's *Resolution 68/167* on the right to privacy in the digital age, the issues arising from *Resolution 68/167* and continuing developments in this area.[3] The key questions I explore are whether such developments are welcome, and whether human rights law is being used in a meaningful way in the face of complex technological developments and our fears regarding the reality of mass surveillance and big data analytics. There are many ways in which these issues can be explored and this article aims to contribute to a deeper conversation within international law scholarship regarding 'digital privacy' and the translation of rights to 'online' contexts. I draw on some domestic developments where necessary, but do not seek to provide either a grand theory of digital privacy or a doctrinal analysis which holds the human rights line that there are laws X and Y and they have been violated in context Z. Either path is significant and necessary, but these are early days in analysing digital privacy and the problems associated with it. It is the task of preliminary analysis and critique which this commentary undertakes.

II A RIGHT TO DIGITAL PRIVACY?

On 18 December 2013, the General Assembly adopted *Resolution 68/167* entitled '*The Right to Privacy in the Digital Age*',[4] co-sponsored by 57 member states. Although adopted without a formal vote and in the soft law manner of the General Assembly, *Resolution 68/167* represents an important development in the move to protect privacy in the digital era and at the international level. The focus of *Resolution 68/167* is on privacy in the digital age, but the *Resolution* can also be seen as a direct and critical rebuke from the international community following the Snowden revelations. *Resolution 68/167* was sponsored by Germany and Brazil, two states that were both affected and embarrassed by the surveillance. Thus, whilst the language of the *Resolution* adopts the reiterative and rather neutral tone of many such resolutions, it can be seen as a significant political move to focus attention on the kind of privacy-intrusive mass surveillance enabled by the internet and digital media environment.

---

[3] *The Right to Privacy in the Digital Age*, GA Res 68/167, UN GAOR, 3rd Comm, 68th sess, 70th plen mtg, Agenda Item 69(b), UN Doc A/RES/68/167 (21 January 2014, adopted 18 December 2013) ('*Resolution 68/167*').

[4] Ibid.

Resolution 68/167 begins by noting 'the rapid pace of technological development' which, on the one hand, 'enables individuals all over the world to use new information and communication technologies', and yet, on the other hand, also 'enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection', which can result in human rights violations.[5] The broader imperative then is to focus on these developments through the lens of human rights law and especially the right to privacy in art 12 of the *Universal Declaration of Human Rights* ('*UDHR*')[6] and art 17 of the *International Covenant on Civil and Political Rights* ('*ICCPR*').[7]

Privacy is reaffirmed as a mechanism for 'realization of the right to freedom of expression', as opposed to a view that privacy is itself a limit upon expression with its democratic significance.[8] In referring to freedom of expression, *Resolution 68/167* stresses the two-way character of the freedom and its significance in terms not only of imparting, but also seeking and receiving, information. Particular emphasis is given to 'the fundamental importance of access to information and democratic participation'.[9]

Privacy as a human right is not to be underplayed in terms of its broader public or even democratic significance. As with the move elsewhere towards translating free speech for 'new' digital- and especially internet-based contexts, particular importance is given to the idea of speech and privacy in terms of the development of norms regarding information and the increasing value attached to ensuring 'access to information' as being a meaningful way of securing human rights online.[10] The use of a human rights framework as a means to bridge and unify otherwise contestable and competing values is familiar and deployed within *Resolution 68/167* in a variety of ways. Connection is made to Frank La Rue's work as UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and to his report on 17 April 2013 analysing 'the implications of States' surveillance of communications for the exercise of the human rights to privacy and to freedom of opinion and expression'.[11]

The context for *Resolution 68/167* is that of 'unlawful or arbitrary surveillance and/or interception of communications, as well as … [the] collection of personal data'.[12] The *Resolution* notes the background justification for such activity, namely 'public security' and combating 'terrorism', but reaffirms that

---

5 Ibid Preamble para 4.

6 *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/810 (10 December 1948).

7 *International Covenant on Civil and Political Rights*, opened for signature 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

8 *Resolution 68/167*, UN Doc A/Res/68/167, Preamble para 5.

9 Ibid Preamble para 6.

10 See, for example, the articulation of 'internet freedom' as a human right: Hillary Rodham Clinton, 'Remarks on Internet Freedom' (Speech delivered at The Newseum, Washington, DC, 21 January 2010) <http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm>; Frank La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN GAOR, 17th sess, Agenda Item 3, UN Doc A/HRC/17/27 (16 May 2011).

11 Frank La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN GAOR, 23rd sess, Agenda Item 3, UN Doc A/HRC/23/40 (17 April 2013) 3 [1].

12 *Resolution 68/167*, UN Doc A/Res/68/167, Preamble para 8.

any such measures should be international law compliant.[13] Of interest here is whether privacy, or indeed human rights, should be given such emphasis in our regulatory response to these issues. Paragraph 1 of *Resolution 68/167* reaffirms the right to privacy as found in the key international human rights frameworks. A related concern is whether the idea of 'digital privacy' involves a process of retranslation and interpretation of this underlying right, thereby bringing traditional principles and jurisprudence up to speed with technological change and development, or whether this 'digital right' might involve new normative developments and ultimately require separate forms of recognition, not only in soft law terms, but also in future recognition such as in the form of a multilateral treaty. Such debates run parallel with debates over what is termed 'internet freedom'.[14]

A methodological weakness of the *Resolution*'s approach is linked with its symbolic affirmation of the need to migrate the protections afforded 'offline', such as privacy, to the 'online' world. Paragraph 2 of *Resolution 68/167* recognises 'the global and open nature of the internet and the rapid advancement in information and communications technologies as a driving force in accelerating progress towards development in its various forms'. This is reminiscent of the blended discourse of development within an information society as witnessed in the World Summit on the Information Society process and framework which has been led by the International Telecommunications Union. Again, that process appears to have stalled in the grip of anxieties regarding multilateral governance of the internet.[15]

Paragraph 3 of *Resolution 68/167* affirms a demarcation between online and offline spaces: 'the same rights that people have offline must also be protected online, including the right to privacy'. To some degree this recognises the permeation of the internet into all aspects of modern life. Indeed, recently Eric Schmidt, the Chief Executive Officer of search and digital media giant Google, remarked that the internet is becoming so ubiquitous that it will soon 'disappear' from our lives.[16] It is in that sense that the online and offline aspects of life will lose any clear or perceived sense of boundary or difference. But such an emphasis in *Resolution 68/167* is also reminiscent of the foundational binary of privacy law: that of public and private which itself has obscured the fact that often both are blurred or that different contexts and facts exist at varying points along a continuum between public and private. Privacy scholarship itself has begun to question these boundaries between public and private and to begin to

---

13 Ibid Preamble paras 9, 11.

14 For a useful overview of developments, see Stephen Tully, 'A Human Right to Access the Internet? Problems and Prospects' (2014) 14 *Human Rights Law Review* 175.

15 See generally Daniel Joyce, 'Human Rights and the Mediatization of International Law' (2010) 23 *Leiden Journal of International Law* 507.

16 Richard Carter, 'Internet Will "Disappear", Google Boss Eric Schmidt Tells Davos', *The Sydney Morning Herald* (Sydney), 23 January 2015.

examine privacy, say, in public places, or to explore the necessity of preserving anonymity in the otherwise public sphere context of the internet.[17]

Resolution 68/167 represents somewhat of a back to the future approach to privacy protection, affirming the ongoing relevance of the analogy of privacy to new contexts such as the internet and mass digital surveillance. The familiar and universalising reach of human rights discourse here both individuates and erases differences, including contextual differences and the deeper question of whether 'digital rights' might in fact need to be rather different. This aspect is rhetorically persuasive, but more needs to be done in terms of understanding not only the problems involved in digital translation of rights, but also in appreciating new contexts on their own terms. The move here politically is nevertheless a useful and simple one — there is a right to privacy and it should be enforced online and in relation to mass surveillance of the kind revealed by the whistleblower Edward Snowden.

However, the more troubling question regarding the longer term utility of the privacy lens and language is pushed to one side and rather simply *Resolution 68/167* calls upon all states '[t]o respect and protect the right to privacy, including in the context of digital communication',[18] to ensure that their procedures, practices and laws are human rights compliant in this regard, and to take relevant measures, including via legislation, to comply with the international framework for privacy protection.[19]

A further aspect which is emphasised in the compliance aspects of paras 4 and 5 of *Resolution 68/167* is the need for relevant, effective and ongoing mechanisms for independent review and scrutiny of state surveillance and data collection. Domestic scrutiny is to be accompanied by UN systemic reporting, and the UN High Commissioner for Human Rights is requested by the General Assembly to

> submit a report [to the Human Rights Council] on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale[20]

with the question to be placed more permanently on the agenda of the General Assembly and other UN human rights institutions.

It is not clear then whether anything new is offered in terms of 'digital privacy' as a means to further develop privacy norms and address conceptual and analytical difficulties which have long plagued the field. Another difficulty is that the *Resolution*'s language reaffirms the metaphor of the internet as a geographical space. This is helpful in terms of understanding the reach, and mapping the networks, of our digital interactions, but it is less helpful to rely on

---

17 See Kirsty Hughes, 'No Reasonable Expectation of Anonymity?' (2010) 2 *Journal of Media Law* 169, 170, 177–8; Kirsty Hughes, 'A Behavioural Understanding of Privacy and Its Implications for Privacy Law' (2012) 75 *Modern Law Review* 806, 835–6; Beate Roessler and Dorota Mokrosinska, 'Privacy and Social Interaction' (2013) 39 *Philosophy and Social Criticism* 771; Megan Richardson, Julian Thomas and Marc Trabsky, 'The Internet Imaginary and the Problem of Privacy' (2012) 17 *Media & Arts Law Review* 257.

18 *Resolution 68/167*, UN Doc A/Res/68/167, para 4.

19 Ibid.

20 Ibid para 5.

a bounded and property-focused sense of the internet as either commercial real estate or as the commons revived. Of course, the internet is reminiscent of both of these aspects, but traditional conceptions of property may obscure, rather than enable, its true possibilities and its complexity.

A further danger is that this view of the internet as a virtual extension of the public sphere removes from view its alternative and rather darker dimensions, dimensions with which of course the Snowden revelations share a lineage. It is too easy to forget the military and strategic origins of the internet and to focus on its civic promise and its countercultural significance. The spatial analogy is not without its uses, but rather than a real estate model (at least in international law terms), a more creative and compelling model might be that of the sea, with its history, romance, innovation, exploitation as a resource, estrangement, danger, militarism, outlaws, connective possibilities of travel and exchange, and of course its perceived need for sui generis international regulation. It might be more useful then to think of the internet in more holistic or systemic terms, as an environment rather than a mechanism or extension of the 'public'. The turning away from a binary conception of offline/online worlds will better match with the reality of our experiences as the internet is more than a destination or 'new world'.

III FURTHER DEVELOPMENTS

More recently, in late 2014, the General Assembly revisited the issue of digital privacy and adopted a further resolution on the subject, *Resolution 69/166*, '*The Right to Privacy in the Digital Age*'.[21] *Resolution 69/166* further illustrates the ongoing contemporary significance of the debate over digital privacy, at least in the General Assembly context and follows a report ('*OHCHR Report*')[22] on the subject by the Office of the High Commissioner for Human Rights ('OHCHR') as requested in *Resolution 68/167*.[23]

In the *OHCHR Report*, the OHCHR continues the theme from *Resolution 68/167* of the digital age as both facilitating the protection and expansion of human rights, but also as enabling their violation, as in the example of mass surveillance, interception of communications and data collection. Technological changes 'facilitate' such surveillance from governments, but the *OHCHR Report* notes also that '[m]ass surveillance technologies are now entering the global market, raising the risk that digital surveillance will escape governmental controls'.[24] Indeed ongoing revelations regarding surveillance of 'global internet traffic' by the US and UK in particular, point to 'a transnational network comprising strategic intelligence relationships between [g]overnments, regulatory control of private companies and commercial contracts'.[25] This analysis brings further into view the role of both public and private entities as

---

21 *The Right to Privacy in the Digital Age*, GA Res 69/166, UN GAOR, 3rd Comm, 69th sess, 73rd plen mtg, Agenda Item 68(b), UN Doc A/RES/69/166 (10 February 2015, adopted 18 December 2014) ('*Resolution 69/166*').

22 Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, UN GAOR, 27th sess, Agenda Items 2 and 3, UN Doc A/HRC/27/37 (30 June 2014) ('*OHCHR Report*').

23 *Resolution 68/167*, UN Doc A/RES/68/167, para 5.

24 *OHCHR Report*, UN Doc A/HRC/27/37, 3 [3].

25 Ibid 3 [4].

privacy transgressors and their mutual complicity. At issue here is both governmental pressure placed upon companies as well as blanket or mandatory third party data retention schemes which are open to abuse in terms of failure to specify the risk sought to be addressed beyond the generality of 'terror', lack of ongoing oversight and especially concern with whether 'use limitations' are in place once the material is collected. As the *OHCHR Report* states:

> The absence of effective use limitations has been exacerbated since 11 September 2001, with the line between criminal justice and protection of national security blurring significantly. The resulting sharing of data between law enforcement agencies, intelligence bodies and other State organs risks violating article 17 of the *Covenant*, because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another.[26]

The role of business in the protection of human rights is a topic of increasing significance within the field, and the subject matter of digital privacy is a useful angle through which to begin to consider the significance of the largely soft law approach to compliance which has been explored.[27]

Other familiar issues raised by the *OHCHR Report* include: extraterritoriality and responsibility; the interrelationship of human rights such as privacy, non-discrimination and speech; the need for guiding principles such as legality, proportionality, transparency and necessity to be meaningfully followed in application; and the need for adequate institutional responses.

The suggestion is made that the Human Rights Committee's ('the Committee') *General Comment No 16*[28] on privacy, whilst providing analogous contexts and principles such as the need for confidentiality of 'correspondence' free from interception, needs to be updated and in effect translated to the digital age, a process which has begun to occur with freedom of expression and opinion, as evidenced by the development in 2011 of *General Comment No 34*[29] which focuses on issues such as access to information and which urges states party to

> take account of the extent to which developments in information and communications technologies, such as the internet and mobile based electronic information dissemination systems, have substantially changed communication practices around the world.[30]

The Committee, in its *General Comment No 16* regarding art 17 of the *ICCPR*, nevertheless highlights that the

> introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions,

---

26 Ibid 9 [27].

27 See generally Justine Nolan, 'The Corporate Responsibility to Respect Human Rights: Soft Law or Not Law?' in Surya Deva and David Bilchitz (eds), *Human Rights Obligations of Business: Beyond the Corporate Responsibility to Respect?* (Cambridge University Press, 2013) 138.

28 Human Rights Committee, *General Comment No 16: Article 17 (The Right to Respect of Privacy, Family, Home, and Correspondence, and Protection of Honour and Reputation)*, 32nd sess, UN Doc HRI/GEN/1/Rev.9 (Vol. I) (8 April 1988) ('*General Comment No 16*').

29 Human Rights Committee, *General Comment No 34: Article 19 — Freedoms of Opinion and Expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011).

30 Ibid 4 [15].

> aims and objectives of the *Covenant* and should be, in any event, reasonable in the particular circumstances.[31]

Whilst the terms of art 17 of the *ICCPR* are broad and extend to issues of reputation, family, home and correspondence, *General Comment No 16* notes that 'this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons',[32] prefiguring the blending of public, covert and private actors who now represent such a significant threat to our privacy. *General Comment No 16* is out-of-date in the sense that it does not address in great detail the digital context for violation of privacy, but it does usefully provide that:

> Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.[33]

The Committee's focus on the treatment of correspondence in art 17 of the *ICCPR* is usefully neutral as regards form or technology and extends to digital correspondence and communication and expression such as emails, text messages and other forms of messaging online. The Committee states:

> The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law … every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.[34]

The Committee emphasises the significance of transparency in relation to privacy-burdensome laws and this in itself challenges the covert and indiscriminate manner of much of the surveillance at present.[35] In sum, while *General Comment No 16* relating to privacy does appear to need updating, on closer inspection it is more useful in the context of digital privacy than might be anticipated.

A further institutional reform mooted by the *OHCHR Report* is to ensure that digital privacy and mass surveillance is either sufficiently addressed in the various human rights reporting mechanisms, or in fact that a new Special Rapporteur or other institutional setting is created within the UN framework to effectively address privacy, in the way that related areas such as speech and

---

31 *General Comment No 16*, UN Doc HRI/GEN/1/Rev.9 (Vol. I), [4].

32 Ibid [1].

33 Ibid [8].

34 Ibid [10].

35 For analysis on this point, see Ben Emmerson, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, UN GAOR, 69th sess, Agenda Item 68(a), UN Doc A/69/397 (23 September 2014) 7 [18], 14 [37], 15 [40].

counterterrorism have developed such mechanisms. This is a significant reform proposal with merit, though it should be noted that some of the alternative institutional mechanisms have already begun to address the issue of mass surveillance and digital privacy.[36]

Following the *OHCHR Report*, the more recent *Resolution 69/166* builds on and strengthens the earlier *Resolution 68/167*. Much of *Resolution 69/166*'s text reiterates and repeats the earlier *Resolution*. *Resolution 69/166* takes account of the *OHCHR Report* and the Human Rights Council's *Resolution 26/13*[37] on 14 July 2014 regarding human rights online and other institutional activities which have taken place to increase awareness and debate surrounding the issue of mass surveillance and the role which digital privacy might play. *Resolution 69/166* recognises the role which the human rights framework can play in analysing this problem and begins to point to specific concerns regarding metadata and unlawful surveillance of digital communications. There is also recognition of the role of business and its responsibilities.

In terms of the operative parts of *Resolution 69/166*, para 4(e) adds strength to the earlier position taken by the General Assembly by calling on states to 'provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations'. The problem here will come in giving some content to this and in creating avenues for redress which can account for the scale and systemic damage caused by the violations involved in mass surveillance. Reliance on an individually-focused remedial framework will rub against questions of access, resources and even efficiency as regards justice. Paragraph 5 of *Resolution 69/166* calls for greater institutional attention to be given to the issue and encourages the

> Human Rights Council to remain actively seized of the debate, with the purpose of identifying and clarifying principles, standards and best practices regarding the promotion and protection of the right to privacy, and to consider the possibility of establishing a special procedure to that end.

Resolution 69/166 thus draws on the analysis of the *OHCHR Report* and on the ongoing debate regarding digital privacy, though it does not go as far as some would like.[38]

---

36 Ibid. A very useful and clear human rights analysis is provided by Emmerson. Ben Emmerson objects strongly to the failure to justify the surveillance programs publicly, though he concedes that such justification 'for mass surveillance of the Internet' might be possible even in human rights terms: at 13 [34]. Emmerson also points to the need for stronger safeguards and supervision and for the programs to be subjected to the human rights methodology of necessity and proportionality: at 13 [35], 14–15 [38].

37 Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, GA Res 26/13, UN GAOR, 26th sess, 38th mtg, Agenda Item 3, UN Doc A/HRC/RES/26/13 (14 July 2014).

38 See Somini Sengupta, 'UN Urges Protection of Privacy in Digital Era', *The New York Times* (New York), 25 November 2014; Association for Progressive Communications, 'Call to Support a Strong UNGA Resolution on the Right to Privacy in the Digital Age' (Press Statement, 4 November 2014) <http://www.apc.org/en/pubs/call-support-strong-unga-resolution-right-privacy>; Association for Progressive Communications, 'APC Statement on UNGA Resolution "Right to Privacy in the Digital Age"' (Press Statement, November 2014) <http://www.apc.org/en/pubs/apc-statement-unga-resolution-%E2%80%9Cright-privacy-digit>; Eileen Donahoe, *Human Rights in the Digital Age* (23 December 2014) Human Rights Watch <http://www.hrw.org/news/2014/12/23/human-rights-digital-age>.

The *OHCHR Report* indicates that mass surveillance on its face may violate privacy and that any state must justify such interference and do so in a transparent and ongoing manner.[39] Necessity and non-arbitrary interference will be key issues in the context of mass surveillance, with the *OHCHR Report* noting that '[t]he secret nature of specific surveillance powers brings with it a greater risk of arbitrary exercise of discretion which, in turn, demands greater precision in the rule governing the exercise of discretion, and additional oversight'.[40] Issues of digital privacy and the scope of surveillance engage questions of extraterritorial application of human rights laws and non-discrimination familiar in other contexts.[41] Issues of practical import include the availability of effective remedies and, also, most significantly, given the covert and secretive nature of surveillance, the role of transparency and independent oversight are emphasised in a human rights approach to digital privacy.

The *OHCHR Report* also makes much of the business and human rights angle, noting the 'strong evidence of a growing reliance by [g]overnments on the private sector to conduct and facilitate digital surveillance'.[42] Mention is made of the role to be played by the *Guiding Principles on Business and Human Rights* and their application in the context of digital privacy protection.[43] For example, companies should develop 'grievance mechanisms' and 'should assess whether and how their terms of service, or their policies for gathering and sharing customer data, may result in an adverse impact on the human rights of their users'.[44]

Overall these two resolutions and the *OHCHR Report*, although engaging with the context of mass surveillance and usefully highlighting the potential role for digital privacy, do not add much further specificity to the pre-existing jurisprudence as regards the right to privacy or address concretely the conceptual challenge involved in violations of such scale and scope. There may be pragmatic reasons for this as conceptualising privacy has proved to be contentious and limiting in many domestic and comparative contexts. In the next Part, I briefly explore these tensions and the place of human rights principles and case law in their elaboration.

IV DEFINING AND CONTAINING PRIVACY

A central tension within privacy law scholarship has been conceptual: how to approach defining the concept, not only in the pragmatic legal sense, as a right or interest to be safeguarded within a court structure, but also in the broader normative sense as a value.[45] For the US legal system an early breakthrough

---

39 *OHCHR Report*, UN Doc A/HRC/27/37, 7 [20], 8 [23], 8 [24], 15 [45].

40 Ibid 10 [29].

41 Ibid 11–12 [31]–[36].

42 Ibid 14 [42].

43 John Ruggie, *Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie: Guiding Principles on Business and Human Rights — Implementing the United Nations "Protect, Respect and Remedy" Framework*, UN GAOR, 17th sess, Agenda Item 3, UN Doc A/HRC/17/31 (21 March 2011).

44 *OHCHR Report*, UN Doc A/HRC/27/37, 15 [43]–[46].

45 Daniel J Solove, *Understanding Privacy* (Harvard University Press, 2009) 98–100, 171–4.

came with Samuel Warren and Louis Brandeis tethering the idea of privacy with 'the right to be let alone'[46] and with the intrusive progress of technology: in their case the democratic development of photography and the accompanying intrusion of the media in the lives of public figures.[47] Elsewhere the common law world struggled with recognising a 'right' to privacy (as it has struggled to give meaning to a common law 'right' of free speech beyond a more negative conception of a residual liberty), relying instead on data privacy laws and the equitable remedy for breach of confidence. The introduction of human rights frameworks has contributed to the development of privacy protection in some common law contexts.[48]

Whilst conceptual hurdles and the problem of defining privacy remain significant obstacles at the domestic and international level, the growth of privacy advocacy and the spread of privacy jurisprudence and law reform has weakened the traditional common law opposition to privacy protection as a right, at least on purely definitional grounds. It appears that it is possible to define privacy, albeit in incomplete and partial ways, subject to necessary refinement and ongoing critique. For example, in New Zealand, a tort of invasion of privacy has been developed by the courts in relatively pure common law terms.[49] If privacy can be defined, at least in terms of a cause of action, the question is whether it should be contained by such definition, and what role a human rights approach should play in this regard.

Indeed, whilst the gaps and failings of comparative and international privacy protection are not to be taken lightly, the challenge of giving privacy content and ensuring meaningful protection is one area where human rights law can potentially assist. It is sometimes through the iterative process of interpretation and the fusion of fact and law that norms can generate and be tested, and through which principles can be revised and reshaped according to new sets of facts and differing sociopolitical contexts. Rather than seeing the statutory and interpretive process of defining privacy as an insurmountable barrier to protecting privacy we could begin to think of privacy jurisprudence as a way to test and stretch privacy, to explore its limitations and defy its previous containment.

Despite our preoccupation as scholars with appellate and norm-generating jurisprudence, it is the facts of a case which often deserve greater attention and upon which an outcome may finally turn. Context offers the possibility for discretion. Principles can bend in the interpretive moment to the exigencies of more mundane and even ultimately pragmatic concerns. This is both a strength and weakness of the common law and of human rights jurisprudence too. The mechanism of the 'margin of appreciation'[50] in European human rights case law

---

46 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193, 193, 195, 205.

47 Ibid.

48 The prime example here is the United Kingdom. For landmark decisions, see *Campbell v MGN Ltd* [2004] 2 AC 457; *Douglas v Hello! Ltd (No 3)* [2006] QB 125; *Google Inc v Vidal-Hall* [2015] EWCA Civ 311.

49 *Hosking v Runting* [2005] 1 NZLR 1. There is also the possibility of statutory reform in the area as recently examined by the Australian Law Reform Commission: Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (2014) 23–4 <http://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123>.

50 *Handyside v United Kingdom* (1976) 24 Eur Court HR (ser A).

is one example of a judicial response to the challenge of making a universal mechanism apply in specific fact circumstances, but within a pluralistic system.

A notable aspect of a human rights approach in such context-dependent territory is, however, that whatever the decision, there is often a ritualised narration and endorsement of the normative principles developed in earlier jurisprudence. This can be systemically satisfying and important in terms of broader norm diffusion, but problematic in terms of justice and remedial outcomes for individual plaintiffs.

There is also the law and technology angle to be addressed. Some have argued, for example, that technological developments have overwhelmed and surpassed traditional normative concerns, resulting in the death of privacy.[51] Another turn is to picture privacy as a choice and its protection as involving consumer education and vigilance in setting our own privacy controls online.[52] Mass surveillance calls both moves into question. Privacy norms do appear to be relevant again, at least rhetorically so, and self-management of privacy settings is ineffective in the face of mass surveillance. An acceptance of the reality of future mass surveillance also points towards 'pragmatic privacy', where it is argued by some that the focus should be less on collection (a given) and more on use, oversight and transparency of process.[53] There is a concern here that this might contribute to a portrayal of mass and undifferentiated surveillance as 'passive' and inevitable, rather than actively invasive of privacy, and therefore questionable in human rights terms. We are urged in one sense to give up on privacy in terms of collection of data, which is an ongoing practice in a multitude of governmental and commercial contexts, and to focus instead on developing principles and guidelines regarding usage.

Conceptual confusion regarding the scope and content of privacy protection, along with technological advances, have been significant limiting factors in terms of privacy protection. However, both factors now push us to consider more deeply the need for further development of international privacy law and for greater attention to be given to the project of digital rights translation. Yet despite recognition of the development and need for international and regional mechanisms for regulation of the internet and digital media, there remains reticence about both the speech impact of such coordinated regulation and also the international community's institutional capacity and willingness to enforce such laws and remedy violations.

In this context the General Assembly's engagement with digital privacy is noteworthy, as it both reminds international actors of the already significant frameworks in place — notably human rights protections and associated mechanisms of proportionality — and points to the need for states to provide remedies for emerging violations on a mass scale, engaging also the responsibility of business. What is proposed by the General Assembly in its

---

[51] For a groundbreaking and early examination of this issue, see A Michael Froomkin, 'The Death of Privacy?' (2000) 52 *Stanford Law Review* 1461. A recent argument that this is a myth can be found in: Neil M Richards, 'Four Privacy Myths' in Austin Sarat (ed), *A World Without Privacy: What Law Can and Should Do?* (Cambridge University Press, 2015) 33.

[52] For further discussion and critique, see Daniel J Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 *Harvard Law Review* 1880.

[53] Craig Mundie, 'Privacy Pragmatism: Focus on Data Use, Not Data Collection' (2014) 93(2) *Foreign Affairs* 28.

resolutions regarding digital privacy is akin to a call for the updating and re-situation of a pre-existing framework. Yet, to date, human rights law has not proven itself especially adept at digital translation. Sometimes the privacy analogy may prove too 'analog' for digital contexts.[54] And there may be strength in the argument that what is needed is a 'law of surveillance' or 'information rules' rather than the development of digital privacy.

V THE INTERNET AND PRIVACY — NEW MEANS OF INVASION AND OLD FORMS OF REGULATION?

Are traditional principles such as privacy adequate to the task and flexible enough to be applied in these new settings and contexts? As I have argued above, these questions remain open, though developments in terms of digital privacy are welcome and suitable vehicles for litigation may assist in this process of digital rights translation.[55] However, important concerns remain. For example, despite the possibilities for a fuller understanding of privacy offered in ongoing litigation and in the updating of privacy jurisprudence and standards to address the reality of violations in the digital age such as mass surveillance, we need to consider whether in fact all our eggs should be placed in the privacy basket.

To further explore this challenge I now turn to discuss the recent work of two international law scholars, Marko Milanovic and Fleur Johns, who take usefully contrasting positions as to the suitability of a privacy framework in emergent digital contexts.

Marko Milanovic, in a forthcoming article on the role of digital privacy in addressing the context of the NSA surveillance scandal, adopts a fairly doctrinal approach and makes the argument that privacy law can address this situation.[56] Milanovic notes that in fact litigants are already turning to privacy and developments in relation to digital privacy to make the argument in human rights terms that mass surveillance is unlawful, that it violates digital privacy and that doctrinal challenges such as extraterritorial application of human rights can be overcome through further jurisprudential development. He writes that '[o]n any assessment the Assembly's resolution on the right to privacy in the digital age represents a major development. It firmly puts the issue of electronic surveillance within the framework of international human rights law'.[57] For Milanovic it is useful as a rhetorical and agenda-setting process.[58] And important questions regarding the applicability of international human rights treaties to the context of

---

54 Fleur Johns and Daniel Joyce, 'Beyond Privacy. Is Prevailing Legal Debate Too Analog for a Digital Age?' (2014) 23(3) *Human Rights Defender* 24.

55 Examples of recent cases and ongoing litigation which continue to shape the contours of digital privacy and questions regarding the legality of mass surveillance include: 'Statement of Facts', *Big Brother Watch v United Kingdom* (European Court of Human Rights, Application No 58170/13, 4 September 2013); *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (Court of Justice of the European Union, C-293/12 and C-594/12, 8 April 2014); *Liberty (The National Council of Civil Liberties) and Government Communications Headquarters* [2014] IPT/13/77/H (UK Investigatory Powers Tribunal).

56 Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age', *Harvard International Law Journal* (forthcoming) <http://ssrn.com/abstract =2418485>.

57 Ibid 5.

58 Ibid 6.

ongoing mass surveillance are addressed in doctrinal and normative terms by Milanovic, who advocates that 'human rights treaties should apply to virtually all foreign surveillance activities', though answers to questions regarding the legality of such programs cannot be presumed.[59]

For Milanovic, an international human rights law approach offers non-discrimination in terms of treatment of citizens in different states and helps to overcome the partisan approach of domestic constitutions to such issues. He states that:

> [T]his is precisely where the universalist normative foundation of human rights comes in: an interpretation which values all human beings equally and is respectful of their individual dignity is inherently more preferable than one that does not.[60]

That might be so, but Milanovic does not address the deeper question of whether international human rights law guarantees equality of outcome and experience of the law. Milanovic sets out a persuasive case for the application of principles derived from the *ICCPR* and *European Convention on Human Rights* to the facts of mass surveillance beyond borders, closely examining the international jurisprudence regarding extraterritorial application. He does significantly point to the limitations of a spatial analysis of such developments[61] and concedes that certain older privacy analogies such as those relating to 'physical searches or interferences … are no longer feasible or are outright misleading' in the context of mass surveillance, but somewhat optimistically he argues that, nevertheless, 'such analogies can be a useful starting point'.[62]

Milanovic pushes both technically and normatively for the resilience of the international human rights law framework and its provisions regarding privacy. Problems are present, but not insurmountable. Balancing can assist and more expansive interpretations and models, especially in relation to extraterritorial application, can begin to perform the work needed to 'update' and translate privacy to the digital age. Perhaps most significantly for Milanovic, we are not 'starting from a blank slate' in setting out the contours of privacy for a digital age.[63] Indeed, one criticism of Milanovic's approach is that despite its vigour and conceptual rigour, there is not enough of a blank slate and that too much is tied to human rights and international legal debates and anxieties, perhaps at the expense of a deeper engagement with the complexities of allocating responsibility and addressing questions of power and distribution. For him then it is a question of determining the content of digital privacy and it is here that both traditional and more contentious views of human rights law will assist. Milanovic urges us to move beyond the hurdle of applicability and to address the content. This is useful, but as noted above, it is doubtful whether the General Assembly resolutions have contributed much in this regard.

By contrast, Fleur Johns, in a provocative and largely critical contribution, points both to the limitations of human rights law at a conceptual and practical

---

59 Ibid 8.
60 Ibid 36.
61 Ibid 51–8.
62 Ibid 49.
63 Ibid 71.

level in addressing the challenge of the digital environment and of big data. Johns focuses on developments regarding big data more broadly, but her arguments are also useful in the context of mass surveillance, for she asks whether it might 'be time to re-think our preoccupation with privacy and associated icons, such as the consenting data subject'.[64] Johns 'contends that there is much more at issue in the governance of the emerging global data economy than technical interface between existing legal systems and well-aired privacy concerns'.[65] Further, some of the politics of data governance which Johns sets out so usefully, such as its insistence on flow and circulation, may in fact be at odds with privacy concerns.[66] Equally the turn to 'transparency' and a discourse regarding access to information may not 'deliver on its promise of empowerment'.[67]

Johns explores the ways in which personal data and privacy concerns 'tend to enshrine an integrated, wilful, relatively self-contained personhood even as they sketch a technological and communicative context in which that personhood is but a contingent assemblage of strewn bits'.[68] The individuation involved in the human rights context appears to disempower the privacy subject who is pitted against the complexity and opacity of the digital economy.[69] In this context the limitations of a digital privacy approach, and of a traditional institutional response, must be examined further and Johns urges collaborative and interdisciplinary mapping of the 'many global runnels and riverlets' of the 'global data flood' to examine the complexity of the contexts before reverting to 'the routine characterisations of law' such as an individual's right to privacy.[70]

VI CONCLUSION

The digital rights project including these recent General Assembly resolutions on the right to digital privacy, along with earlier debates regarding internet freedom, are significant developments. But as the process of translating rights for online contexts deepens, conceptual, political and practical issues will continue to arise. There has been resistance to the idea of digital privacy from states involved in mass surveillance, which in itself points to privacy as having at least some rhetorical utility. There is also important doctrinal work to be done to give the notion of digital privacy some content. Milanovic points in this direction and to the clarifying role of ongoing litigation. But the complexity of the digital environment, the UN's well-known institutional limitations and the practice of surveillance on such a scale all need greater thought. Johns usefully provokes us to confront the limitations of privacy in the era of big data, to consider new methods and perspectives, to think more deeply about what is really at stake and to ask whether traditional concerns with privacy (or speech) may in fact obscure other useful techniques or questions.

---

64 Fleur Johns, 'The Deluge' (2013) 1 *London Review of International Law* 9, 27.
65 Ibid 14.
66 Ibid 15–18, 22.
67 Ibid 21.
68 Ibid 25.
69 Ibid 26
70 Ibid 34.

The move to articulate our concerns arising from the Snowden revelations in terms of digital privacy does, nevertheless, help to focus attention on the 'invasive' dimensions of what is occurring. A digital right to privacy must entail institutional responses from states, business and the UN itself. It also provides a framework with which to consider important questions of legality, necessity and proportionality. Yet despite the dynamic development of privacy jurisprudence in domestic and international contexts, the concept of privacy itself does not always seem fit for the task of addressing such problems. More broadly this is a problem of unaccountable power and of the authoritarian instincts of those who govern and control. A right to digital privacy is one strategy to address this, but a much larger question regarding liberty and collective political resistance is involved. As Glenn Greenwald has written, 'it is human beings collectively, not a small number of elites working in secret, who can decide what kind of world we want to live in'.[71]

[71] Greenwald, above n 1, 253.