THE BATTLE OF CIVIL LIBERTIES AND THE VULNERABILITY OF TERRORISM: HOW DO WE AVOID AN ORWELLIAN SOCIETY?

Tracy Albin*

Privacy is one of the biggest issues in the continuously growing digital age. This paper will conduct an analysis of privacy and surveillance laws in Australia, the United States, and the European Union in light of growing terrorism concerns around the globe. It will assess the status of privacy rights in the current technological economy, with an examination of recent developments by the United Nations in relation to the right to privacy in the digital age. It is important for government agencies, corporations, and individual members of society to understand the current position at an international level in order to inform themselves and to participate in the ongoing evolution of the debate. A conclusion will be drawn as to the correct balance that should be achieved between the interests of governments in surveilling its population in pursuit of counter-terrorism initiatives and the protection of individuals' human rights, in prospective international policy development.

I Introduction

Resolution 68/167 was adopted by the United Nations (**UN**) General Assembly in December 2013 in response to growing concerns regarding the impact of increased surveillance abilities on human rights in a rising digital age.[1] Many international instruments afford protection to privacy in the offline world. For example, the *International Covenant on Civil and Political Rights* (**ICCPR**) provides protection for individuals from arbitrary or unlawful interference with their privacy, family, home, or correspondence.[2] Other international instruments provide similar protections, including the *International Convention on the Protection of the Rights of all Migrant Workers and Members of their Families* (**Convention on Migrant Workers**)[3] and the *UN Convention on*

* Tracy Albin, LLB (Hons) (Curtin University, Perth WA). Solicitor at GTC Lawyers Perth, WA. Editorial Consultant for the *International Trade and Business Law Review.* Responsibility for the text lies with this author and all errors are hers alone.

[1] United Nations General Assembly, *The Right to Privacy in the Digital Age,* GA Res 68/167, UN GAOR, 3rd Comm, 68th sess, 3rd meeting, Agenda Item 69(b), A/68/PV.70 (18 December 2013).

[2] *International Covenant on Civil and Political Rights,* opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

[3] *International Convention on the Protection of the Rights of all Migrant Workers and Members of their Families,* adopted 18 December 1990, A/RES/45/158.

the Rights of the Child (**Convention on the Rights of the Child**).[4]

Since the introduction of the Resolution, various stakeholders have expressed concerns to the UN regarding the mechanisms for the protection of human rights on digital platforms and the ability of the laws of various member states to keep up to date with the rapidly changing face of technology. The transgression of offline human rights protections to the online sphere is of particular interest, and the issue has been considered by the European Court of Justice (**ECJ**) in multiple cases concerning the legality of domestic legislation permitting surveillance of individuals.[5] Against this backdrop, the General Assembly adopted Resolution 69/166, encouraging the Human Rights Council to consider establishing a special procedure to advance the protection of human rights in the digital world.[6] By way of Resolution 28/16, the Human Rights Council appointed a Special Rapporteur on the right to privacy in April 2015, to hold office for a period of three years.[7]

With all of this in mind, and the existence of an increasing threat of terror in the modern day, the question still remains: how do states adequately balance the ever-growing threat of terror with the rights of individuals? The tension between the two continues today, despite the progress being made by the UN. This is particularly so where states begin to outsource their work and data collection. This paper will hone in on this issue, discussing the various ways that states currently do, or do not, balance these competing interests. This will follow a brief overview of the current international framework for the protection of privacy in the digital age. The paper will also discuss the features required for an effective international instrument regarding the same.

The author wishes to distinguish between mass surveillance and the collection and retention of data for the purpose of targeted surveillance of suspects. While it is recognised that specific surveillance of known threats to national security is authorised by national laws with good reason, the purpose of this article is to focus on the mass surveillance that has resulted from these laws, to which limited or ineffective procedural safeguards exist. It is the proportionality of this mass surveillance to the protection of national security that seeks to be questioned in this article, in light of the protection of the right to privacy in international law.

[4] *UN Convention on the Rights of the Child,* adopted and opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990).

[5] See eg *Zakharov v Russia* (European Court of Justice, Application no. 47143/06, 4 December 2015).

[6] United Nations General Assembly, *The Right to Privacy in the Digital Age,* GA Res 69/166, UN GAOR, 3rd Comm, 68th sess, 3rd meeting, Agenda Item 68(b), A/69/PV.73 (18 December 2014).

[7] United Nations Human Rights Council, *The Right to Privacy in the Digital Age,* GA Res 28/16, UN GAOR, Agenda Item 3, A/HRC/28/L.27 (26 March 2015).

II Privacy - An Ancient And Fundamental Right

The right to privacy is mirrored in several international instruments. Article 12 of the Universal Declaration of Human Rights states:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacks.[8]

Article 17 of the ICCPR is substantially similar and provides:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.[9]

The General Comment on article 17 of the ICCPR produced by the Human Rights Committee of the Office of the High Commissioner for Human Rights describes the rationale of this provision:

> As all persons live in society, the protection of privacy is necessarily relative. However, the competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant. Accordingly, the Committee recommends that States should indicate in their reports the laws and regulations that govern authorized interferences with private life.[10]

The Committee continues:

> 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. Searches of a person's home should be restricted to a search for necessary evidence and should not be allowed to amount to harassment.[11]

Despite this, against the backdrop of a recent spate of terrorist activities and tragedies since 2015, most states have now enacted legislation allowing governments to access personal information, with certain – often inadequate – limitations. Reasons for

[8] Universal Declaration of Human Rights, adopted 10 December 1948, Res 217 A (III).
[9] *International Covenant on Civil and Political Rights,* opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17.
[10] Human Rights Committee, *General Comment 16,* 23rd sess, UN Doc. HRI/GEN/1/Rev.1, (1994) [7].
[11] Ibid [8].

permitting intrusion include where there is reasonable suspicion of terrorist activities, conspiracy to commit terrorism, or other criminal activity. The question remains: to what extent do members of society give up their right to privacy in order to prevent terrorism and how are these competing interests being addressed?

There is great controversy surrounding the legitimacy of laws that permit surveillance, but which go beyond what is necessary to ensure the safety of the states' population. While there is a general understanding of the important role surveillance activity of governments plays in the protection of national security, the existence of legislative safeguards limiting that surveillance to what is reasonable and required in the circumstances remains equally important. The interaction of these interests and the current tension will be discussed from an international perspective below.

III Privacy Around The World: Australia, The European Union And The United States

A *Australia*

Following the 9/11 attacks, governments around the world readily introduced new and far-reaching anti-terrorism legislation which fuelled the apparent 'liberties v security' debate;[12] Australia was no exception. Sometimes referred to as 'hyper-legislation',[13] Australia's anti-terrorism regime affords a myriad of wide-reaching surveillance powers to the Australian Security Intelligence Organisation (**ASIO**). One of the most relevant legislative instruments here is the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA**). The TIA regulates the government's ability to access stored communication and intercept information passing across telecommunication networks.

The TIA prohibits interception of telecommunications unless authorised by a warrant issued under chpt 2, pt 2-2 and chpt 3 of the Act.[14] Under these parts, the Attorney-General may issue warrants to ASIO where there is a reasonable suspicion that the person whose communication will be intercepted is engaging in activities against the security interests of the nation. It must also be demonstrated that the interception will be likely to assist ASIO in protecting security through intelligence measures.[15] Interception warrants may only be issued for investigations relating to serious offences, as defined in s 5D of the TIA.

The aim of these measures is to combat increases in organised crime arising from the ease with which communication can remain undetected. However, recent changes to the legislation which now require telecommunication providers to mandatorily retain

[12] Konrad Lachmayer and Normann Witzleb, 'The Challenge to Privacy from Ever Increasing State Surveillance: A Comparative Perspective' (2014) 37(2) *University of New South Wales Law Journal* 748, 748–49.
[13] By whom? Citation required.
[14] *Telecommunications (Interception and Access) Act 1979* (Cth), chpt 2, pt 2-2, chpt 3.
[15] Ibid s 5D.

and store metadata of its users for access by the government have caused significant controversy, with the Human Rights Commission of Australia (**HRC**) questioning its scope.[16] The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) (**Bill**) has also been slammed by the HRC for reaching beyond what is reasonably justified for the furtherance of national security and intelligence operations against serious crime.[17]

In their submission to the Parliamentary Joint Committee on Security and Intelligence, the HRC notes that the Bill does not outline what data will be retained under the amendments, the term 'content' is not defined, and the retention period of 1 year is inappropriate for the introduction of a new regime.[18] Moreover, the circumstances in which communications data can be accessed are too broad and the amendments fail to put an independent authorisation system in place that is removed from the executive arm of government.[19]

David Watts, Victorian Commissioner for Privacy and Data Protection, in noting the rigid nature of Australia's development of privacy protection, acknowledges that with the recent developments of the UN Special Rapporteur and the increasing focus on this area, Australia needs to engage in active and sustained leadership by developing policy, law, and common law that further the protection of privacy.[20]

B *The European Union*

The European Union introduced data retention laws, namely the *Data Retention Directive* (**Directive**) in 2006.[21] Australia's data retention laws are largely modelled on the Directive, which imposes obligations on public telecommunication corporations to retain identified categories of data, including location data generated or processed by them, such as the date, time, duration, and type of communication.[22] However, the Court

[16] Australian Human Rights Commission, *Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014,* AHRC, <https://www.humanrights.gov.au/submissions/inquiry-telecommunications-interception-and-access-amendment-data-retention-bill-2014#Heading76>.

[17] Ibid.

[18] Ibid.

[19] Ibid.

[20] Commissioner David Watts, 'Personality and Privacy in Australia' (Speech delivered at UN Special Rapporteur's Conference on Privacy, Personality and Flows of Information New York University Faculty of Law New York 19 and 20 July 2016) 7.

[21] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC* [2006] OJ L 105/54. See eg Theodore Konstadinides, 'Mass Surveillance and Data Protection in EU Law – The Data Retention Directive Saga' in Maria Bergström and Anna Jonsson Cornell (eds), *European Police and Criminal Law Cooperation* (Hart Publishing, 2013) 69.

[22] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC* [2006] OJ L 105/54, arts 1(1)–(2).

of Justice of the European Union (**CJEU**) struck down the Directive in April 2014 for being disproportionately intrusive to the privacy rights afforded in the European Charter of Fundamental Rights.[23] The Directive demonstrates the wide-reaching and detrimental effects of anti-terrorism laws. In 2011, eight EU member states allowed the Directive to operate in relation to all criminal offences, not just serious offences as originally intended.[24] This demonstrates the potential for exploitation of public fear by intelligence authorities afforded by surveillance laws. Such exploitation is often used to justify an expansion of the scope of such laws, allowing for unreasonable intrusion.

However, recent changes brought in April 2016 have attempted to counteract this potential for extrajudicial interference with the right to privacy. *Directive (EU) 2016/680 of the European Parliament and of the Council*[25] sought to reinforce the importance of the protection of personal privacy and to encourage governments and enforcement organisations to observe higher levels of protection when pursuing criminal matters. For instance, the Directive states: 'the free flow of personal data between competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences ... should be facilitated while ensuring a high level of protection of personal data'.[26] The Directive also makes bold suggestions for the imposition of new measures on private entities who may be responsible for holding and/or disclosing personal data in the pursuit of criminal matters. For instance, the Directive states that: 'a body or entity which processes personal data on behalf of such authorities within the scope of this Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to this Directive'.[27] The effect of this, particularly due to the confidential nature of data sharing and police investigations, is yet to be seen.

Another interesting feature of the Directive is its extra-territorial reach outside of the EU. Any person using telecommunication infrastructure inside the EU is subject to having their data information stored and retained.[28]

In 2008, the EU adopted another highly controversial anti-terrorism measure, the *Council Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters* (**Framework Decision**),[29] which remains in force today. Article 13 of the Framework Decision requires member states to 'protect the fundamental rights and freedoms of natural persons when

[23] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources; Kärntner Landesregierung v Seitlinger* (European Court of Justice, C-293/12; C-59/14, 8 April 2014) [58].
[24] Lachmayer and Witzleb, above n 16, 754.
[25] *Directive (EU) 2016/680 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA.*
[26] Ibid (4).
[27] Ibid (11).
[28] Ibid 755.
[29] *Council Framework Decision 2009/315/JHA on the Organisation and Content of the Exchange of Information Extracted from the Criminal Record between Member States* [2009] OJ L 93/23.

their personal data is processed for the purpose of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties'.[30] While this seems prima facie beneficial to the protection of public privacy rights, it is subject to article 1(4) which provides that the document is 'without prejudice to essential national security interests and specific intelligence activities in the field of national security'.[31]

There are also other exceptions limiting privacy rights. For example, article 17 of the Framework Decision guarantees the right of the individual to access processed personal data. However, this can be curtailed by national legislation for a variety of very broad discretionary reasons found in article 17(2), including:

a. To avoid obstructing official or legal inquiries, investigations or procedures;

b. To avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties;

c. To protect public security;

d. To protect national security; or

e. To protect the data subject or the rights and freedoms of others.[32]

Following the entry into force of the *Lisbon Treaty* in 2009,[33] and the *Treaty on the Functioning of the European Union* (**TFEU**),[34] there are now measures being taken to produce a document replacing the Directive, with aims to clarify the issue and achieve a balance between conflicting privacy rights and surveillance measures.[35] This draft Directive also contains an international element which significantly impacts privacy rights. Pursuant to arts 33 and 34, personal data can be transferred to third countries or international organisations where that information is necessary for the enforcement of criminal laws and provided that there are adequate or appropriate safeguards in place. Furthermore, article 36 allows a departure from these provisions, providing for transfer of data where it is essential for the prevention of an immediate and serious threat to public security of a member state or a third country. This arguably reflects the heart of the debate: to what extent is it necessary to forgo human rights to privacy in order to protect against a potential imminent threat to national security or public welfare? The EU takes a very activist approach in this area.

[30] Ibid art 13.
[31] Ibid art 1(4).
[32] Ibid art 17(2).
[33] *Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community*, signed 13 December 2007, [2007] OJ C 306/1 (entered into force 1 December 2009).
[34] *Consolidated Version of the Treaty on the Functioning of the European Union* [2010] OJ C 83/47.
[35] *Draft Directive* [2012] COM (2012) 10.

C *The United States*

The impact of 9/11 on national security laws was understandably most severe in the United States (**US**). One of the most controversial measures to take effect following the attacks was the introduction of the *Patriot Act*,[36] which has given the National Security Agency (**NSA**) broad surveillance powers over domestic and international citizens.[37] Under the *Patriot Act*, the NSA can collect telephone records and metadata in bulk.[38] These actions have consistently been approved by the Foreign Intelligence Surveillance Court pursuant to s 215 of that Act. The *Patriot Act* also gives the Federal Bureau of Investigation (**FBI**) extensive powers to conduct national security investigations.[39] The FBI can issue National Security Letters allowing them access to various sources, including libraries, bank accounts, post offices, and casinos.[40] In an attempt to avoid increasing powers of intelligence agencies, the *Privacy Act 1974* (US) (***Privacy Act***) imposes standards on federal agencies when collecting, using, maintaining, and disclosing personal information.[41] However, the *Privacy Act* does not extend to cover visitors or immigrants and does not cover records created by or held by intelligence agencies, placing numerous sources of information outside its ambit of protection.[42]

Under the US model, temporary measures have often become permanent and the complexity of the laws has steadily increased to a point where administrative powers are continuously pulling away from judicial controls.[43] This has a disastrous impact on privacy rights in the US. While the US Constitution provides limited privacy guarantees, particularly in the fourth amendment, the right is particularly weak due to the strength of the right to free speech.[44] The US Courts have continued to severely inhibit the effect of the fourth amendment.

---

[36] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* 115 Stat 272.

[37] Kent Roach, *The 9/11 Effect: Comparative Counterterrorism* (Cambridge University Press, 2011) 184–6.

[38] See eg David Medine et al, 'Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court' (Report, Privacy and Civil Liberties Oversight Board, 23 January 2014).

[39] See generally Andrew E Nieland, 'National Security Letters and the Amended Patriot Act' (2007) 92 *Cornell Law Review* 1201.

[40] Ibid.

[41] Andrew Charlesworth, 'Clash of the Data Titans? US and EU Data Privacy Regulation' (2000) 6 *European Public Law* 253, 259–60.

[42] Lachmayer and Witzleb, above n 16, 765.

[43] Ibid 763.

[44] See generally Lewis R Katz, 'In Search of a Fourth Amendment for the Twenty-first Century' (1990) 65(3) *Maurer School of Law: Indiana University* 549; Michael W Price, 'Rethinking Privacy: Fourth Amendment "Papers" and the Third-party Doctrine' (2016) 8 *Journal of National Security Law and Policy* 247; Raymond Shih Ray Ku, 'The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance' (2002) 86 *Minnesota Law Review* 1325; Peter Goldberg, 'Consent, Expectations of Privacy, and the Meaning of Searches in the Fourth Amendment' (1984) 75(2) *Journal of Criminal Law and Criminology* 319; Arthur Leavens, 'The Fourth Amendment and Surveillance in a Digital World' (2015) 27(4) *Journal of Civil Rights and Economic Development* 709; Andrew E Taslitz, 'The Fourth Amendment in the Twenty-first Century: Technology, Privacy and Human Emotions' (2002) 65(2) *Law and Contemporary Problems* 125.

For instance, in *United States v Miller*,[45] and *Smith v Maryland,*[46] the US Supreme Court held that any personal information which a person voluntarily communicates to a third party – such as a bank or a telephone company – does not enjoy the protection of the Fourth Amendment. A further difficulty in this area is the continued technological developments which require the Constitution to adapt to new surveillance measures. In *United States v Jones,*[47] the US Supreme Court was required to consider the legality of police surveillance which involved placing tracking devices on a suspect's car while it was parked in a public space. The police actions were deemed unconstitutional and a violation of the Fourth Amendment. However, it is accepted that this will not always be the case. As new technology is made available to police and federal surveillance agencies, the Fourth Amendment will continue to be placed under significant stress as new interpretations are considered, leaving the Supreme Court to decide the dispute between human rights and State surveillance.

Under the Obama administration, these laws have been significantly limited. This comes after the Snowden revelations, which exposed the mass surveillance and grave intrusion into the private lives of US citizens, with very little or no justification and through the use of secretive measures.[48] The *Freedom Act*,[49] enacted in June 2015, saw the end of bulk collection of data[50] and sought to limit the secretive nature of surveillance in the US.[51] President Obama, as he then was, argued that this Act reversed the treacherous terrain laid out by the *Patriot Act*, and restored balance to the debate between civil liberties and anti-terrorist measures.[52] Given the considerable public light this subject has received in the last few years, it is expected that measures such as these around the world will have a greater focus on balancing human rights and counter-terrorism measures, as people grow more critical of the ability of governments to pry into their private lives.

IV The Debate in a Contemporary Context

As seen above, there are a number of international faces to surveillance laws. It is noted that as more surveillance measures are introduced, their field of application is

[45] [1976] USSC 66; 425 US 435 (1976).
[46] [1979] USSC 131; 442 US 735 (1979).
[47] 132 S Ct 945 (2012).
[48] See generally Joyce M Yoon, *Edward Snowden, Criminal or Patriot: Media Coverage of National Security Agency Document Leaks* (Honours Thesis, Andrews University, 2015); Margaret Kwoka, 'Leaking and Legitimacy' (2015) 48 *University of California Law Review* 1387; Charlie Smith, 'The Snowden Effect: Three Years After Edward Snowden's Mass-surveillance Leaks, Does the Public Care How They Are Watched?' (2016) 45(3) *Index on Censorship* 48.
[49] *Freedom Act* (H R 2048, Pub L No 114–23) (2015).
[50] Ibid § 201.
[51] Ibid §§ 604, 605.
[52] Patricia Zengerle and Warren Strobel, *Obama Signs Bill Reforming Surveillance Program* (3 June 2015) Reuters <https://www.reuters.com/article/us-usa-security-surveillance-passage/obama-signs-bill-reforming-surveillance-program-idUSKBN0OI2I920150603>.

widening.[53] Most surveillance laws extend beyond simply combatting terrorist efforts and allow national law enforcement agencies to monitor and access personal information of those persons suspected of being involved in even minor offences.[54] In addition to this, the safeguards against sharing information across borders and amongst States are slowly diminishing.[55] While there is a national and international interest in preventing large-scale terrorist activities, there is reasonable speculation that information sharing is being conducted for reasons not originally intended by the legislation. In a world of increasing globalisation and rapidly increasing technological capabilities, oversight and the ability to control the activities of governments and intelligence agencies is a real concern.

Most protections of privacy afforded by judicial systems, constitutions, or national legislation are easily avoided by reason of national security rationales. Governments often exploit fear to gain public approval when exercising their surveillance powers and not many people understand or appreciate the reach of these measures into their private lives. This is a long-recognised tactic, noted by Alexander Hamilton in *The Federalist* (No 8) in the late 18th century:

> Safety from external danger is the most powerful director of national conduct. Even the ardent love of liberty will, after a time, give way to its dictates. The violent destruction of life and property incident to war, the continual efforts and alarm attendant on a state of continual danger, will compel nations the most attached to liberty to resort for repose and security to institutions which have a tendency to destroy their civil and political rights. To be more safe, they at length become willing to run the risk of being less free.[56]

Lengthy retention periods, extensive intrusion powers, and decreased regulation of governments have been a central focus of the debate today. Following exposures of State surveillance activities such as the Snowden revelations and the related activities of the NSA, the international community has placed a spotlight on surveillance laws and has taken an active role in protecting human rights.[57] This is evidenced in the recent steps taken by the Office of the High Commissioner of Human Rights (**OHCHR**). Still, several questions remain. In an environment of increasing globalisation at a rate that is difficult to contain, how will the right to privacy continue to be protected? Who is responsible for ensuring compliance with these protections? In what circumstances does national security trump the right to privacy? Who will make governments and intelligence agencies accountable? These challenges face the United Nations and member states today, and the outcome of the next few years of debate and discussion is difficult to predict with certainty. The following section will consider what necessary features

[53] Ibid 774.
[54] Roach, above n 37, 227–9.
[55] Lachmayer and Witzleb, above n 16, 774.
[56] Professor George Williams, *Does Australia Need New Anti-Terror Laws?* Civil Liberties Australia, <http://www.cla.asn.au/News/terror-laws-some-good-some-unneeded/>.
[57] Michael V Hayden, *Beyond Snowden: A NSA reality check* (January 2014) World Affairs, <http://www.worldaffairsjournal.org/article/beyond-snowden-nsa-reality-check>.

must be included in an international instrument dealing with the protection of privacy rights in a digital age, according to the discourse available and the author's own views.

V Considerations For Further Development

A *Developing an International Framework*

One of the key suggestions arising from discussions in this area is the development of an international instrument, capable of being ratified by all member states, for the regulation of the access and use of personal information by governments and corporations.[58] One of the most obvious benefits of this is the creation of a unified standard of conduct which in turn increases confidence in governments and transparency at an international level.[59] This also has the potential to increase cooperation between States. However, in order to be truly effective, the instrument would need to take the form of a treaty or other binding document rather than a guideline or model law. This would ensure that all member states who sign and ratify the instrument are bound to adhere to its terms and will be liable for sanction in the event of derogation. This of course will enhance the integrity of the measures being taken by the United Nations and give strength to the initiative.

Another positive outcome of such a measure would be its extra-territorial application.[60] As noted earlier, some States afford greater privacy rights under their national laws to their own citizens but fail to afford that protection to non-citizens. Apart from being discriminatory, this allows for the mistreatment of immigrants, tourists, and other non-citizens for arbitrary reasons. If the UN were to introduce a legally binding treaty, the same protection would be afforded to all individuals, whether they belong to a particular State or not. This not only increases equality but facilitates the development of precedence as the instrument continues to be developed and interpreted by those States as well as international courts. Uniformity in this space not only strengthens privacy rights but is also in line with principles such as the rule of law and the prohibition against discrimination based on race or nationality.[61]

Another side to this development that may not be considered initially is the ability for an international instrument for the protection of privacy to facilitate the operation of

[58] Daniel Joyce, 'Privacy in the Digital Era: Human Rights Online?' [2015] 16 *Melbourne Journal of International Law* 1, 4.
[59] C Nagle, *Submission G196*, 26 November 2002; Office of the Federal Privacy Commissioner, *Submission G294*, 6 January 2003.
[60] Lachmayer and Witzleb, above n 16, 775–77.
[61] See generally *International Convention on the Elimination of All Forms of Racial Discrimination,* opened for signature 21 December 1965, 660 UNTS 195 (entered into force 4 January 1969); *International Covenant on Civil and Political Rights,* opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976), art 4.

anti-terrorism and surveillance laws.[62] A fundamental aspect of the suggested instrument would be the requirement of increased disclosure and transparency of surveillance activity by governments and corporations. This increases confidence in, and reliability of, these bodies and is likely to encourage citizens to cooperate more readily and mitigate opposition to these laws, which is largely based on concerns of secrecy and corruption. By involving the public with the development of national laws and providing a stronger framework for disclosing how information is accessed and used, their confidence in those processes grow and their resistance to surveillance measures is accordingly reduced.[63]

While the benefits of such a regime are recognised, regard must also be had to the need for international unity in developing and ultimately adopting such a regime. To enhance the practicality of this paper, and the suggestions for reform contained within, it is prudent to recognise the difficulty that may arise in this respect. Given the most recent divisions in this space, it seems unlikely – or at least a long way in the future – that the large geopolitical players will arrive at an agreement at how best to balance the protection of the civil right to privacy and the need for surveillance in pursuit of security measures.[64]

B *Increased Regulation of Corporations*

With the development of an international instrument necessarily comes the increased regulation of corporations that are involved in the surveillance activities of governments. This includes, by way of example, those telecommunication companies who are required by law to collect and store personal data and metadata of their customers for use by the relevant authorities and intelligence agencies. Businesses are collecting personal information of their customers more often in the twenty-first century which creates a plethora of information available for access by governments. The use of that data is consistently questioned by the public who are often unaware of how their information is being stored or used. Further problems are encountered when that information is released to the public or data retention systems are hacked, leading to public confidence in these entities suffering. This naturally creates discontent and opposition to surveillance measures. One of the most prominent examples in the past five years is the Snowden leaks, which reignited the debate about the protection of civil liberties and government

[62] N Nheu and H McDonald, 'By the People, For the People? Community Participation in Law Reform' (2010) Law and Justice Foundation of NSW <http://www.lawfoundation.net.au/report/lawreform>.

[63] Ibid; Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* (Hamish Hamilton, 2014) 253.

[64] See generally Monica Zalnieriute, 'The Promise and Potential of Transgovernmental Cooperation on the International Data Privacy Agenda: Communicative Action, Deliberate Capacity and Their Limits' (2016) 32 *Computer Law and Security Review* 31; Ira S Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3(2) *International Data Privacy Law* 74; Matthew R VanWasshner, 'Data Protection Conflicts Between the United States and the European Union in the War on Terror: Lessons Learned from the Existing System of Financial Information Exchange' (2008) 39 *Case Western Reserve Journal of International Law* 827.

surveillance in the digital age.[65]

The same principles that apply to government regulation can and should therefore be applied to corporations. National laws should be required to reflect principles of privacy and transparency to facilitate the principled surveillance of persons as well as improve the public's perception of how their data is stored and used. This would subsequently bolster anti-terrorism measures and support national security initiatives. One way to solidify and strengthen these measures would be to include the requirement to enact such national laws in the aforementioned international instrument, creating uniformity around the globe. It necessarily follows that to improve the perception of surveillance measures on an international scale, improvements at a national level must first be implemented. Disparity amongst States would create detrimental gaps in the international framework and would inhibit the development of uniform human rights in this area.[66]

C *Key Features of an International Instrument*

1 *Defined Periods of Retention*

In addition to requiring corporations and governments to disclose how personal information is being stored and used, there should also be a uniform retention time imposed.[67] This would see all relevant bodies collecting and storing personal information for a defined and non-arbitrary period of time. Not only would this again increase confidence in the procedures of data collection but it would also ensure that the information is not stored for a disproportionate amount of time beyond where it is no longer relevant to an investigation. Further, it would mean that no personal information is available to be used or exploited by different people or agencies which were not involved in the matter at first instance. This reduces the amount of people who have access to this information and furthers privacy considerations.

2 *Increasing Public Access to Information*

Increased access of the public to information being stored and used must also be considered.[68] If transparency is increased and individuals are afforded greater access to the information being used by surveillance bodies, they are more likely to trust or at least have increased confidence in those processes. This would be particularly relevant to those people who may be the subject of an investigation for reasons other than being guilty of a crime. This may arise, for example, where an individual has an association with a suspect but is not necessarily involved in the crime itself. For those people to be

[65] See generally Hayden, above n 52.

[66] Jörg Kammerhofer, 'Uncertainty in the Formal Sources of International Law: Customary International Law and Some of Its Problems' (2004) 15(3) *European Journal of International Law* 523, 524–35.

[67] Parliamentary Joint Committee on Intelligence and Security, Commonwealth Parliament, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (2015) chpt 4, [4.188], [4.19], [4.105]; Victor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2011).

[68] Joyce, above n 53, 9; Fleur Johns, 'The Deluge' (2013) 1 *London Review of International Law* 9, 21.

able to access the information being used and the reasons for its use, there is a possibility that they may find the procedures more agreeable.

An inescapable issue that may arise as a result of allowing the public access to that information is the risk that an ongoing investigation may be compromised. Measures would therefore need to be introduced to combat that risk. This may include requiring persons seeking to access the information to agree to a gag order before being granted access, or seeking a court order prohibiting any unwarranted disclosure of the information to third parties. In each instance, this would need to be extensively considered by the relevant stakeholders before such a system could be implemented.

3 *Increasing Accountability*

An elementary principle that must be promoted in any instrument regulating privacy of information is accountability. Governments and corporations accessing and sharing information must be made accountable for their intrusion into the private lives of their citizens. Problems arise when governments enact laws or regimes that allow those bodies to access and use personal information without the need for prior authorisation from either a judicial or government body or in the absence of any accountability measures. Allowing these bodies to use personal information without requiring them to provide legitimate reasons for the basis of their use creates the perception that they may be doing so in an arbitrary way that breaches human rights. It also creates further tension between the public perception of data collection and the policy rationales of surveillance for counter-terrorism measures.

In creating a legislative regime that provides remedies to those people whose information is dealt with in breach of human rights, the UN should also impose standards requiring the relevant body to notify an individual that their information is being used and stored, the reasons for using it, and how they can gain access to the information. This increases accountability and reduces the perception that these bodies are recklessly using personal data in an unregulated environment to the detriment of personal privacy rights.[69]

A further measure worth considering is the creation of obligations for corporations, such as telecommunication companies, to refuse to disclose personal data to government agencies where adequate reasons are not provided in order to avoid breaches of human rights standards.[70] By making corporations accountable, and imposing fines or other punishments which impact them financially as well as harm their reputation, they are made more accountable to the public when dealing with private information. Consequently, confidence in their ability to protect privacy increases. As mentioned above, this also has the effect of facilitating anti-terrorism measures.

[69] Human Rights Committee, above n 13, 13–4.
[70] Ibid 14–5.

4 *Independent Authorisation of Access to Data*

Recent comments by the UN Special Rapporteur on Privacy have refreshed calls for an independent body in each state for the authorisation of surveillance pursuant to national laws. Mr Joe Cannataci, in October 2017, has commented that:

> The right to privacy can never be absolute in the fight against crime and in national security, but democracies need checks and balances such as prior authorization of surveillance and the subsequent oversight of these activities, in order to preserve the very freedoms that define democracies.[71]

This position has been further reinforced by the ECJ, which, in April 2014, held that the EU legislature's newest Data Retention Directive[72] did not adequately uphold the proportionality principle with respect to certain provisions in the EU Charter of Fundamental Rights.[73] In reaching this finding, the ECJ observed the absence of procedural and substantive safeguards in the Directive to protect against unreasonable and unlawful intrusion into an individual's private life.[74] In particular, the Court noted that access to retained data was not subject to prior review by an independent administrative body tasked with limiting access to what is strictly necessary for the purpose of prevention, detection, and prosecution of criminal acts.[75]

The need for checks and balances on the actions of governments is not a new concept; most states strive to adopt transparent practices in order to garner the support of their constituents for their administrative actions. The area of privacy and data retention is no exception. However, the topic has only recently received attention and thus many states have not yet adopted an independent review body for the purpose of authorising access to, and use of, stored data. This is therefore a ripe area for proposed reform, to strengthen the system of data retention and use by authorised agencies, and further improve the transparency of security operations. Each state may benefit from such an independent body to limit the use of such data to those situations where it is necessary for the investigation and prosecution of security threats, rather than for the use of mass surveillance contrary to international human rights.

---

[71] Mr Joe Cannataci, *Surveillance, Big Data and Open Data to Top UN Expert's Privacy Agenda* (Speech Delivered at UN General Meeting, New York, 20 October 2017).

[72] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (no longer in force).

[73] Specifically, arts 7,8 and 52(1)): see generally *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources et al* (European Court of Justice) Joined Cases (C-293-12), (C-594-12) (8 April 2014).

[74] Ibid [61].

[75] Ibid [62].

V Conclusion

Many commentators believe that 'the hard truth is that the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether'.[76] However, the UN and the OHCHR are in a unique position now to reframe privacy rights, to create new legislative measures, and to adopt a position that reflects the interests of governments, the public, and international organisations. With the introduction of the Special Rapporteur and the increased awareness of the need for an intervention in this space, the UN should capitalise on the willingness for governments and the public to engage and facilitate the development of such a regime. With careful consultation, debate, and scholarly discussion involving all stakeholders, the right to privacy in the digital age can be protected. Where there is strong support for a measure to be taken, there will likely be strong engagement by parties to achieve a satisfactory outcome.

A balance needs to be struck between the requirement for anti-terrorism measures and surveillance laws to protect the public and the need to uphold the sanctity of privacy as a fundamental human right. The instances where intrusion into the private lives of individuals is permitted for public protection need to be more clearly defined and those bodies effecting the intrusion need to be held accountable for their actions. There needs to be increased regulation of how information is stored and used, as well as a clearer definition of what is required to satisfy the breach of privacy for the greater good. The rule of law needs to be upheld and a uniform approach needs to be taken. In a world where terrorism is on the rise and international conflicts are an increasing risk, there is no doubt that surveillance is an integral part of national security. However, the rapid rate at which technology is advancing and the increased ways in which 'Big Brother' can access our private information and monitor our day-to-day lives causes unease on a global scale. In order to increase confidence in those processes, the UN and member states need to cooperatively take immediate action by developing an international instrument to better regulate this area.

[76] Ben Emmerson QC, UN Special Rapporteur on counter-terrorism and human rights <https://www.amnestyusa.org/sites/default/files/ai-pi_two_years_on_from_snowden_final_final_clean.pdf>.