

Minerva Access is the Institutional Repository of The University of Melbourne

Author/s:

Desta, Kinfe Yilma

Title:

Reimagining international law of privacy in the digital age

Date:

2019

Persistent Link:

<https://hdl.handle.net/11343/230810>

Terms and Conditions:

Terms and Conditions: Copyright in works deposited in Minerva Access is retained by the copyright owner. The work may not be altered without permission from the copyright owner. Readers may only download, print and save electronic copies of whole works for their own personal non-commercial use. Any use that exceeds these limits requires permission from the copyright owner. Attribution is essential when quoting or paraphrasing from these works.

REIMAGINING INTERNATIONAL LAW OF PRIVACY IN THE DIGITAL AGE

KINFE DESTA

ORCID ID: 0000-0003-2514-0491

**Submitted in Total Fulfilment of the Requirements of the Degree of Doctor
of Philosophy**

June 2019

**Melbourne Law School
The University of Melbourne**

ABSTRACT

This thesis examines the question of how international law should respond to the challenges of securing digital privacy. Driven mainly by the transnational nature of privacy threats involving private actors as well as States, calls are increasingly made for an ‘international’ privacy framework to meet these challenges. The thesis investigates such recurring calls from the perspective of two global privacy initiatives that posit a progressive vision for the right to privacy in the digital age. Using Internet Bill of Rights (IBRs) and the ongoing United Nations (UN) discourse on the ‘right to privacy in the digital age’ as case studies, it examines the role of emerging initiatives in reimagining current international law of privacy in the digital age. Scholarship investigating IBRs, the (data) privacy literature and the broader field of international law are yet to interrogate the role of, or situate, such initiatives in international law. Nor has international law’s role in addressing the ‘privacy problem’ in the digital environment been considered in the literature. In response to this lacuna, the thesis takes the novel approach of exploring the role of IBRs and the evolving UN privacy discourse in making international privacy law better-equipped in the digital age.

The thesis begins by examining whether current international law of privacy is equipped to address the challenges presented by the digital age. It finds that because of historical antecedents, the normative and institutional structures of international privacy law are ill-equipped to address the ‘privacy problem’ in the digital age. The thesis then examines the role of IBRs and the UN Privacy discourse in making the international law of privacy better-equipped in the digital age. It demonstrates that the ‘freestanding’ and ‘contributory’ roles of these initiatives are negligible, but they possess a ‘catalytic’ role which may shape the normative and methodological directions of a more practical reform.

Adopting a pragmatic approach, this thesis argues that addressing the privacy problem in the digital age requires reimagining the law along the direction charted in those initiatives but through an approach that is incremental, practical, multifaceted and programmatic. Mapped onto the overarching international human right to privacy framework and drawing upon global privacy initiatives, the thesis then proposes two layers of privacy law reform. It, first, presents the case for a soft law approach towards addressing normative gaps, and secondly, argues for a dialogical approach towards lessening institutional-structural gaps in international privacy law.

DECLARATION

This is to certify that:

- a.** the thesis comprises only my original work towards the PhD except where indicated in the Preface;
- b.** due acknowledgement has been made in the text to all other material used; and
- c.** the thesis is less than 100,000 words in length, exclusive of the bibliography and appendices.

PREFACE

Earlier and longer versions of chapters 2 and 4 have been published in the *International Review of Law, Computers and Technology* Vol. 33 No. 2, 2019 (originally published online in January 2018) and *Nordic Journal of International Law* Vol. 87, No. 4, 2018 respectively.

ACKNOWLEDGMENTS

Many people have been supportive during my candidature.

First of all, I would like to express sincere thanks to my supervisors Profs Andrew Kenyon, Megan Richardson and John Tobin for all forms of support, patience, understanding and constructive criticisms. In particular, I am grateful to my principal supervisor Andrew for his consistent and balanced supervision throughout my candidature; to Megan for her generosity from the start to the end; and to John for the encouragements.

Secondly, I am thankful to Prof Tim Lindsay AO, who has been the chair of my Advisory Committee for the entire period of my candidature, for his support, understanding and highly valuable advice.

Thirdly, many thanks to Prof Hilary Charlesworth and A/Prof Mark Taylor, who have been academic assessors at my confirmation and completion seminars, for the highly useful feedback and insightful suggestions.

Fourthly, I am thankful to friendly folks at the Law School, particularly those on Level 9 where I was based in the first year: Hilary Charlesworth, Hamish Carr, Jason Bosland, Matthew Harding, Dale Smith, Hon Marcia Neave AO (who was the judge-in-residence at the time), Susan Kneebone, Monika Zalnieriute, fellow PhD students Monique Cormier, Vicki Huang and Simon McKenzie. I am also grateful to Rebecca Crosser, from the Office for Research, for her support from the admission stage to completion.

Fifthly, I am grateful to The University of Melbourne and Melbourne Law School for the generous award of scholarships, travel funds and teaching fellowships.

Sixthly, I would like to thank many friends and colleagues in Melbourne and beyond for various forms of support, especially Halefom Hailu and Tayechalem Moges, whose camaraderie was invaluable during difficult times.

Finally, special thanks to my mother Abayë and sister Mimi for all their constant support.

ACRONYMS

ACLU	American Civil Liberties Union
AU	African Union
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CRC	Convention on the Rights of the Child
CRPD	Convention on the Rights of Persons with Disabilities
DRIP	Declaration on the Rights of Indigenous Peoples
ECHR	European Convention on Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
EFF	Electronic Frontier Foundation
EU	European Union
GC	General Comment
GDPR	General Data Protection Regulation
GNI	Global Network Initiative
IAB	Internet Architecture Board
IBRs	Internet Bill of Rights
ICANN	Internet Corporation for Assigned Names and Numbers
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICJ	International Court of Justice
ICPDPC	International Conference of Privacy and Data Protection Commissioners
ICTs	Information and Communication Technologies
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IOM	International Organization for Migration
IRP Charter	Charter of Internet Rights and Principles
ITU	International Telecommunication Union
ICRMW	International Convention on the Rights of Migrant Workers and Members of their Families
OECD	Organization for Economic Cooperation and Development
OHCHR	Office of the High Commissioner for Human Rights
PETs	Privacy Enhancing Technologies
PPD	Presidential Policy Directive
SDGs	Sustainable Development Goals
SRP	Special Rapporteur on the Right to Privacy
TLS	Transport Layer Security
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law
UNDP	United Nations Development Program
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNGA	United Nations General Assembly
UNHCR	United Nations High Commission for Refugees
UPR	Universal Periodic Review
WIPO	World Intellectual Property Organization
WSIS	World Summit on Information Society
WTO	World Trade Organization

TABLE OF CONTENTS

ABSTRACT	ii
DECLARATION.....	iii
PREFACE	iv
ACKNOWLEDGMENTS	v
ACRONYMS.....	vi
 INTRODUCTION.....	 1
 I THE RIGHT TO PRIVACY IN THE DIGITAL AGE	 1
A <i>The ‘Privacy Problem’ in the Digital Age</i>	1
1 <i>Transnationalization of Privacy Threats</i>	1
2 <i>Privatization of Privacy Threats</i>	2
3 <i>Sophistication of Privacy Threats</i>	3
4 <i>Imperatives of an ‘International Law’ Response</i>	3
B <i>International Law’s Privacy Problem</i>	5
1 <i>Normative Limits</i>	5
2 <i>Institutional-Jurisprudential Limits</i>	7
C <i>Promises of International Privacy Initiatives</i>	8
D <i>Argument of the Thesis</i>	10
II STATE OF THE ART AND THE RESEARCH QUESTION.....	12
A <i>The Status Quo Approach</i>	11
B <i>The Hard Legalization Approach</i>	11
C <i>The Institutional Approach</i>	17
D <i>The Soft Legalization Approach</i>	19
E <i>The Disjunction in Approaches</i>	20
F <i>The Research Question</i>	21
III METHODOLOGY AND ANALYTICAL FRAMEWORK	22
IV THESIS OUTLINE	24

PART I: CONSIDERING INTERNATIONAL LAW OF PRIVACY IN THE DIGITAL AGE

 CHAPTER 1 — DIGITAL PRIVACY AND THE REACH OF INTERNATIONAL HUMAN RIGHTS LAW	 27
I INTRODUCTION.....	27
II BACKGROUND TO THE RIGHT TO PRIVACY IN INTERNATIONAL LAW	28
A <i>The Cold War Effect</i>	28
1 <i>Softer Monitoring Mechanisms</i>	28
2 <i>Vague Formulation of Rights</i>	30
B <i>The Privacy Inattention Effect</i>	32

III WITHOUT “BLINDSPOTS”? LIMITS OF THE (INTERNATIONAL) HUMAN RIGHT TO PRIVACY FRAMEWORK IN THE DIGITAL AGE	35
A <i>Normative Gaps</i>	35
1 <i>Problems of Scope</i>	35
2 <i>The Curious Case of (Internet) Corporations</i>	46
B <i>Institutional-structural Gaps</i>	49
C <i>Jurisprudential Gaps</i>	51
1 <i>Treaty Body Jurisprudence</i>	52
2 <i>Jurisprudence of HR Council Bodies</i>	56
IV CONCLUSION.....	58

CHAPTER 2 – DIGITAL PRIVACY AND BOUNDARIES OF UNITED NATIONS’ DATA PROTECTION FRAMEWORK..... 60

I INTRODUCTION	60
II BACKGROUND TO UNITED NATIONS’ DATA PROTECTION FRAMEWORK.....	61
A <i>The Cold War Effect</i>	61
B <i>The (Data) Privacy Inattention Effect</i>	64
III FALLING INTO DISUSE: EXCESSES AND GAPS OF UNITED NATIONS’ DATA PRIVACY FRAMEWORK.....	67
A <i>Problems of Substance and Approach</i>	67
1 <i>Dispersive Approach to Data Privacy</i>	67
2 <i>Problem of (Over) Soft Legalization</i>	74
3 <i>Problem of Juridical Quality</i>	79
B <i>Problems of Institutionalization</i>	81
1 <i>Institutional Fragmentation</i>	81
2 <i>Monitoring Challenges</i>	86
IV CONCLUSION.....	87

PART II: POSITIONING GLOBAL PRIVACY INITIATIVES IN INTERNATIONAL LAW

CHAPTER 3 – DIGITAL CONSTITUTIONALISM: DIGITAL PRIVACY AND PROMISES OF INTERNET BILL OF RIGHTS..... 89

I INTRODUCTION	89
II MAKING SENSE OF INTERNET BILL OF RIGHTS: ORIGINS, NATURE AND SCOPE	90
A <i>Origins of IBRs as a Constitutional Project</i>	90
B <i>Locating Convergence in IBRs Initiatives</i>	92
1 <i>Evolutionary Project</i>	92
2 <i>Rights Novelty</i>	93
3 <i>Momentary Project</i>	94
4 <i>Norm Cross-feralization</i>	95
5 <i>Multi-stakeholder Experimentation</i>	96
C <i>Miscellany of Legal Sources and Forms in IBRs</i>	97
D <i>The Right to Privacy in IBRs</i>	100

III THE ROLE OF INTERNET BILL OF RIGHTS IN REIMAGINING INTERNATIONAL LAW OF PRIVACY.....	104
A <i>Freestanding Role: Hurdles for an International IBRs</i>	104
1 <i>Diffuse and Momentary Project</i>	105
2 <i>Conceptual Ambiguities</i>	106
3 <i>The Desirability Dilemma</i>	109
4 <i>Feasibility Challenges</i>	110
5 <i>Procedural and Substantive (II)Legitimacy</i>	112
B <i>Contributory Role: Prospects of Shaping Law and Practice</i>	115
1 <i>Enriching Global Privacy Dialogues</i>	115
2 <i>Shaping Lawmaking</i>	116
3 <i>Stimulating Judicial and Industry Practices</i>	117
C <i>Catalytic Role: Prospects of Charting Normative Directions</i>	119
IV CONCLUSION.....	120

CHAPTER 4 – INCHOATE CONVERSATION: DIGITAL PRIVACY AND PROMISES OF THE UNITED NATIONS’ DISCOURSE ON THE “RIGHT TO PRIVACY IN THE DIGITAL AGE”

I INTRODUCTION.....	121
II DISCUSSING THE NATURE AND SCOPE OF THE PRIVACY DISCOURSE	122
A <i>Background to the Discourse</i>	122
B <i>Novelties of the Discourse</i>	124
1 <i>Novelty of Approach</i>	124
2 <i>Novelty of Substance</i>	126
III THE ROLE OF THE PRIVACY DISCOURSE IN REIMAGINING INTERNATIONAL LAW OF PRIVACY.....	133
A <i>Freestanding Role: Elaborative and Interpretive Functions</i>	133
1 <i>The Privacy Resolutions as Elaborative Soft Law</i>	133
2 <i>The Privacy Resolutions as Authoritative Interpretation of Art 17 ICCPR</i>	136
B <i>Contributory Role: Towards Universalizing Privacy Standards</i>	137
1 <i>Accretion of General International Law (of Privacy)</i>	138
2 <i>Cross-fertilizing Global Privacy Norms</i>	143
C <i>Catalytic Role: Prospects of Charting Normative and Methodological Directions</i>	146
1 <i>Political Capital for Meaningful Reform</i>	146
2 <i>Innovative Approaches to Privacy</i>	150
IV CONCLUSION.....	151

PART III: REIMAGINING INTERNATIONAL LAW OF PRIVACY PRAGMATICALLY

CHAPTER 5 – JUST A SUPPLEMENT: TOWARDS AN (INTERNATIONAL) SOFT LAW ON THE RIGHT TO PRIVACY

I INTRODUCTION.....	154
II VIRTUES OF A SOFT LAW SUPPLEMENT IN THE INTERNATIONAL PROTECTION OF DIGITAL PRIVACY	156

A <i>Reimagining the Right to Privacy in the Digital Age</i>	156
B <i>Globalizing Emergent Privacy Standards</i>	160
C <i>Facilitating Progressive Development of (Privacy) Law</i>	162
III WHAT SUPPLEMENT? SKETCHING NORMATIVE STRUCTURES OF THE SOFT LAW ..	165
A <i>Clarifying Scope of the Right to Privacy in the Digital Age</i>	166
1 <i>Decoupling Protected Interests</i>	166
2 <i>Subset of Privacy Rights</i>	167
3 <i>Permissible Restrictions</i>	168
B <i>Core Privacy Principles</i>	169
1 <i>Extraterritoriality of the Right to Privacy</i>	169
2 <i>(Data) Privacy Principles</i>	170
3 <i>Independent Surveillance Oversight</i>	171
C <i>Defining Obligations and/Roles of State and Non-State Actors</i>	172
1 <i>Obligations of States</i>	173
2 <i>Obligations/Roles of Internet Corporations</i>	175
3 <i>Roles of Other Non-State Actors</i>	183
D <i>A Question of Form</i>	184
IV CONCLUSION.....	188

CHAPTER 6 — MORE BUT FOCUSED DISCOURSE: TOWARDS A DIALOGICAL APPROACH TO DIGITAL PRIVACY.....

I INTRODUCTION	189
II VIRTUES OF A DIALOGICAL APPROACH IN THE INTERNATIONAL PROTECTION OF DIGITAL PRIVACY	190
A <i>Dialogue as a Pragmatic Future</i>	190
B <i>Dialogue as a Responsive Strategy</i>	192
III WAYS OF CONVERSATION: THE CASE FOR A MULTI-STAKEHOLDER PRIVACY FORUM.....	194
A <i>Foundations of the Forum</i>	194
1 <i>Enriching Multilateralism with Multi-stakeholderism</i>	195
2 <i>Rebuilding Cooperative Dialogue</i>	196
3 <i>‘Encouragement of Human Rights’</i>	197
B <i>Roles of the Forum</i>	198
C <i>Procedural Considerations</i>	201
D <i>The Forum and Limits of Multi-stakeholderism</i>	204
IV CONCLUSION.....	206

CONCLUSION, FINDINGS AND PROSPECTS.....	208
I THE ‘PRIVACY PROBLEM’ AND THE ROLE OF INTERNATIONAL LAW	208
A <i>In Search for a Role</i>	208
B <i>Looking Through the Lens of Global Emergent Law</i>	209
II FINDINGS OF THE THESIS	210
A <i>International Law of Privacy and Its Shortcomings in the Digital Age</i>	210
B <i>Global Privacy Initiatives and Their Limits</i>	212
C <i>Reimagining International Privacy Law in the Digital Age</i>	213
III SEIZING THE MOMENT FOR PRACTICAL REFORM.....	214
 BIBLIOGRAPHY.....	 i
APPENDICES	xliii

Appendix 1: *The Italian Declaration of Internet Rights (July 2015)*

Appendix 2: *The Right to Privacy in the Digital Age, GA Res 73/179 (17 December 2018)*

Appendix 3: *A Précis of the (International) Soft Law on the Right to Privacy*

INTRODUCTION

Successful laws normally either entrench existing norms, clarifying any uncertainties or ambiguities or reinforce developing norms...

Reed, *Making Laws for Cyberspace* (OUP, 2012) 12

I THE RIGHT TO PRIVACY IN THE DIGITAL AGE

A The 'Privacy Problem' in the Digital Age

The human right to privacy is one of the fundamental rights guaranteed in national, regional and international law.¹ It is widely considered an 'enabling' right in that its protection facilitates the enjoyment of other fundamental rights such as freedom of expression, religion and association.² So, securing the right to privacy is not only an end in itself but also a means for the realization of these other civil and political rights. But upholding the right to privacy in the digital age faces novel challenges thereby impacting the enjoyment of a broad range of human rights. Unlike the pre-digital era, the threats that the right faces in the digital age are complex, dynamic, geographically unbounded and involve multiple, and often obscure actors. What is here referred to as the 'privacy problem' in the digital age exhibits three mutually-reinforcing dimensions that capture the new ways in which the right to privacy is undermined.³ As shall be outlined below, not only does interference with the right to privacy occur increasingly in the transnational context but it also involves little regulated private actors that hold key roles in the rapidly shifting technological ecosystem.

1 Transnationalization of Privacy Threats

One obvious manifestation of the digital environment is that it creates a range of new possibilities for cross-border violation of the right to privacy. The global nature of communication technologies enables State and non-State actors to violate the right to privacy of individuals located in different jurisdictions. While cross-border human rights violations are not entirely new, the breadth of transnational privacy

¹ See, e.g., *Universal Declaration of Human Rights*, GA Res 217A(III), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/810 (10 December 1948) art 12; *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17.

² See, e.g., Eric Barendt, 'Privacy and Freedom of Speech' in Andrew Kenyon and Megan Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, 2006) 11-12, 26-27, 30.

³ Cf Lilian Edwards, 'Reconstructing Consumer Privacy Protection Online: A Modest Proposal' (2004) 18 *International Review of Law, Computers and Technology* 313, 319 [applying the term 'privacy problem' (narrowly) to capture loss of consumer trust and erosion of privacy in cyberspace due to 'multinational corporatism and ubiquitous transnational data flows'].

violations has grown exponentially with the global Internet. As the Snowden revelations have shown, American and British intelligence agencies engage in far-reaching mass domestic and foreign surveillance, including against leaders of foreign countries.⁴ The prevailing business model in cyberspace also entails routine corporate collection, processing, aggregation and repurposing of personal data on a transnational scale.⁵ In the digital context, personal privacy can be and often is, therefore, invaded by actors located in jurisdictions well beyond the remit of national legal systems. With the largely borderless nature of communication networks, these international actors can reach, unlike their ‘brick-and-mortar’ equivalents, billions of users worldwide without any physical presence in the jurisdiction in question.

2 Privatization of Privacy Threats

Compounding the transnationalization phenomenon is the rise of little-regulated transnational private power in the digital space.⁶ Much of the Internet’s core physical and technical infrastructure as well as services are now owned and served by private corporations.⁷ But while Internet users around the world rely on their infrastructures and services, most of these corporations are governed by the law of one or more States, which may themselves adopt diverging approaches.⁸ Furthermore, many of the goods and services offered in the Internet space are governed through private contractual mechanisms between Internet corporations and individual users.⁹ And often, these terms of use are not only unilaterally imposed and changed (and hence non-negotiable) but also incomprehensible to lay users.

This state of affairs is increasingly transforming technology companies, to use Eichensehr’s words, into ‘competing centers of power’, seemingly on par with governments when it comes to their ability to impact the enjoyment of human rights.¹⁰ With unprecedented access to and use of personal data of billions of users worldwide, technology companies wield considerable influence on the enjoyment of

⁴ See generally David Fidler (ed), *The Snowden Reader* (Indiana University Press, 2015) part II.

⁵ See, e.g., Christopher Millard, ‘Data Privacy in the Clouds’ in Mark Graham and William Dutton (eds), *Society and the Internet: How Networks of Information and Communication are Changing Our Lives* (Oxford University Press, 2014) 333 et seq.

⁶ Angela Daly, *Mind the Gap: Private Power, Online Information Flows and EU Law* (Hart Publishing, 2016) 18-21.

⁷ See Laura DeNardis, *The Global War for Internet Governance* (Yale University Press, 2014) ch 1 and 2.

⁸ See Chris Reed, *Making Laws for Cyberspace* (Oxford University Press, 2012) 14.

⁹ See Lee Bygrave, *Internet Governance by Contract* (Oxford University Press, 2015) 2-3 (noting that ‘contracts provide the legal bricks and mortar of the present structure’ of Internet governance).

¹⁰ Kristen Eichensehr, ‘Digital Switzerlands’ (2019) 167 *University of Pennsylvania Law Review* (forthcoming) 7-20. In a claim (later attributed to a rogue employee), Zuckerberg stated that Facebook now is like a nation-state. Quoted in Jonathan Zittrain, ‘A Bill of Rights for the Facebook Nation’ on *The Chronicle of Higher Education* (20 April 2009) <<https://bit.ly/2lj8gpq>>

the right to privacy.¹¹ But as shall be demonstrated in this study, present international (human rights) law has little to offer in constraining the influence of corporations generally.¹² What complicates this even more is that, as shown by the Snowden disclosures, corporations operate in tandem with governments in their transnational privacy invasive practices.¹³ The problem, then, is not solely privatization of privacy threats but also abdication by States of their roles to regulate private actors and hence ‘protect’ the right to privacy.¹⁴

3 Sophistication of Privacy Threats

Sophistication of privacy threats is another aspect of the privacy problem in the digital age to note here. Invasive practices of both States and corporations are increasingly being reinforced by new technologies such as big data analytics, artificial intelligence, machine learning, spyware and malware.¹⁵ The ways in which the right to privacy could be undermined is becoming more seamless, surreptitious and accessible. Not only are these technologies accessible with anyone with the economic means but they can be, and are indeed, deployed to invade privacy across borders. The proliferation of market for surveillance technologies, which remains little regulated, best illustrates this phenomenon.¹⁶ Sophistication of privacy threats, presented by transnational actors, not only facilitates privacy violations and complicates avenues for remedies but also tends to normalize otherwise privacy invasive practices. More crucially, such dynamism of the digital environment undercuts the effectiveness of orthodox protection mechanisms such as time-taking adjudicative processes.

4 Imperatives of an ‘International Law’ Response

Highlights of the ‘privacy problem’ in the digital age, outlined above, reveal that the right to privacy in the digital age cannot effectively be secured only through national and regional systems of protection. Part of the challenge relate to the *ability* of these systems of protection to address the privacy problem. At the national level, for example, most jurisdictions either face jurisdictional limits or lack of resources to

¹¹ See Orla Lynskey, ‘Grappling with “Data Power”: Normative Nudges from Data Protection and Privacy’ (2019) 20 *Theoretical Inquiries in Law* 189, 201-202.

¹² See, e.g., Andrew Clapham, *Human Rights Obligations of Non-State Actors* (Oxford University Press, 2006) 25-41.

¹³ See Neil Richards, ‘The Dangers of Surveillance’ (2013) 126 *Harvard Law Review* 1934, 1958.

¹⁴ For purposes of this thesis, the terms ‘Internet corporation’ — alternatively referred to as ‘technology companies’ or ‘Internet companies’ — refer to those private corporations such as Google and Facebook that provide web-based digital services and products.

¹⁵ See, e.g., Normann Witzleb et al, ‘An overview of Emerging Challenges in Privacy Law’ in Norman Witzleb et al (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press, 2014) 2 [noting that ‘rapid technological developments are a major driver of the current concern with privacy’]; Omer Tene, ‘Privacy: The New Generations’ (2011) 1 *International Data Privacy Law* 15, 16-21 [discussing the impact of a ‘new generation of technologies’ on (data) privacy].

¹⁶ See, e.g., ‘The Global Surveillance Industry’ (Privacy International) <<https://bit.ly/2Isuqde>>

counter the challenge. In jurisdictions where there may be fewer jurisdictional challenges – for instance the United States as the home to many big technology companies, political *will* is wanting. US courts have constantly rejected the extraterritorial reach of the right to privacy in international law and drawn distinction between citizens/permanent residents and foreigners.¹⁷ The same can often be seen in surveillance legislation of other ‘Five Eyes’ States.¹⁸ Such discriminatory legal approaches leave citizens of foreign countries without meaningful remedies for arbitrary invasion of privacy.

Jurisdictional limits similarly undercut the ability of even relatively effective systems of regional protection regimes. The success stories of both the Council of Europe (CoE) and the European Union (EU) are circumscribed by, inter alia, case backlog and compliance deficit.¹⁹ And of course, no comparable regime exists, for example in the Asia-Pacific.²⁰ Where such a regime exists, for instance in Africa, it often lacks the necessary resources to meet the challenges.²¹ Thus, the lack of jurisdiction over transnational actors, coupled with resource constraints and absence of political will, leaves billions of individuals without any meaningful recourse and remedies at the national or even regional level. Critically, the characteristically dynamic nature of the digital space where the nature and extent of privacy threats shift constantly as well as the identity and role of actors, challenges the effectiveness of adjudication as a redress mechanism in the digital age.²²

Aspects of the ‘privacy problem’ outlined above largely underpin the often-made case for,²³ and initiatives on,²⁴ an international law response. But such recurring calls for an international privacy framework of some sort give rise to a series of questions, including the following: whether current international law is ill-equipped, in the first place, to address the privacy problem; and if that is really the case, what role(s), or rather place, do these initiatives have in addressing the problem? More broadly, how should international law respond to the ‘privacy problem’ in the digital age? This thesis examines such questions surrounding the need for an international law response to the privacy problem from the perspective of two international privacy initiatives: proposals for an IBRs and the ongoing UN discourse on the ‘right to

¹⁷ See ch 1 and 5.

¹⁸ New Zealand, for instance, sets lower standards of protection for aliens, for example by allowing surveillance without judicial warrant. See, e.g., ‘New Zealand Must Respect Its International Human Rights Obligations’ (Privacy International, 2018) <<https://bit.ly/2AVmThk>>

¹⁹ See ch 6.

²⁰ See, e.g., Dinah Shelton and Paolo Carozza (eds), *Regional Protection of Human Rights* (Oxford University Press, Vol. I, 2nd ed, 2013) 90 et seq.

²¹ Ibid, 73 et seq.

²² See ch 6.

²³ See, e.g., Ronald Krotoszynski Jr., *Privacy Revisited: A Global Perspective on the Right to Be Left Alone* (Oxford University Press, 2016) 9-10; Konard Lachmayer, ‘Rethinking Privacy Beyond Borders: Developing Transnational Rights on Data Privacy’ (2015) 20 *Tilburg Law Review* 78.

²⁴ See more in section C below and further in ch 3-4.

privacy in the digital age'. It interrogates the respective role of these initiatives in reimagining current international law of privacy to make it better equipped in the digital age.²⁵

B International Law's Privacy Problem

By and large, the absence of a robust international privacy framework has been the rallying cry of the persistent calls for an international law response to the privacy problem. And indeed, as this study will demonstrate, international law has so far proved ill-equipped to attend to the privacy problem in the digital age. Gaps in current international law of privacy include a range of normative and institutional weaknesses that cumulatively created a jurisprudential dearth on the right to privacy. The proliferation of various international privacy initiatives in the past few decades, especially in the aftermath of the Snowden revelations, is in part an attempt at to address international law's privacy problem. This thesis seeks to examine the suitability of such initiatives in attending to the various gaps in present international privacy law, foreshadowed below and explored further in chapters 1 and 2.

1 Normative Limits

Current international law of privacy has not moved beyond high-level abstract principles contained in human rights treaties, and practically less significant soft data privacy instruments. Since its recognition in 1948 by the Universal Declaration of Human Rights (UDHR), the right to privacy has been successively recognized in a number of binding human rights treaties. But the right has been formulated in an exceedingly vague manner in high-level abstract principles. As examined in chapter 1, the formulation of the right to privacy is even weaker than the rather common tendency of framing human rights vaguely in human rights treaties.²⁶ The net result is that the uncertainty of scope severely limits the possibility of remedial measures in individual cases.²⁷ Ambiguity of scope also obscures the respective obligations of States and non-State actors vis-à-vis the right to privacy.

²⁵ The phrase 'international law of privacy' – alternatively referred to as 'international privacy law' – is meant to capture all rules of international law concerning the right to privacy. This includes relevant UN treaties and soft law instruments that touch on aspects of the right to privacy, including data privacy; but deliberately excludes (1) a set of UN soft laws on consumer protection and competition regulation that are not only less known but also faintly address (consumer) privacy and (2) regional privacy laws such as EU law, which are referred to only for comparative purposes. See, e.g., *UN Guidelines for Consumer Protection*, GA Res 70/186, 70th sess, Agenda item 18(a) UN Doc A/RES/70/186 (4 February 2016).

²⁶ On this tendency, see John Tobin, 'Seeking to Persuade: A Constructive Approach to Human Rights Treaty Interpretation' (2010) 23 *Harvard Human Rights Journal* 201, 201.

²⁷ See Daniel Cooper and Christopher Kuner, 'Data Protection Law and International Dispute Resolution' (2017) 382 *Recueil des Cours* 1, 48.

The UN data privacy framework, the second segment of international privacy law, is also riddled with several weaknesses.²⁸ The Guidelines for Computerized Personal Data Files (UN Data Privacy Guidelines),²⁹ the principal UN data privacy instrument adopted in 1990, not only has become slightly obsolete but has also been practically ineffective.³⁰ A number of other soft law instruments adopted under the auspices of the UN also do not offer a sound basis for data privacy protection.³¹ More recently, a number of UN specialized and related agencies have adopted internal data protection policies which apply when personal data are processed by these agencies.³² While these policies are modern, and largely based on European data privacy standards, the intra-agency nature of these instruments limits their normative value in international law.

Another major normative gap concerns the regulation of the private sector. International human rights law does not impose direct human rights obligations on corporations.³³ It is only through the positive obligation of States that corporations are held to account for human rights violations. But, this vertical application of human rights by which States would ‘protect’ individuals against private sector infringements falters in the face of recent disturbing revelations. Technology companies routinely collaborate with State actors in various forms, including through granting unfettered access to user data or supplying surveillance

²⁸ In European (data) privacy discourse, a distinction is often drawn between the notions of ‘privacy’ and ‘data protection’ (referred to as data privacy in this study, unless stated otherwise) in the light of recognition of the distinct rights to privacy and to data protection in the EU Fundamental Rights Charter. The prevailing view is that while the two rights overlap to a greater degree, data protection protects more than privacy interests, and that privacy may not protect all types of personal data. Moreover, privacy encompasses more than the protection of personal data. Against this backdrop, the thesis treats the ‘human right to privacy’ and ‘data privacy law’ as sources of digital privacy protection. The reference to ‘data protection’ as a ‘regulatory field of data privacy’ is meant to capture the bureaucratic and mechanical nature of data protection legislation governing the collection, storage, processing and disclosure of personal data. See, e.g., Maria Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publishing, 2017) ch 1. This thesis follows Wack’s description of the notion of privacy as the right not to be subject to incursions into one’s private domains understood more broadly. See Raymond Wacks, *Privacy: A Very Short Introduction* (Oxford University Press, 2015) 2. Whereas the rather nuanced phrase ‘digital privacy’ is used in this thesis to denote privacy in the context of digital communications.

²⁹ *Guidelines for the Regulation of Computerized Personal Data Files*, GA Res 45/95, UNGAOR, 45thsess, 68thplen mtg, UN Doc A/Res/45/95 (14 December 1990).

³⁰ See Lee Bygrave, ‘International Agreements to Protect Personal Data’ in James Rule and Graham Greenleaf (eds), *Global Privacy Protection: The First Generation* (Edward Elgar, 2008) 30.

³¹ See, e.g., *Fundamental Principles of Official Statistics*, GA Res 68/261, 68thsess, Agenda item 9, UN Doc A/RES/68/261 (29 January 2014).

³² See, e.g., ‘Policy on the Protection of Personal Data of Persons of Concern to the UNHCR’ (The UN Refugee Agency, May 2015).

³³ See HR Committee, *General Comment No. 31: Nature of Legal Obligation Imposed on State Parties to the Covenant* 80thsess, UN Doc CCPR/C/21/Rev.1/Add.13 (26 May 2004) [8].

technologies.³⁴ What is more, the existing international framework for the private sector, i.e. the Ruggie Principles, barely covers human rights in the digital context.³⁵ The ongoing UN treaty process to translate the Guiding Principles into a binding instrument, besides its little hope of materializing soon, also does not appear to address the human rights obligations of technology companies.³⁶

The weak structure of international privacy law has historical roots. Most of the drafting work of the relevant instruments was undertaken during the ideologically divided Cold War era. The political controversies between the West and the East have had direct impact in the way these instruments were formulated. The now vaguely worded provisions of the human right to privacy in international human rights law were results of deliberate political compromises reached between political rivals of the time.³⁷ The setback caused by ideological differences was further exacerbated by the little attention paid to the right to privacy, in a stark contrast to other rights, by the drafters of the instruments. Similarly, the drafting of the UN Data Privacy Guidelines was also plagued by ideological controversy which derailed the process for over two decades, and ultimately resulted in merely Guidelines.³⁸

2 Institutional-Jurisprudential Limits

Little has been forthcoming when it comes to the jurisprudence developed so far around these high-level abstract principles of the human right to privacy. Propelled by structural problems of the UN human rights system, treaty bodies – particularly the Human Rights Committee (HR Committee) – are yet to produce a robust jurisprudence on the right to privacy. Unlike the relatively effective systems of human rights protection at regional levels in Europe and the Americas, structural problems have hampered the development of a robust privacy jurisprudence. The case law of the Committee has offered limited guidance on the right to (digital) privacy.³⁹ Other avenues for developing jurisprudence such as concluding observations of treaty bodies are not best-suited to unpack the content of the right to privacy in the digital context. The General Comment (GC) on the right to privacy, adopted in 1988, is largely obsolete and does not adequately cover important aspects of the right to (digital) privacy. And little has emerged so far from the work of the recently installed Special Rapporteur on the Right to Privacy (SRP). The lack of any institutional machinery in the UN data privacy framework has also meant limited development of data privacy jurisprudence.

³⁴ See, e.g., generally Alan Rozenshtein, 'Surveillance Intermediaries' (2018) 70 *Stanford Law Review* 99; see also 'Surveillance Technologies' (EFF) <<https://bit.ly/1fFUph9>>

³⁵ *Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework*, 17th sess, Agenda item 3, UN Doc A/HRC/RES/17/4 (6 June 2011).

³⁶ See ch 1.

³⁷ Ibid.

³⁸ See ch 2.

³⁹ See ch 1.

C Promises of International Privacy Initiatives

As hinted above, the cross-border nature of the Internet, and the lack of a robust privacy framework has long prompted calls for an ‘international’ framework,⁴⁰ and indeed, concrete proposals have also been launched.⁴¹ While academia has been at the forefront of such calls,⁴² other actors including civil society groups, UN organs and a coalition of domestic data protection authorities have taken concrete initiatives. The imperatives for an international privacy framework emerged with some force (and substance) in the wake of the Snowden revelations in 2013. For instance, shortly after his appointment, and in the aftermath of Snowden, the SRP has called for a ‘Geneva style convention’.⁴³ In a direct response to this call, what came to be called the ‘Snowden Treaty’ has been reportedly drafted by ‘experts in international law and legal experts on Internet freedoms and surveillance’, through a process that involved Snowden himself.⁴⁴

High-level proposals have also emerged. One, for instance, suggests negotiation of a ‘social compact’ among governments, private corporations, individuals and the technical community to adequately protect privacy rights in the digital age.⁴⁵ A

⁴⁰ For an earlier call for an ‘international’ framework, see ‘Montreux Declaration: The Protection of Personal Data and Privacy in A Globalized World – A Universal Right Respecting Diversities’ (International Conference of Privacy and Data Protection Commissioners, Montreux, Switzerland, 2005) cum ‘Madrid Privacy Declaration’ (3 November 2009); see also Catherine Rampell, ‘Google Calls for International Standards on Internet Privacy’, *The Washington Post* (online), (15 September 2007) <<http://wapo.st/2kXZAZz>>. See also generally Christopher Kuner, ‘An International Legal Framework for Data Protection: Issues and Prospects’ (2009) 25 *Computer Law and Security Review* 307; Ariel Wade, ‘A New Age of Privacy Protection: A Proposal for An International Personal Data Privacy Treaty’ (2010) 42 *George Washington International Law Review* 659. Perhaps, the earliest formal call for a seemingly international (privacy) law was made by the Nigerian delegation at the 1968 Teheran Conference on Human Rights. In a draft Resolution, which the Conference unfortunately was unable to consider due to ‘lack of time’, Nigeria had proposed for a study group to be created to study the impact of modern technologies on human rights, and then to draw up an ‘appropriate convention’. As shall be considered in chapter 2, the Teheran Conference is where the process that led to the adoption of the UN Data Privacy Guidelines originated. See *Nigeria: Draft Resolution* in Annex to the Final Act of the Teheran Conference on Human Rights, UN Doc A/CONF.32/C.2/L.28 (May 1968) [18].

⁴¹ See, e.g., ‘Joint Proposal for a Draft of International Standards on the Protection of Privacy and Personal Data: The Madrid Resolution’ (November 2009) <<https://bit.ly/2QOXtqQ>>

⁴² See section II below for a survey of scholarship in the area.

⁴³ Quoted in Adam Alexander, ‘Digital Surveillance ‘worse than Orwell’, says new UN Privacy Chief’, *The Guardian* (online), 25 August 2015 <<http://bit.ly/2h2bEYF>>

⁴⁴ ‘The Snowden Treaty: A New International Treaty on the Right to Privacy, Protection Against Improper Surveillance and Protection of Whistle-blowers’ (September 2015) <<http://www.snowdentreaty.org/>>; see also Murtaza Hussain, ‘“Snowden Treaty” Calls for End to Mass Surveillance, Protections for Whistle-blowers’, *The Intercept* (online), (25 September 2015) <<http://bit.ly/1OZZn3I>>

⁴⁵ See, e.g., ‘Toward a Social Compact for Digital Privacy and Security: Statement by the Global Commission on Internet Governance’ (Chatham House, 2015) 13; Cf Simon Chesterman, *One Nation*

related development was that the (then) UN Secretary-General Ban Ki-moon's Expert Advisory Group assembled to provide recommendations on taking advantage of the 'data revolution' to achieve the Sustainable Development Goals (SDGs).⁴⁶ The Group's report provided recommendations, including one for 'global standards on data privacy', and highlighted some data privacy principles.⁴⁷ The (then) Secretary-General's final report, however, did not go beyond emphasising the need to uphold the protection of privacy in making use of data for achieving SDGs.⁴⁸

More substantive and focused initiatives that seek to introduce a new or expanded set of privacy standards have also emerged. This thesis focuses on two of such initiatives that are normatively substantive, and with some potential to foster the progressive development of international law.⁴⁹ One post-Snowden initiative takes a form of IBRs. While the idea of IBRs predates the Snowden revelations,⁵⁰ IBRs initiatives of various forms and types have emerged in the wake of the revelations. While some are already adopted – or are tabled – in the form of national legislation, most are launched as advocacy and hortatory instruments.⁵¹ Most IBRs documents embody a set of digital rights, principles and governance forms, including on the right to privacy which often is specified into several rights and principles.

The other major post-Snowden initiative is the ongoing discourse at the UN on the 'right to privacy in the digital age'.⁵² As part of this discourse, the UN has so far adopted a series of Resolutions which incrementally flag some substantive privacy principles. In what appears to be a cross-fertilization of norms, these soft law instruments tend to further develop the corpus of the human right to privacy in international law based on various sources, including IBRs. The recent appointment of a SRP is also one outcome of this developing discourse. Further, and importantly, the series of Resolutions adopted both by the UN General Assembly (UNGA) and

Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty (Oxford University Press, 2011) ch 9.

⁴⁶ 'Data Revolution Advisory Group Named by UN Secretary General' (UN Media Release, 29 August 2014) <<http://bit.ly/2mycqzs>>

⁴⁷ 'A World That Counts: Mobilizing the Data Revolution for Sustainable Development' (Report Prepared at the Request of the UN Secretary General by the Independent Expert Advisory Group on a Data Revolution for Sustainable Development, November 2014) 3, 21-23.

⁴⁸ See *The Road to Dignity by 2030: Ending Poverty, Transforming All Lives and Protecting the Planet*, Synthesis Report of the UN Secretary-General on the Post-2015 Agenda, UN Doc A/69/700 (December 2014) 39.

⁴⁹ For purposes of this thesis, the expression 'progressive development of international law' is not intended to represent its technical meaning in the Statute of the International Law Commission. The use here is in its ordinary meaning by which it captures the development of international law (of privacy), including but not limited to, through legislative, quasi-legislative, and judicial mechanisms. Cf *Statute of the International Law Commission* (21 November 1947) art 15.

⁵⁰ For an earlier discussion on IBRs, see Stefano Rodotà, 'A Bill of Rights for the Internet Universe' (2008) 21 *The Federalist Debate* 1.

⁵¹ See ch 3.

⁵² See ch 4.

the Human Rights Council (HR Council) are gradually, albeit less coherently, elucidating the content of right to privacy. Critically, the Resolutions tend to specify the role of Internet corporations.

D Argument of the Thesis

The thesis joins the debate on the appropriateness of global privacy standards but approaches it in a particular manner, i.e. from the perspective of two international privacy initiatives. It examines the roles of these emerging initiatives in reimagining the international law of privacy in a manner that accommodates the new realities of the digital age. The thesis adopts a three-level framework of analysis, focusing on the 'freestanding', 'contributory' and 'catalytic' roles of the initiatives. The 'freestanding role' concerns the way in which the respective initiative would evolve as an autonomous international law response to the privacy problem. The possibility of shaping the development of law (international, regional or national), judicial and industry practices describes the 'contributory role'. By 'catalytic role', the reference is to the potential of the relevant initiative to shape the 'normative and methodological direction' of future reforms of the international law of privacy.⁵³

The thesis argues that emergent privacy norms of these progressive initiatives have some potential in further developing the right to privacy based on the new realities of the digital environment. But it contends that a number of factors limit the extent to which these initiatives may contribute towards reimagining international privacy law in the digital age. To address this impasse, the thesis argues that what is needed now is an approach that builds on, but goes beyond, the merits of these initiatives. Mapped against the UN human right framework, the thesis proposes a pragmatic, but principled, approach to international privacy law that is suitable to deal with the 'privacy problem' in the digital age.⁵⁴

The thesis chooses to use IBRs and the UN Privacy discourse as case studies for three reasons. First, these two initiatives have a potential to spur the progressive development of international law of privacy. As shall be shown in chapters 3 and 4, both initiatives cast the right to privacy in a more sophisticated and elaborate manner. This departs from the high-level nature of other privacy initiatives, or proposals. And, this makes them appropriate case studies to examine their role in reimagining international law of privacy in the digital age. Second, the two initiatives are generally global in scope, and hence, offer a useful vantage point in examining the role of international law in securing the right to privacy in the digital age. The series of UN Privacy Resolutions, for instance, are international soft laws that tend to reimagine the existing international privacy framework. Third, unlike

⁵³ The terms 'normative direction' is borrowed from Koh. See Koh, below n 803, 270.

⁵⁴ Cf Alexandra Huneus, 'Human Rights and the Future of Being Human' (2018) 112 *AJIL Unbound Symposium on UDHR at 70 and the Future of Being Human* 324, 328 [Noting that human rights law (and discourse) generally offers a framework for varying conversations and serve as a 'site of cross-fertilization'].

other initiatives highlighted above, the case studies are part of a relatively sustained and coherent global privacy discourse. As shall be shown, both initiatives have incrementally evolved over the years, particularly since the Snowden revelations. The UN Privacy discourse, for example, is still ongoing with new and substantive resolutions being adopted both by the UNGA and HR Council.

II STATE OF THE ART AND THE RESEARCH QUESTION

Scholarship that considers questions around an international privacy framework predates the Snowden revelations. One finds incidental scholarly commentary on whether, and in what form, an international (data) privacy framework is needed.⁵⁵ The debate on the need for, and pertinent form of such framework, has, however, taken on a new force in the wake of the revelations. And as yet, there is little consensus, despite a general agreement on the need for a global privacy framework, on the nature and form of such framework has divided academic commentary. Moreover, a closer review of the literature reveals that it has barely considered the role of emerging privacy initiatives in fulfilling the goals of that long-sought ‘global privacy framework’ or more generally in reimagining the international law of privacy in the digital age. Nor has it been part of a sustained discussion, as almost every scholarly viewpoint emerged in isolation of the others. Nevertheless, some common themes can be discerned. The scholarship in this area can be subsumed into four broad categories. What follows examines each category, its limits and poses research question(s) to situate the thesis in the literature. A caveat is, however, in order: the survey of the literature is restricted to scholarship written in English due to the author’s language limitation. That said, the survey is sufficiently — if not definitely — covers all the relevant literature, and no non-English literature has been deliberately omitted because of language constraints.

A The Status Quo Approach

In the first category, one finds scholarship that appears to favour maintaining the status quo. It simply assesses the compatibility or otherwise of the surveillance practices disclosed by the Snowden revelations with present international human rights law.⁵⁶ In so doing, it assumes that existing standards are fit for purpose in the digital age, and hence leaves aside investigating the value of new normative standards. Part of the reason for reliance on existing law appears to be challenges of realizing any stronger international framework in the present political reality. But

⁵⁵ See, e.g., Kuner, above n 40.

⁵⁶ See, e.g., Ilina Georgieva, ‘The Right to Privacy Under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR’ (2015) 31 *Utrecht Journal of International and European Law* 104, 104-130; Stephen Schulhofer, ‘An International Right to Privacy? Be Careful What You Wish For’ (2016) 14 *International Journal of Constitutional Law* 238, 239-261.

this also means that the potential of emerging initiatives is overlooked in this literature.

A version of the status quo perspective, prompted partly by the uncertainties of or gaps in treaty law, reaches to other sources of (international) law. One viewpoint holds that the right to privacy is now a rule of customary international law, and hence applies against all States.⁵⁷ The existence of a rule of customary international privacy law is argued for based on the wider recognition of the right to privacy in domestic and regional law as well as the recent adoption of Privacy Resolutions by the UN. Another viewpoint, advanced by Sourgens, holds that the right to privacy has attained the status of 'general principles of law' because of the widespread recognition of the right to privacy in the private law of major legal systems of the world.⁵⁸

Such attempts to look beyond treaty law, but still within the existing(international) law, appear to settle for the status quoin terms of standards. That is, there is no suggestion that a new set of human rights standards are necessary, or even if necessary – due to perhaps the usual feasibility concerns associated with establishing new treaty law, rules of general international law would provide adequate protection to digital privacy. As discussed further in chapter 4, such attempts to draw from rules of customary international law, or general principles of law, do little to remedy the inadequacy of the international law of privacy. To what degree the existence of a customary norm or general principles would assist in reimagining international privacy law is thus not entirely clear. Because the purported customary norm(s) draws from existing privacy standards, the role of emergent privacy law in strengthening international privacy law's normative architecture is not also considered. Sourgens' argument even raises a question of whether general principles of law could be distilled from domestic private laws. This is precisely because the right to privacy, as an international human right, is a matter of (international) public law.

B The Hard Legalization Approach

A second category of literature, which opts for some form of hard law option, comes in various forms. One argues for 'internationalizing' a regional law, a common candidate being the CoE Data Protection Convention 108.⁵⁹ This viewpoint sees the Convention as the most, if not the only, viable option towards an international (data) privacy law through accession by States that are not members of the CoE. The accession mechanism has so far brought a handful of countries within the

⁵⁷ See, e.g., Alexandra Rengel, *Privacy in the 21st Century* (Martinus Nijhoff, 2013) 108; Monika Zalnieriute, 'An International Constitutional Moment for Data Privacy' (2015) 23 *International Journal of Law and Information Technology* 99, 121 et seq.

⁵⁸ Frédéric Sourgens, 'The Privacy Principle' (2017) 42 *Yale Journal of International Law* 345, 367-392.

⁵⁹ See, e.g., Graham Greenleaf, 'A World Data Privacy Treaty? 'Globalisation' and 'Modernisation' of Council of Europe Convention 108' in Witzleb et al (eds), above n 15, 92-138.

Convention System.⁶⁰ But, the potential of the Convention as a future of international law of privacy may be overestimated. For one, it evidently focusses only on an aspect of the right to privacy – i.e. processing of personal data – and does not address other important aspects of digital privacy such as government surveillance practices. Indeed, as in many data privacy instruments, the Convention does not apply in cases where processing of personal data is undertaken, inter alia, for national security purposes. State parties could make a declaration that exempts data processing for national security purposes.⁶¹

Regulation of government surveillance measures, including by spy agencies, law enforcement and immigration authorities as well as domain-specific regulatory agencies, falls in a separate area of law sometimes referred to as – in the domestic context – ‘law of national security surveillance’.⁶² And, no comprehensive international treaty regulating government surveillance, including intelligence sharing between governments, currently exists.⁶³ The recently adopted modernized convention, Convention 108+, slightly rolls back the current national security exemption. But it still permits exceptions under certain conditions when personal data is processed for national security purposes.⁶⁴

Secondly, the CoE Convention is not a self-executing, or self-contained, instrument. This means that no institutional regime tailored to enforce it is envisaged. The Convention, and its Additional Protocol, provides for a set of data privacy principles and mandates the creation of domestic data protection authorities by State parties. The modernization of the Convention has not also gone far enough in strengthening the role of the ‘Consultative Committee’, now renamed as the ‘Convention Committee’. To a large extent, the Committee retains its advisory role.⁶⁵ Thus, the lack of a dedicated enforcement machinery reduces the Convention’s potential to, by and large, a model law. In countries where rule of law is not sufficiently upheld, relevant institutions lack independence and resources, and where there are no robust civil society networks, the Convention – once acceded to – might not bring about significant difference in terms of (data) privacy protection. Many countries, particularly in Africa, where data privacy legislation has recently been introduced are also yet to install data protection authorities.

⁶⁰ See details at <<https://bit.ly/2Mh8tvp>>

⁶¹ See *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, opened for signature 28 January 1981, ETS No. 108 (entered into force 1 October 1981) art 3(2).

⁶² See, e.g., Francesca Bignami and Giorgio Resta, ‘Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance’ in Eyal Benvenisti and Georg Nolte (eds), *Community Interests Across International Law* (Oxford University Press, 2018) 357-358.

⁶³ See Ashly Deeks, ‘Regulating Foreign Surveillance Through International Law’ in Fred Cate and James Dempsey (eds), *Bulk Collection: Systematic Government Access to Private-Sector Data* (Oxford University Press, 2017) 351-353.

⁶⁴ *Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, opened for signature 10 October 2018, CETS No. 223 (not yet in force) art 11(1(a)).

⁶⁵ *Ibid*, art 23.

One possibility by which provisions of the Convention may find some enforcement is through the European Court of Human Rights (ECtHR) by which the Court draws from the Convention in interpreting Article 8 of the European Convention on Human Rights and Fundamental Freedoms (ECHR). But this also comes with its own limitations. One is that the jurisdiction of the ECtHR is limited to the 47 CoE member States, and secondly, whether the Court could rely on an extraneous instrument in applying the Article 8 is open to debate on legitimacy grounds.⁶⁶ Greenleaf, who has long advocated for the ‘globalization’ of Convention 108 through accession by non-CoE member States, recently suggested a way to address this institutional gap. He argues that once acceding States are required by the CoE to simultaneously ratify the First Optional Protocol to the International Covenant on Civil and Political Rights (ICCPR), which mandates a complaints procedure, the CoE 108’s provisions could be enforced by the HR Committee.⁶⁷

Given that the Committee’s mandate is to apply only the ICCPR, the suggestion raises a question of competence. But importantly, the slow pace in which the accession by non-State parties have moved so far reduces the appeal of Greenleaf’s idea of globalizing Convention 108. Since 2013, only a handful of non-CoE member States have acceded to the Convention.⁶⁸ And, the accession so far – like the recent surge in adoption of national data privacy legislation worldwide – is arguably prompted by pragmatic economic considerations, particularly with a view to facilitate trade with the EU.⁶⁹ Human rights considerations have thus taken the back seat. Making accession to the convention conditional upon ratifying another, less favoured, treaty may also reduce the appeal of accession as a ‘globalization’ device. These contexts reduce the potential of globalizing the CoE data privacy Convention. Moreover, the prospect of a global privacy treaty mediated by the CoE, as Bygrave notes, will be affected by its regional status and bias.⁷⁰

A regional approach to global governance of critical issues like digital privacy can also be problematic more generally. The international relations literature cautions that regional mechanisms could be impediments towards seeking a more global

⁶⁶ For legitimacy questions in the context of ECtHR, see Michael Hamilton and Antoine Buyse, ‘Human Rights Courts as Norm-Brokers’ (2018) 18 *Human Rights Law Review* 205, 207, 212, 216.

⁶⁷ Graham Greenleaf, ‘The UN Special Rapporteur: Advancing A Global Privacy Treaty?’ (2015) 136 *Privacy Laws and International Business Report* 6, 7-9; for a recent iteration, see Graham Greenleaf, ‘The UN Should Adopt Data Protection Convention 108 as Global Treaty’ (Law Research Series No 24, University of New South Wales, 2018) 2-5.

⁶⁸ See <<https://bit.ly/2IPrMPPr>>

⁶⁹ See, e.g., Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press, 2015) 43; on the recent proliferation of data privacy legislation in Africa prompted by trade considerations, see Alex Makulilo, ‘The Future of Data Protection in Africa’ in Alex Makulilo (ed), *African Data Privacy Laws* (Springer, 2016) 371-373. One of the driving factors for the enactment of the Australian Privacy (Private Sector) Amendment Act 2000 was similar trade consideration. See, e.g., ‘Explanatory Memorandum’, Privacy (Private Sector) Amendment Bill 2000 (Cth) 11.

⁷⁰ Lee Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014) 206-207.

solution to critical global challenges like ‘privacy problem’.⁷¹ States with strong bureaucratic structures and economic power may resist the pursuit of an international response. Add to this the fact that regional mechanisms generally have uneven capacities to respond even at the regional level. As noted above, regional bodies such the AU are not as institutionally capable as the CoE is in addressing the ‘privacy problem’ in the digital age.

A related proposal seeks to show the plausibility of introducing a global (data) privacy treaty negotiated under the auspices of the World Trade Organization (WTO).⁷² Nomination of the WTO as a possible forum relies on three points: its organizational mandate of lowering global trade barriers, its robust institutional apparatus and its ‘all-in organizational structure’ covering most trade-related matters.⁷³ Sinnreich suggests that the proposed treaty must be restricted to setting the ‘minimum thresholds’ for data privacy laws in member States such as maximum period of data retention and the required text of privacy policies.⁷⁴ Besides the feasibility concern particularly given ongoing trade wars, the proposal faces a number of other hurdles.

As Sinnreich himself admits, the primary objection to the proposal would come from the WTO which consistently distanced itself from being a forum for addressing digital privacy matters.⁷⁵ The institutional mandate of the WTO, i.e. to facilitate free international trade, including transborder data flows, makes it also less pertinent for data privacy legislation whose underlying goal rather is to protect (data) privacy without unnecessarily limiting free trade. This point relates to what Bygrave ascribes to the ‘commercial bias’ of the WTO to sufficiently and impartially uphold data privacy interests.⁷⁶ The likelihood of a WTO-based data privacy treaty seems even less when considering the fact that its resources are already absorbed by administering numerous trade-related agreements.

Narrower treaty options are argued for in the other area of scholarship on government surveillance, be it under the auspices of the CoE,⁷⁷ a global instrument built around a set of procedural norms on surveillance drawn from domestic laws of

⁷¹ See, e.g., Ian Goldin, *Divided Nations: Why Global Governance is Failing, and What We Can Do About It* (Oxford University Press, 2013) 91-92.

⁷² Aram Sinnreich, ‘An International Approach to Data Privacy’ (Policy Briefing Note, Center for Media and Social Impact, American University, August 2018) 8-9; for an earlier contemplation of the WTO as a possible forum for international (data) privacy treaty, see Colin Bennett and Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, 2006) 108.

⁷³ *Ibid.*

⁷⁴ *Ibid.*

⁷⁵ See ‘The WTO and Internet Privacy’ (Fact and Fiction: Misunderstanding and Scare Stories) <<https://bit.ly/2P9arPD>> (noting that ‘the WTO has had nothing whatever to do with Internet privacy’).

⁷⁶ Bygrave, above n 70, 48.

⁷⁷ Eliza Watt, ‘The Right to Privacy and the Future of Mass Surveillance’ (2017) 21 *The International Journal of Human Rights* 773, 773-799.

western countries,⁷⁸ a treaty exclusively among western democratic countries,⁷⁹ a merely EU-US ‘no-spy’ agreement,⁸⁰ or just an additional protocol to Article 17 of the ICCPR that clarifies the issue of extraterritoriality.⁸¹ Scholarship in this group not only is limited to ‘digital surveillance’ but also narrower in scope, both in terms of who gets to join the treaty and normative sources. But importantly, this category mostly overlooks emerging initiatives such as IBRs and the UN privacy discourse, and hence their normative significance in filling the void in global surveillance regulation.

A smaller section of the scholarship in this category advocates a broader treaty option. One, for instance, calls for ‘global privacy standards’ that primarily embrace a general right to privacy that, among other themes, recognizes the extraterritorial application of the right.⁸² Specifics of this proposal, however, are left wanting: for instance, what content the general right would have, how such a right would be adopted, and in what form? Also unclear is how such a right would interact with existing international rules/rights such as Article 17 of the ICCPR – would it repeal these or be a supplemental/ amendment sub-right? Another related proposal has been for an IBRs to be adopted by a ‘public supranational legislator’ based on input from the private sector.⁸³ Similar problems of ambiguity as to the scope and authority of the instrument, and at which level it would be adopted, arise here as well.

Other broader concerns bedevil this category of scholarship. One is that no plausible reason is offered as to why, and whether, such a proposed treaty is feasible in the present reality of international politics. As Bygrave rightly notes, the prospects of a (data) privacy treaty will be frustrated by a host of factors, including ideological differences, other policy considerations such as national security and trade as well as the lack of a pertinent body to broker the instrument.⁸⁴ And whether a proposed

⁷⁸ Ashley Deeks, ‘An International Legal Framework for Surveillance’ (2015) 55 *Virginia Journal of International Law* 291, 293 et seq.

⁷⁹ See generally Ian Brown et al, ‘Towards Multilateral Standards for Surveillance Reforms’ (Oxford Internet Institute Discussion Paper, 2015).

⁸⁰ David Cole and Federico Fabbrini, ‘Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders’ (2016) 14 *International Journal of Constitutional Law* 220, 220-237; see also Ian Brown, ‘The Feasibility of Transatlantic Privacy-protective Standards for Surveillance’ (2015) 23 *International Journal of Law and Information Technology* 23.

⁸¹ Jordan Paust, ‘Can You Hear Me Now? Private Communication, National Security, and the Human Rights Disconnect’ (2015) 15 *Chicago Journal of International Law* 612, 612-651.

⁸² Valsamis Mitsilegas, ‘Surveillance and Digital Privacy in the Transatlantic “War on Terror”: The Case for A Global Privacy Regime’ (2016) 47 *Columbia Human Rights Law Review* 1, 73-77.

⁸³ Giovanna De Minico, ‘Towards an Internet Bill of Rights’ (2015) 37 *Loyola of Los Angeles International and Comparative Law Review* 1, 19-30.

⁸⁴ Bygrave, above n 70, 205-207; see also Lauren Saadat and Shannon Ballard, ‘A Way Ahead for Global Privacy Standards? – Thoughts on a UN Convention on Data Protection, International Standards and International Agreements: Which is the Best Option?’ (2007) 89 *Privacy Laws and Business* 14, 15.

treaty, once drafted and adopted, would be signed and ratified by a critical mass of States is highly uncertain.⁸⁵ The wider membership of the UN might also emerge as a challenge in building consensus around a global instrument.⁸⁶ Indeed, one of the reasons the UN itself had been hesitant in proposing an international (privacy) instrument is the perceived divergence of opinion on how such an instrument would fare with other existing rights and the different legal contexts in which such legislation would operate.⁸⁷ The extent of this challenge might have multiplied over the past few decades or so due to the phenomenon called in the international relations literature ‘multipolarity’.⁸⁸ The number of States, added to the diversity of their interests and the complexity of modern global problems, has grown exponentially thereby making the prospect of global consensus on critical global issues less likely.

The common feasibility concern aside, the constant failure to reconcile the proposed treaty option with the existing treaty (and soft law) regime is a limitation of the literature. This is significant in that any reform idea, unless it explicates how it interacts with or complements, or even supplants, the existing framework, is unlikely to materialize.

C The Institutionalist Approach

Another area of scholarship favours an institutional rearrangement, either through the creation of a new monitoring body or revitalization of existing institutions. De Hert and Papakonstantinou argue that the missing link in global (data) privacy protection is the lack of an agency tasked to oversee protection of data privacy in the context of transnational data processing.⁸⁹ In their view, once the institutional gap is filled, existing law particularly the UN Data Privacy Guidelines already offers – at least tentatively – sufficient normative guidance. De Hert and Papakonstantinou suggest that the proposed agency could be fashioned like the World Intellectual Property Organization (WIPO), an inter-governmental specialized agency of the UN.

⁸⁵ Ibid, 206.

⁸⁶ See Perry Keller, *European and International Media Law: Liberal Democracy, Trade and the New Media* (Oxford University Press, 2011) 349.

⁸⁷ See Report of the Secretary-General, *Respect for the Privacy of Individuals and Integrity and Sovereignty of Nations in the Light of Advances in Recording and Other Techniques*, UN Doc E/CN.4/1116 (23 January 1973) [177].

⁸⁸ See, e.g., Thomas Hale et al, *Gridlock: Why Global Cooperation Is Failing When We Need It Most* (Polity Press, 2013) 34-40.

⁸⁹ Paul De Hert and Vagelis Papakonstantinou, ‘Moving Beyond the Special Rapporteur on Privacy with the Establishment of a New, Specialized United Nations Agency: Addressing the Deficit in Global Cooperation for the Protection of Data Privacy’ in Dan Svantesson and Dariusz Kloza (eds), *Transatlantic Privacy Relations as a Challenge to Democracy* (Intersentia, 2017) 521-532. For an earlier (and longer) rendition of the argument, see Paul De Hert and Vagelis Papakonstantinou, ‘Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?’ (2013) 9 I/S: *A Journal of Law and Policy for the Information Society* 271 et seq.

While the authors do not explicitly call for a data privacy treaty per se – at least as a matter of urgency – their support for a new agency presupposes the negotiation and adoption of a treaty. The WIPO is an inter-governmental agency created through a treaty: the WIPO Convention.⁹⁰ It is also not fully clear whether the idea of a new agency seeks to use relevant existing treaties such as the ICCPR as legal basis in lieu of negotiating one anew. But even this would be a peculiar proposition, not least because some form of legislative measure, most likely an amendment to the ICCPR, would be required to create the proposed agency.⁹¹ This, in turn, raises the same issue of feasibility associated with a treaty solution.

To what extent the proposed data privacy agency would address institutional concerns associated with the right to privacy is also questionable. The possible functions of the proposed agency, for example whether it would also be an adjudicative body, is not clear. Based on the WIPO analogy, the most the agency could do is promotion of global data privacy protection and facilitating cooperation among States.⁹² The rather desirable options for access to remedies, for example available through domestic data privacy authorities and courts, cannot be achieved through a WIPO-type data privacy agency. WIPO's alternative dispute resolution services also do not seem to be ideal to matters concerning data privacy.

Moreover, the argument – at least in its updated version – springs from the perception that the appointment of a SRP is an inadequate institutional response. In that sense, it appears to underestimate the potential of the already existing institutional arrangements such as the HR Committee. But more fundamentally, the institutionalist perspective overvalues the UN Data Privacy Guidelines which, as shall be shown in chapter 2, are mostly superseded by progressive data privacy standards elsewhere. As such, it does not consider whether and the ways in which emergent privacy standards may complement or revitalize extant UN data privacy standards to bring them up to speed with post-1990 developments in the data protection arena.

A slightly varied version of the institutionalist perspective expects existing institutional structures to step up and adapt existing privacy standards to the new realities of the digital age. Fischer-Lescano argues that the HR Committee should apply the right to privacy directly in the context of interference both by States and Internet corporations.⁹³ In light of the considerable influence of these corporations in

⁹⁰ *Convention Establishing the World Intellectual Property Organization* opened for signature 14 July 1967 (entered into force 1 June 1984) [as amended in 1979].

⁹¹ Another concern associated with WIPO is bias. It is said to be ' beholden to intellectual property interests'. See, e.g., Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press, 2006) 170.

⁹² See WIPO Convention, above n 90, art 4.

⁹³ Andreas Fischer-Lescano, 'Struggles for a Global Internet Constitution: Protecting Global Communication Structures Against Surveillance Measures' (2016) 5 *Global Constitutionalism* 145, 145-172.

the digital space, the traditional ‘statist’ scope of human rights law is unsustainable, and they must be held directly accountable. He further suggests that the Committee must interpret the right to privacy broadly to encompass a ‘right to cryptography’ that imposes an obligation on both States and corporations to ‘promote opportunities for use of cryptography’.⁹⁴ The Committee could – within its limited capacity and resources – pursue, the argument goes, doctrinal adaptations of the ICCPR to cyberspace.

While this view pragmatically builds on the present framework, it leaves open some fundamental issues. One is that it offers little as to how, and on what basis, such ‘doctrinal adaption’ would be pursued by the Committee. Is it through progressive interpretation of the ICCPR, or drawing from comparative sources? Secondly, it tends to overvalue the capacity of the Committee, a part-time body of experts that operates through three sessions annually, each held just for four weeks. Thirdly, the legal basis to unilaterally impose direct human rights obligation on corporations is doubtful. In the absence of some form of legislative support that gives such new mandate, and of course political support of States and the private sector, it appears to be an untenable proposition.

As discussed in chapter 1, both early and ongoing UN efforts of introducing a legally binding instrument on business and human rights have met stiff resistance from some States and transnational corporations. Fischer-Lescano’s call for a ‘right to cryptography’ echoes the IBRs Project’s trademark ‘right to (use) encryption’ but nowhere is there a mention of IBRs or the UN Privacy Resolutions where the use of encryption is increasingly emerging as an important theme. The purported obligation of ‘promoting opportunities’ is also ambiguous as to, for instance, whether it would involve just a negative obligation or positive obligation as well.⁹⁵

*D The Soft Legalization Approach*⁹⁶

A final area of the literature favours a soft law approach towards reimagining privacy in digital age. The fledgling scholarship on IBRs appears to envision a sort of cosmopolitan ‘Internet constitution’ that shapes policy and judicial practice at the local level. Rodotà, for instance, envisions a charter of rights for the Internet that a ‘crowd of judges’ in each jurisdiction would apply in addressing questions of human

⁹⁴ Ibid, 170.

⁹⁵ A related institutionalist viewpoint supports a multi-level ‘transnationalization of rights’, including the right to privacy. Alwicker recommends that progressive interpretation of international human rights by relevant stakeholders including courts, transnational civil society actors and legislatures. Details of the proposed interpretive approach are, however, left wanting. See Tilmann Alwicker, ‘Transnationalizing Rights: International Human Rights Law in Cross-Border Contexts’ (2018) 29 *European Journal of International Law* 581, 604-606.

⁹⁶ With apologies to Abbott et al for the terms ‘soft legalization’, which captures the codification of international law rules in soft law. See Kenneth Abbott et al, ‘The Concept of Legalization’ (2000) 54 *International Organization* 401, 401-402.

rights on the Internet.⁹⁷ But to which such instrument reference will be made is not clear. Whether it is envisioning a newer instrument to be adopted, or just referring to one or more of the existing IBRs such as the one launched under the auspices of the UN Internet Governance Forum (IGF), is not readily clear.⁹⁸ If it is the latter, a question of competence arises – on what legal basis would domestic courts refer to an external instrument like IBRs in their interpretive exercises?

A variant of the soft legalization approach is the support for a ‘model law’ that would provide guidance to domestic lawmakers,⁹⁹ or a soft law in the form of a treaty body GC.¹⁰⁰ The model law proposal is based on several of the United Nations Commission on International Trade Law’s (UNCITRAL) model laws. But as in the case of the ‘internationalizing regional law’ approach discussed above, this proposal substantially relegates the matter to States, to adopt and apply the law. That the model law would be non-binding further reduces the impact of the law in bringing about tangible results.

E The Disjunction in Approaches

In addition to the specific points about each area of literature discussed above, there are three overarching limitations applicable to the field. Firstly, the debate was not always part of a sustained discourse. Some scholarly viewpoints emerged in total isolation of, or without any visible engagement with, other viewpoints. One may attribute this disjoint in the academic debate to two factors. A primary factor could be the fledgling nature of the literature on the international aspect of the right to privacy. As the above survey of the literature illustrates, a robust body of scholarship on international privacy law is yet to emerge. The other factor relates to the short lifespan of the Internet. This would mean that the legal discourse around it is at the early stages in examining the implications of the Internet on international

⁹⁷ See Rodotà, above n 50; see also Rikke Jorgensen, ‘An Internet Bill of Rights?’ in Ian Brown (ed), *Research Handbook on Governance of the Internet* (Edward Elgar, 2013) 369-370. For a related argument for a ‘non-hierarchical’ IBRs to be created in a multi-stakeholder fashion, see Wolfgang Benedek et al, ‘The Humanization of Internet Governance: A Roadmap Towards a Comprehensive Global (Human) Rights Architecture for the Internet’ (Paper presented at the 3rd Annual GigaNet Symposium, Hyderabad, India, 2 December 2008).

⁹⁸ See ‘Charter of Human Rights and Principles for the Internet’ (5th ed, 2018); see also ch 3. In an earlier work, Rodotà had flagged the idea of drafting an ‘informational constitution’ or ‘information bill of rights’ but does not go beyond casually mentioning that the said bill of rights would guarantee the ‘right to search for, receive and distribute information, the right to informational self-determination and the right to informational privacy’. As such, common IBRs are not envisaged in the ‘informational constitution’. See Stefano Rodotà, ‘Protecting Informational Privacy: Trends and Problems’ in Willem Ates et al (eds), *Information Law Towards The 21st Century* (Kluwer Law and Taxation Publishers, 1992) 264.

⁹⁹ See Christopher Kuner, ‘The European Union and the Search for an International Data Protection Framework’ (2014) 2 *Groningen Journal of International Law* 54, 66-67.

¹⁰⁰ See, e.g., Rikke Jorgensen, Can Human Rights Law Bend Mass Surveillance? (2018) 3 *Internet Policy Review* 1, 6.

law and vice versa.¹⁰¹ As Raustiala rightly notes, ‘despite its global importance, the Internet remains little studied by international lawyers’.¹⁰² This means the role of international law in attending to the ‘privacy problem’ has not been a subject of comprehensive and sustained inquiry.

Secondly, the literature fails to provide a complete perspective on the inadequacies of international privacy law in protecting digital privacy. As the above discussion suggests, each proposal addresses only an aspect of the right to privacy in international law. No major attempt has, therefore, been made to look at the questions regarding the right to privacy in a comprehensive manner. This study is an attempt to lessen that void in the literature by undertaking an international law analysis of the right to privacy in the digital age.

Thirdly, the existing scholarship does not address the role of emerging initiatives such as IBRs and the ongoing UN privacy discourse in reimagining the right to privacy in international law. As shall be examined in chapters 3 and 4, these initiatives tend to envision the right to privacy in a new light that would partly respond to gaps in the present international privacy law. The thesis draws upon the progressive tendencies of these initiatives, exploring the ways in which international privacy may be reimagined in the digital age.

F The Research Question

The central question of the thesis is how international law should, or could, respond to the new challenges of securing digital privacy. Unlike earlier literature, it asks what role that emerging international privacy initiatives play in the progressive development of international privacy law to accommodate the realities of the digital age. In the process, it further asks the following auxiliary questions:

- a. What is the current state of international privacy law in securing the right to privacy in the digital environment, and how has this been shaped by historical antecedents?
- b. What are the roles of IBRs initiatives and the evolving UN discourse on the ‘right to privacy in the digital age’ in reimagining international privacy law?
- c. What is the pragmatic international law response to the ‘privacy problem’ in the digital age?

The central argument is that rethinking the right to privacy in international law must entail a comprehensive approach that critically embraces but goes beyond emerging global reform initiatives. In so doing, it must be geared towards a focused and practical approach that offers effective solutions to the privacy problem in the digital age.

¹⁰¹ See Michael Schmitt, ‘Introduction’ in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar, 2015) 2-3.

¹⁰² Kal Raustiala, ‘Governing the Internet’ (2016) 110 *American Journal of International Law* 491, 492.

III METHODOLOGY AND ANALYTICAL FRAMEWORK

The thesis primarily adopts a doctrinal research method, examining the role of *current* international law of privacy and *emergent* standards in upholding digital privacy. Thus, the focus is on existing and emergent norms, rights and principles on the right to privacy in international law. These include relevant privacy rules of international human rights and data privacy laws as well as emergent privacy norms contained in IBRs initiatives and UN Privacy Resolutions. Reference is also made to a range of relevant literature from diverse areas of law, including human rights law, public international law, data privacy law, Internet law and theories of rights. That the applicable digital privacy norms draw from multiple sources means that the literature is also diverse. For example, the relevant literature on theories of rights is considered in examining the nature and legal significance of IBRs.

To some extent, the thesis also employs a comparative approach. It does so mainly in two respects. One is when it examines gaps in current international law of privacy. The law and practice of regional systems of human rights and data privacy protection are referred to where applicable. The second is in investigating the nature and scope of IBRs initiatives and UN Privacy Resolutions. Both the IBRs Project and the Privacy Resolutions are products of cross-fertilization of norms, including norms and principles borrowed from domestic and regional laws. In examining these emergent privacy norms, incidental references are made to their counterparts in domestic or regional law and judicial decisions with a view to properly explicate the nature, scope and significance of these norms.

This thesis proceeds from the premise that the right to privacy *is* a fundamental and universally accepted human right, subject to restriction only under legally prescribed conditions.¹⁰³ But as flagged in section I above – and further explored in chapters 1 and 2, current international law of privacy is largely unfit for the digital age. In the process of exploring ways of reimagining the law in the digital age, the thesis adopts a pragmatic approach. This pragmatic orientation of the thesis has parallels with the little-known pragmatic approach to international law articulated by Schieder.¹⁰⁴ While his theoretical approach is premised on the traditional ‘statist’ nature of general international law, its five key elements largely coincide with the thesis’s analytical framework.¹⁰⁵ Thus, the pragmatic approach to international privacy law explored in the thesis has four key components: *incremental and*

¹⁰³ See, e.g., generally Beate Roessler, ‘Privacy as a Human Rights’ in (2017) 117 *Proceedings of the Aristotelian Society* 187.

¹⁰⁴ See Siegfried Schieder, ‘Pragmatism and International Law’ in Harry Bauer and Elisabetta Brighi (eds), *Pragmatism in International Relations* (Routledge, 2009); see also Siegfried Schieder, ‘Pragmatism as a Path Towards A Discursive and Open Theory of International Law’ (2000)11 *European Journal of International Law* 663. [Translated by Iain Fraser].

¹⁰⁵ These five key elements are: instrumentalism, historicism, contextualism, perspectivism and eclecticism.

*historically-minded, practical, programmatic, and multi-faceted.*¹⁰⁶ These features orient the examination throughout the thesis.

A primary component of the thesis's pragmatic approach is that it is *incremental and historically-minded*. Its 'incremental' nature captures that fact that it is mapped onto, builds on and is supplementary to present structures of privacy law in general and international privacy law in particular.¹⁰⁷ Reform ideas explored in chapters 5 and 6 are meant to fill gaps – both normative and institutional – in international law explored in chapters 1 and 2. This supports the overall 'historically-minded' orientation of the thesis, capturing the idea that answers to existing and emerging challenges are usefully informed by history. In particular, the thesis emphasises on relevant historical occurrences in international human rights law in looking to the future of the right to privacy. Chapters 1 and 2, for instance, look back at the drafting history of the respective regimes for the protection of the rights to privacy and data privacy in order to properly appreciate the present framework. Normative and institutional reform ideas proposed in chapters 5 and 6 are also historically-minded. The proposed soft law is inspired by several precedents in the UN practice, as is the proposed privacy forum.

The second component is *practical* which conveys the relative suitability of measures for implementation.¹⁰⁸ As noted already, the primary objective of the thesis is to propose a set of measures that would effectively address international law's privacy problem. In that spirit, chapters 5 and 6 propose a suite of practical measures designed to lessen normative and institutional gaps in the international law of privacy.

Programmatic is the third component which reflects the anti-formalist feature of pragmatism in that law and juridical decision making must be open to new experiences and reversibility to adjust to new developments.¹⁰⁹ This makes it a dynamic and progressive approach as opposed to an approach that sees law as a fixed set of rules and processes. The thesis's approach to the right to privacy seeks to clarify ways by which international law can be moulded to remain fit for purpose in

¹⁰⁶ Note also that these elements of pragmatism correspond to four features of the 'constructive approach' to human rights treaty interpretation developed by Tobin: *principled, clear and practical, coherent in reasoning and context sensitivity*. See Tobin, above n 26, 15-48. These are noted further below.

¹⁰⁷ Cf 'principled interpretation'. Tobin, id, 15, citing also Maarten Bos, 'Theory and Practice of Treaty Interpretation' (1980) 27 *Netherlands International Law Review* 135 (stating that for a treaty interpretation to be persuasive, it must be made in light of principles agreed upon by the interpretative community).

¹⁰⁸ Cf 'clear and practical interpretation'. Id, 25, citing also Bos, above n 107 (noting the need for a treaty interpretation to yield a meaning capable of being applied in daily life).

¹⁰⁹ Cf 'context sensitive interpretation'. Id, 40-48, citing also Martti Koskenneimi, *From Apology to Utopia: The Structure of International Legal Argument* (Cambridge University Press, 2006) (noting that treaty interpretation must be context-sensitive and hence it must be applicable to the relevant context).

securing digital privacy. Informed by contemporary challenges that digital privacy faces, this thesis explores responsive mechanisms for protecting digital privacy. The proposed institutional reform of creating a multi-stakeholder forum, for instance, would help the UN privacy regime remain adaptive to changing circumstances.

The fourth aspect of the thesis's pragmatic approach is *multi-faceted*. A multi-faceted approach is one that is informed by and builds on components drawn from multiple sources.¹¹⁰ A primary virtue of heterogeneity is that it benefits from insights borrowed from different sources. The thesis broadly reflects eclecticism with elements drawn from a variety of sources, including insights from various areas of law, and scholarship. In examining UN privacy standards, the thesis examines, for example, a broad range of instruments, including relevant human rights treaties and the attendant case law as well as general and domain-specific data privacy instruments. Chapters 3 and 4 examine the legal significance of IBRs and a series of UN Privacy Resolutions. Reform ideas explored in chapters 5 and 6 are also informed by and draw insights from heterogeneous sources.

IV THESIS OUTLINE

The thesis is structured into six substantive chapters. This introductory part provided a background to the thesis, situated the thesis in the relevant literature and outlined its research questions. It further outlined the analytical framework and methodology that guides the study. The remainder of the thesis develops in six chapters, and a conclusion where a summary of the findings is presented.

Chapters 1 and 2 respectively examine the extent to which international human rights law and the UN data privacy framework uphold digital privacy. This provides the backdrop against which the role of emerging international privacy initiatives in reimagining the international law of privacy in the digital age is examined. Chapter 1 argues that the current human right to privacy framework is ill-equipped to uphold digital privacy. It traces the reasons behind its present weak structures to the drafting history of the UDHR and the ICCPR during the Cold War era. In chapter 2, the second important but often overlooked source of international privacy law is examined: the UN data protection framework. The chapter argues that plagued by deep normative fragmentation and the lack of a robust institutional framework, the UN draft framework offers little protection to data privacy. It further locates the causes for the present weak structure of the data privacy framework in the political controversies of Cold War period.

¹¹⁰ Cf 'coherent interpretation'. Id, 28-39, citing also Leanor Soriano, 'A modest Notion of Coherence in Legal Reasoning: A Model for the European Court of Justice' (2003) 16 *Ratio Juris* 296 (noting that the interpretation must draw from the views and expertise of relevant actors and ensure system coherence).

Having explored gaps in existing law, the thesis then proceeds to examine whether, and to what extent, global privacy initiatives contribute in addressing its gaps in chapters 3 and 4. Chapter 3 takes up the first of these initiatives: the IBRs Project. It argues that its progressive vision for privacy notwithstanding, the role of IBRs in reimagining international privacy law is limited by a host of conceptual and practical factors. It then submits that a more promising role for the IBRs Project is 'catalytic' by which it shapes the 'normative direction' of international privacy law reform. Chapter 4 addresses the second initiatives: the ongoing UN privacy discourse. It investigates the extent to which the discourse addresses gaps in international law. The chapter argues that while Resolutions adopted as part of this discourse have little to offer in lessening gaps in the existing regime, they offer the foundation for future reform efforts.

Having examined the state of existing law in chapters 1 and 2 and boundaries of emergent norms in chapters 3 and 4, chapters 5 and 6 argue for a pragmatic approach to international privacy law. In chapter 5, it is argued that an international (soft) law is needed to address normative gaps in existing law, to globalize emergent privacy norms and further facilitate progressive development of privacy law in the digital age. In that sense, the proposed soft law would fulfil functions of Reed's imaginary 'successful law' – alluded to in the epigraph – in entrenching existing norms while clarifying ambiguities *and* reinforcing developing norms. Chapter 6 considers virtues of a dialogical approach in addressing some of the pressing institutional gaps in present international law of privacy. It explores virtues of installing a multi-stakeholder privacy forum as a way of building consensus and facilitating cooperation among key actors on current and emerging privacy challenges.

The final part of the thesis presents a summary of findings, contributions of the thesis and highlight areas for further research. A key finding of the thesis is that addressing the 'privacy problem' in the digital age through international law must critically embrace global privacy initiatives but be grounded on a pragmatic approach. Such an approach should not only draw upon emergent norms but also build on the existing legal and institutional framework.

Looking to the future, this part of the thesis briefly touches on prospects of ongoing initiatives, particularly the ongoing UN privacy discourse. While the discourse is still in flux (and hence with no predictable future), its novel approach to corporate human rights obligations presents new a frontier not only to international privacy law but also to the broader UN regime on 'business and human rights'.

**PART I: CONSIDERING INTERNATIONAL LAW OF
PRIVACY IN THE DIGITAL AGE**

CHAPTER 1 — DIGITAL PRIVACY AND THE REACH OF INTERNATIONAL HUMAN RIGHTS LAW

I INTRODUCTION

This chapter examines whether, and to what extent, international human rights law is well-equipped to uphold digital privacy. The right to privacy is guaranteed in a number of international human rights instruments. The primary sources of privacy rights are the UDHR and the ICCPR which guarantee the right to privacy in an almost identical manner.¹¹¹ The right to privacy is also guaranteed in other specialized UN instruments such as the Convention on the Rights of the Child (CRC), the Convention on the Rights of Persons with Disabilities (CRPD) and the International Convention on the Rights of Migrant Workers and Members of their Families (ICRMW).¹¹² The chapter investigates the scope of right to privacy in these instruments, and the accompanying jurisprudence, to show whether international human rights law is fit for purpose in the digital age. It finds that current international human rights law provides weak protection for digital privacy.

As shall be shown in this chapter, the human right to privacy in international law is formulated in ambiguous and high-level abstract principles, thereby making its scope uncertain. The poor formulation of the right to privacy is exacerbated by the lack of a robust and dynamic institutional machinery. The monitoring of the right to privacy is left to a Committee of experts that operates on a part-time basis, and for a short duration. These factors have cumulatively led to a stagnation in the development of a privacy jurisprudence that responds to the threats present in the digital environment. The chapter further uncovers that the present weak structures of the right to privacy in international human rights have some historical antecedents. It locates the root causes of these gaps in the controversies of the Cold War period and the apparently little attention paid to the right to privacy during the drafting of earlier human rights accords. A vaguely crafted privacy provision in the hastily adopted UDHR was simply replicated in the ICCPR, and other subsequent treaties, without any improvement of form or substance.

In undertaking a regime analysis, the chapter seeks to provide a background against which the roles of emerging international privacy initiatives are considered in chapters 3 and 4. The examination reveals where gaps lie in existing law that may be

¹¹¹ UDHR, above n 1, art 12; ICCPR, above n 1, art 17.

¹¹² *Convention on the Rights of the Child*, opened for signature 20 November 1989, 1577 UTS 3 (entered into force 2 September 1990) art 16; *Convention on the Rights of Persons with Disabilities*, opened for signature 30 March 2007, 2515 UNTS 3 (entered into force 3 May 2008) arts 22-23; *International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families*, opened for signature 18 December 1990, 2220 UNTS 3 (entered into force 1 July 2003) art 14.

addressed by these initiatives. The chapter concludes that despite the ambivalence at the UN whether existing privacy standards are adequate – exhibited in the ongoing UN privacy discourse – international human rights law acutely needs some form of reform, and emerging initiatives offer an alternate way forward.

II BACKGROUND TO THE RIGHT TO PRIVACY IN INTERNATIONAL LAW

A look back at the history of the negotiation, drafting and adoption of the UDHR and ICCPR in general and their privacy provisions in particular offers useful insight regarding the current structure of the right to privacy in international law. This section discusses two major issues that left significant marks in the present structure of the human right to privacy: (a) the impact of political and ideological divisions that clouded the gestation of the right and (b) the possible impact of drafting missteps, or inattention, of the privacy provisions in the present normative and institutional structures.

A The Cold War Effect

The end of the Second World War undoubtedly was a watershed moment particularly in leading to the revival of an interest in international cooperation to prevent similar devastating wars.¹¹³ But the post-war period during which the UDHR was drafted and particularly the Cold War period during which most of the work on the ICCPR was carried out were largely periods of deep political and ideological divisions.¹¹⁴ Major multilateral efforts in the human rights field would not move far enough unless significant political compromises were struck to meet the demands of each side of the political spectrum. As this section illustrates, these compromises are reflected in at least two defining features of the current international human rights regime: treaty monitoring and formulation of human rights, including the right to privacy.¹¹⁵

1 Softer Monitoring Mechanisms

With a view to enlist as many States as possible, it was imperative to introduce softer systems of human rights monitoring.¹¹⁶ States were opposed to a regime that posits strong international monitoring machinery.¹¹⁷ The UN Charter's cardinal principle of

¹¹³ See William Edmundson, *An Introduction to Rights* (Cambridge University Press, 2004) 105.

¹¹⁴ See Christopher Roberts, *The Contentious History of the International Bill of Human Rights* (Cambridge University Press, 2014) 66-71.

¹¹⁵ See Henry Steiner, 'Individual Claims in A World of Massive Violations: What Role for the Human Rights Committee?' in Philip Alston and James Crawford (eds), *The Future of the UN Human Rights Treaty Monitoring* (Cambridge University Press, 2000) 17, 22.

¹¹⁶ *Ibid.*, 19-23.

¹¹⁷ See Boutros Boutros-Ghali, 'Introduction' in *United Nations and Human Rights (1945-1995)* (United Nations Blue Book, 1995) 46.

non-intervention in matters of domestic jurisdiction particularly played out strongly in this regard.¹¹⁸ The current human rights regime is, as a result, premised on the recognition of peaceful co-existence of divergent polities and respect for the national sovereignty of States.¹¹⁹ Indeed, as Forsythe writes, even before the idea of the UDHR surfaced, the superpowers were not keen on international human rights at the start of the San Francisco Conference in 1945.¹²⁰

An indication for the lack of interest in stronger monitoring under the ICCPR is that the individual communications procedure was strongly resisted by State parties.¹²¹ The procedure was pushed to the eleventh hour during the negotiation, and finally tucked away in an Optional Protocol. The issue of international monitoring had, of course, been controversial from the outset of drafting universal instruments in general. The UNGA, for instance, had considered the idea of introducing a 'right to petition' into the then draft UDHR but later abandoned so that it could be addressed under the forthcoming Covenants.¹²² The former Commission on Human Rights also had reportedly resisted the pressure from the UNGA to introduce an individual petitioning procedure.¹²³ Instead, in 1956 the Commission installed – in response to pressures from the UN Economic and Social Council – a softer reporting procedure based on the UDHR but was terminated later because it brought little results.¹²⁴ Similar complaint procedures introduced in 1967 and 1970, which respectively allowed individual and group petitions on 'gross patterns of gross violations', were rescinded for lack of success.¹²⁵

The Commission's resistance was, however, merely a reflection of the wishes of States. This is because the Commission, which was an inter-governmental body, had solicited views of States on possible 'international supervision and complaints monitoring mechanisms' as well as the propriety of a global human rights court

¹¹⁸ See *Charter of the United Nations* (1945) art 2(7).

¹¹⁹ See Yogesh Tyagi, *The Human Rights Committee: Practice and Procedure* (Cambridge University Press, 2011) 38-41.

¹²⁰ David Forsythe, 'The United Nations and Human Rights: 1945-1985' (1985) 100 *Political Science Quarterly* 249, 251.

¹²¹ See Boutros-Ghali, above n 117, 46.

¹²² *Right to Petition*, GA Res 217 B(III), UNGAOR, 3rdsess, 183rdplen mtg, UN Doc A/810 (10 December 1948); see also John Humphrey, 'The International Bill of Rights: Scope and Implementation' (1976) 17 *William and Mary Law Review* 527, 536, 540.

¹²³ See Vratislav Rechota, 'The Development of the Covenant on Civil and Political Rights' in Louis Henkin (ed), *The International Bill of Rights: The Covenant on Civil and Political Rights* (Columbia University Press, 1981) 48-49.

¹²⁴ See Philip Alston, 'The Commission on Human Rights' in Philip Alston (ed), *The United Nations and Human Rights: A Critical Appraisal* (Oxford University Press, 1992) 183-184; see also Tom Farer and Felice Gaer, 'The UN and Human Rights: At the End of the Beginning' in Adam Roberts and Benedict Kingsbury (eds), *United Nations, Divided World: The UN's Roles in International Relations* (Clarendon Press, 2nd ed, 1993) 273.

¹²⁵ See Antonio Cassese, *International Law in a Divided World* (Clarendon Press, 1986) 304-305.

during the drafting of the ICCPR.¹²⁶ But States' lack of political will to be subjected to international supervision had led to proposals based on compromises. The monitoring of the ICCPR ultimately fell in the hands of 18 part-time experts with largely advisory roles. The present monitoring system essentially is a cooperative framework rather than adversarial and relies on the good faith of State parties.¹²⁷ The individual communications procedure, which is relegated to an optional instrument, has unsurprisingly garnered relatively lower ratification by State parties.¹²⁸ This, in practice, meant that notorious violators of privacy rights such as the US have not ratified the Protocol.

But this politically-induced weak system of monitoring has had a more nuanced ramification to the present structures of international law of privacy. As the analysis below will show, the right to privacy provisions in international human rights law are framed in an exceedingly vague manner. But, because Cold War politics created a softer monitoring mechanism, this normative obfuscation could not be addressed by powerless treaty bodies. Hampered by structural problems, the HR Committee, for instance, has not been able to develop a robust privacy jurisprudence.

2 Vague Formulation of Rights

Terminological vagueness is the second area where the influence of political compromises is strongly felt. Human rights are, of course, often framed in vague terms and deliberately so with a view to leave room for the technical details and exceptions to be determined by State parties.¹²⁹ Such deferrals would permit accommodating socio-economic, cultural, political and religious divergences among nation-states. This approach had particularly animated the drafting of the UDHR's privacy provision whose speedy adoption generally was made possible because it couches rights in 'general principles'.¹³⁰ As will be shown further below, vagueness of the privacy provision is more acute than other rights in the ICCPR. The almost identical right to privacy provision of the Covenant was also quickly adopted because, as reportedly noted by the Philippine delegate, there was already

¹²⁶ See Hersch Lauterpacht, *International Law and Human Rights* (Stevens and Sons Limited, 1950) 278.

¹²⁷ See Jack Donnelly, 'International Human Rights: A Regime Analysis' (1986) 40 *International Organization* 599, 609-610; see also Makau Mutua, 'Looking Past the Human Rights Committee: An Argument for De-Marginalizing Enforcement' (1998) 4 *Buffalo Human Rights Law Review* 211, 216.

¹²⁸ See Eric Posner, *The Twilight of Human Rights Law* (Oxford University Press, 2014) 96.

¹²⁹ At the time of writing, the Optional Protocol has been ratified only by 116 States, compared to 172 ratifications of the ICCPR. This, of course, holds true also for the Optional Protocols to the other UN treaties that guarantee the right to privacy such as the CRPD the Optional Protocol of which has merely 94 State parties and the CRC's Optional Protocol which has only 44 State parties. See <<http://indicators.ohchr.org/>>

¹²⁹ See Oliver Diggelmann and Maria Cleis, 'How the Right to Privacy Become a Human Right' (2014) 14 *Human Rights Law Review* 441, 451.

¹³⁰ *Ibid*, 443-444.

agreement on the general principles involved.¹³¹ Indeed, it was already acknowledged at the 9th session of the Covenant's drafting Committee in 1957 that translating the 'general principles' articulated under Article 12 of the UDHR into precise legal terms is difficult.¹³²

This reveals two important points in understanding the present structure of the human right to privacy in international human rights law. One is that it was known from the very start that the privacy provision was 'general' (and perhaps made so deliberately). Secondly, its replication under the ICCPR is partly because the drafters were not sure how best to put the right in a less generic manner. The ultimate reproduction into the ICCPR without any significant change might also speak more about the level of importance the drafters had attached to the right to privacy. This also runs counter to what drafters of the UDHR had hoped. In writing before the drafting of the ICCPR began, Malik – one of the drafters of the UDHR – had noted that the then impending Covenant would 'define with a greater degree of legal precision at least some of the rights proclaimed in the Declaration'.¹³³

A closer look at the drafting history of the ICCPR sheds more light onto the present terminological make-up of the privacy provision. As the UN set out to translate the UDHR into binding treaties, there were two competing proposals on the form and content of these upcoming instruments. The first proposal favoured the drafting of a general human instrument and then the particulars would be addressed through subsequent specific instruments.¹³⁴ The second view, which vied for a rather detailed instrument, maintained that a general instrument would be a mere replication of the UDHR.¹³⁵ Doubtless, the first view is reflected in the current version of the ICCPR's privacy provision, which is a sheer replication of Article 12 of the UDHR. The truncated nature of the privacy provisions of both the UDHR and the ICCPR, framed in high-level abstract principles, is significant. Significant because it raises the central question of whether such principles must be seen as 'carved in stone' – and continuing to apply across changing times. Could a right crafted with the post-war 20th century in mind be fit for purpose to the new realities of the digital age?

The fact that post-ICCPR human instruments, as shall be noted later, appear to respond to technological developments suggests that the aim, while crafting the UDHR (and essentially the ICCPR), might have been more than articulating eternal general principles. One also traces interest among drafters of the Covenant in crafting the right to privacy based on the conditions of the day. An example is that an Israeli delegate had suggested including protection of 'telegraphic and telephonic

¹³¹ Ibid, 451.

¹³² See Marc Bossuyt, *Guide to the "Travaux Préparatoires" of the International Covenant on Civil and Political Rights* (Martinus Nijhoff Publishers, 1987) 339.

¹³³ Charles Malik, 'Human Rights in the United Nations' (1951) 6 *International Journal* 275, 278.

¹³⁴ See Boutros-Ghali, above n 117, 44.

¹³⁵ Ibid.

communications’ under Article 17 as these were common media of communication at the time.¹³⁶ This lends weight to the argument that the present human rights standards needed reforms based on the new realities of the digital age.¹³⁷ The now prevalent proposals for a new set of human rights for the digital age in the form of IBRs or international data privacy treaty proceed from the assumption that the digital age dictates new human rights norms or major translation and adaptation in the context of the digital environment. That is, in today’s world of digital connectivity they suppose the need for something beyond the evolution of a ‘living document’.

In sum, the present weak structure of the UN framework on the human right to privacy is partly a result of Cold War politics. Deep ideological divisions that clouded the climate under which the Covenant was drafted forced the use of terms that would intrude as little as possible into the sovereign rights of Cold War foes.

B The Privacy Inattention Effect

The UDHR and the ICCPR’s general propensity to vague language is mainly attributable, as discussed above, to the deliberate decision of its drafters to reflect the political compromises of the time. But that is not the complete story. The right to privacy provision of the Covenant, and the other UN human rights treaties that reproduce the right, has been particularly affected by drafting inattention. This can best be illustrated by, first, looking at the account of drafters and secondly, by simply comparing the text of privacy provisions with other rights in the ICCPR. The right to privacy has not received as much attention during the drafting as other rights that found relatively clear formulation in the Covenant.

One finds useful insights on this point from the account of figures who played key roles during the drafting of the UDHR. Malik’s account, for instance, reveals that not only the drafting exercise was plagued by urgency but also that themes that received significant discussion during the drafting of the UDHR did not include the right to privacy. Instead, rights that had received attention were the right to life, rights of the accused, right to freedom of religion and the right to free speech particularly the conditions under which they may be limited.¹³⁸ This suggests that the right to

¹³⁶ See Diggelmann and Cleis, above n 129, 450, footnote 56.

¹³⁷ Indeed, the former UN Secretary-General had conceded that the UDHR indeed entails ‘some gaps’ and that it touches only peripherally certain human rights problems particularly those caused by ‘scientific and technical developments’. See Boutros-Ghali, above n 117, 27.

¹³⁸ Charles Malik, ‘Human Rights in the United Nations with Text of Draft Covenants’ (1952) 1 *United Nations at Work* 1, 12; see also Megan Richardson, *The Right to Privacy: Origins and Influence of a Nineteenth Century Idea* (Cambridge University Press, 2017) 113 (noting the little discussion about the inclusion of the right to privacy during the drafting).

privacy, let alone possible restriction clauses, had received little attention during the drafting of the UDHR.

Malik further wrote:

[...] the archetype of what we were trying to ensure was freedom from discrimination and from arbitrary arrest, and freedom of religion and speech. It never occurred to us that anything else was as important as these.¹³⁹

He further added that when the emphasis shifted, it shifted towards socio-economic and cultural rights.¹⁴⁰ Arguably, the neglect shown towards the right to privacy has affected the way how the provision was formulated in the UDHR. This point finds support in the admission of another important figure, Humphrey, who at the time was Director of the UN Human Rights Division and more importantly, one who compiled the initial draft of the UDHR. Humphrey wrote:

[...] some of the rights would have been enunciated differently had the Declaration been prepared by learned legal draftsmen; and it is possible that its style might have been improved [...].¹⁴¹

This is an important insight when one considers the fact that UDHR's privacy provision was simply replicated later (almost) verbatim into the ICCPR.

Beyond these insights and admissions, sheer textual comparison of the right to privacy and other Covenant rights speak volumes about the 'privacy inattention effect'. Covenant rights such as freedom of religion, expression and association are far better formulated than the right to privacy. These rights are stipulated in more direct and elaborate manner particularly in terms of the grounds under which restrictions apply.¹⁴² This is in contrast with the omission of a limitation clause from the privacy provision of the ICCPR. Imprecise terms such as 'arbitrary' are also not attached to these rights thereby avoiding potential difficulties in interpretation. In the context of the right to freedom of expression for instance, there was also reportedly thorough discussion on the substance of the right to freedom of expression including on the linguistic details among members of the drafting committee.¹⁴³ This strengthens the claim that Article 17 of the ICCPR was

¹³⁹ Ibid.

¹⁴⁰ Ibid.

¹⁴¹ John Humphrey, 'The Universal Declaration of Human Rights' (1949) 4 *International Journal* 351, 355-356.

¹⁴² ICCPR, above n 1, arts 18-21.

¹⁴³ See Molly Land, 'Toward International Internet Law' (2013) 54 *Harvard International Law Journal* 394, 418-421.

haphazardly crafted, and the drafters seemingly attached little importance to the right to privacy.¹⁴⁴

As noted above, the drafting Committee merely replicated Article 12 of the UDHR into the ICCPR because there was already agreement on the principles. No such replication, however, occurred when other rights of the Covenant were drafted. Like the right to privacy, the rights to freedom of speech, religion and association were formulated in understandably 'general principles' under the UDHR.¹⁴⁵ But these principles were later translated into fairly elaborate rights under the ICCPR. Consider Art 19 of the UDHR which reads as follows:

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

This general proviso was later translated into a fairly elaborate provision Art 19 of the ICCPR, with a fully-fledged limitation clause.

This illustrates not just the compromise-induced vagueness but also, perhaps mainly, inattention during the drafting Article 17 of the ICCPR. What makes this more unfortunate is that the Covenant merely replicated Article 12 of the UDHR, the drafting of which also had exhibited some element of haste. Due to ideological impasse of the time, the former Commission on Human Rights had reportedly pushed for the Declaration to be adopted as quickly as possible.¹⁴⁶ The Commission had even rejected requests by some delegates to postpone the adoption of the Declaration to the following year so that it could be examined more closely.¹⁴⁷ This later led to eight abstentions from some of these delegates. In considering the fact that these abstentions were made mainly by countries from the 'Eastern' bloc led by Russia,¹⁴⁸ one might arguably state that problems of 'ideological divisions' and 'haphazard drafting' fed each other in producing the current normative structure of the right to privacy. Along similar lines, there was a concern during the drafting of the UDHR that the Declaration might not achieve meaningful consensus, and that modest goals be pursued instead.¹⁴⁹

In summary, the present normative and institutional structures on the right to privacy are negatively affected by two factors. These are ideological divisions that

¹⁴⁴ Of a similar view, Diggelmann and Cleis, above n 129, 457.

¹⁴⁵ UDHR, above n 1, arts 18-20.

¹⁴⁶ See Farer and Gaer, above n 124, 248-249.

¹⁴⁷ Ibid.

¹⁴⁸ See Johannes Morsink, *The Universal Declaration of Human Rights: Origins, Drafting and Intent* (University of Pennsylvania Press, 1999) 21-24.

¹⁴⁹ See Benedetto Croce, 'The Rights of Man and the Present Historical Situation' in *Human Rights: Comments and Interpretations* (Columbia University Press, 1949) 93-95.

dictated political compromises and an element of haphazard drafting of the relevant human rights treaties in general and the right to privacy provisions in particular. These two factors have resulted in a normatively vague right to privacy rules and an institutionally weak regime that cumulatively hampered the development of a robust jurisprudence on the right to digital privacy. The next section examines these normative, institutional and jurisprudential weaknesses of the international regime for the protection of digital privacy.

III WITHOUT “BLIND SPOTS”? LIMITS OF THE (INTERNATIONAL) HUMAN RIGHT TO PRIVACY FRAMEWORK IN THE DIGITAL AGE

The present UN framework on the right to privacy exhibits three major gaps: normative, institutional and jurisprudential dearth. Building on above historical context, and comparative law, this section demonstrates how these gaps have made the international law of privacy ill-equipped in securing digital privacy.

A Normative Gaps

Normative limitations of the present regime relate mainly to two major issues. The primary limitation concerns the vague manner in which the right to privacy is formulated in UN human rights instruments. Terminological and conceptual vagueness inherent in existing privacy norms obscures the scope of the right, and as a result, hinders proper implementation of the right. The second limitation relates to the lack of clear and strong normative standards regarding the human rights responsibilities/obligations of Internet corporations vis-à-vis right to digital privacy. What follows considers these two normative limitations of international human rights law.

1 Problems of Scope

As already highlighted, the right to privacy in existing international human rights instruments is framed in an exceedingly vague language. This has made it difficult to ascertain the scope and content of the right. Article 12 of the UDHR, for instance, reads as follows:

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 the protection of the law against such interference or attacks.

This provision basically replicates Article 12 of the UDHR, except that the term ‘unlawful’ is introduced to the privacy provision right next to ‘arbitrary’, and at the

limb of the provision that protects ‘honour’ and ‘reputation’.¹⁵⁰ The manner in which the right to privacy is formulated under the ICCPR – and other subsequent UN human rights instruments for that matter – raises three issues of scope. This section considers these three issues of scope, along with the rather broader issue surrounding the extraterritorial scope of Art 17 ICCPR.

(a) (De)coupling Privacy and Reputation

The present terminological make-up of Article 17 ICCPR – and privacy provisions of the CRPD, ICRMW and CRC – indicates that the provision is more than a privacy provision.¹⁵¹ Art 17 of the ICCPR, for instance, reads as follows:

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.

This provision guarantees the right to privacy both in its ‘negative’ [Art 17(1)] and ‘positive’ [Art 17(2)] dimensions. While the former requires States to ‘respect’ the right to privacy of individuals, the latter imposes an obligation to ‘protect’ against violation by private actors. It is, however, vital to note that this provision protects a bundle of interests. In addition to privacy, it protects two broad set of interests: ‘reputation’ and ‘honour’. This has, in turn, created confusion as to the possible link between the right to privacy on the one hand and reputation or honour on the other. A look back at the drafting history of the Covenant offers little but one learns from background documents of the UDHR that the nexus between privacy and reputation/honour was a topic of some discussion.¹⁵² But the debate was primarily about whether the inclusion of reputation/honour into the privacy provision might affect the protection of free speech.¹⁵³ Michael reports that there was indeed a discussion at the UNGA’s Third Committee regarding the inclusion of ‘reputation and honour’ in Article 17 of the ICCPR but offers no further details.¹⁵⁴

The HR Committee, the treaty body that monitors the ICCPR, sends mixed signals in its GC 16 regarding the possible link between privacy and reputation/honour. The

¹⁵⁰ ICCPR, above n 1, art 17.

¹⁵¹ Cf Myres McDougal et al, ‘Aggregate Interest in Shared Respect and Human Rights: The Harmonization of Public Order and Civic Order’ (1977) 23 *New York Law School Law Review* 183, 229 (stating that Art 12 of the UDHR is ‘broader than the technical concept of privacy and pregnant with potentiality for further expansion’).

¹⁵² See Lars Rehov, ‘Article 12’ in Asbjorn Eide et al (eds), *The Universal Declaration of Human Rights: A Commentary* (Scandinavian University Press, 1992) 188-189.

¹⁵³ Ibid.

¹⁵⁴ James Michael, *Privacy and Human Rights: An International and Comparative Study with Special Reference to Developments in Information Technology* (Dartmouth, 1994) 21.

very heading of the GC, titled ‘right to privacy’, suggests that Article 17 is a solely privacy provision, and by extension, reputation/honour is not, as such, a privacy interest. But the GC’s paragraph on ‘reputation and honour’ appears to suggest otherwise, as it presents the latter as distinct interests.¹⁵⁵ The Committee’s GC 31 further hints that Article 17 comprises ‘privacy-related’ guarantees but offers no clarification on how these interests, assuming these include honour and reputation, relate to privacy.¹⁵⁶ The Committee’s GC on Freedom of Expression provision of the ICCPR, where ‘reputation’ is one ground of restriction, also does not clarify the meaning of reputation in the context of privacy.¹⁵⁷ In describing the right to privacy only in terms of ‘privacy, family, home and correspondence’, the series of post-Snowden UN Privacy Resolutions suggest that Article 17 of the ICCPR is solely a privacy provision. And, as such reputation and honour have little to do with privacy. A more recent report of the SRP adds to the confusion in vaguely stating that the ‘right to protection of reputation’ under Article 12 of the UDHR and Article 17 of the ICCPR is ‘distinct from yet akin to privacy’.¹⁵⁸

So, whether privacy has any conceptual link with reputation/honour is unclear. Doubtless, reputation/honour are, as Griffin rightly notes, matters of legitimate interest but relate rather to the law of defamation.¹⁵⁹ Even where reputation and honour are worthy of protection as fundamental rights, it is not clear why they are lumped together with privacy. Furthermore, given the fact that Art 19(3)(a) of the Covenant mentions ‘respect of the rights or reputation of others’ as one legitimate ground for the restriction of the right to free speech, inclusion of reputation within the privacy provision might be seen as a redundancy.¹⁶⁰ But again, a strict reading of Art 19(3)(a) – especially the disjunctive ‘or’ – could also lend an argument that even the reference to reputation here is not as a right as such. Or, it is not at least conceived as a right recognized under the Covenant or in international human rights law in general.

¹⁵⁵ HR Committee, *General Comment 16: Art 17 (Right to Privacy): 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) [11].

¹⁵⁶ GC 31, above n 33, [8].

¹⁵⁷ HR Committee, *General Comment 34: Art 19: Freedom of Opinion and Expression*, 102nd sess, UN Doc CCPR/C/GC/34 12 (September 2011) [21] [28].

¹⁵⁸ *Report of the Special Rapporteur on the Right to Privacy, Joseph Cannataci*, UN Doc A/HRC/34/60 (24 February 2017) [46(i)].

¹⁵⁹ See James Griffin, *On Human Rights* (Oxford University Press, 2009) 703. [Griffin further notes that provisions stipulating right to reputation/honour are ‘badly drawn’ to the extent that ‘they need interpretation tantamount to redrafting’. Id, 209]. Note also the Tallinn Manual where the International Group of Experts treated ‘protection of defamation’ separately from the right to privacy, see Michael Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) 187.

¹⁶⁰ Of a similar view, see Michael, above n 154, 20.

This viewpoint finds support when one considers how the ECHR, the privacy provision of which was modelled based on Article 12 of the UDHR, treats the matter. Background documents of the ECHR reveal that references to reputation and honour were deliberately excluded from the privacy provision and ultimately taken to Art 10 as an exception to the right to freedom of expression.¹⁶¹ One account holds that the deliberate exclusion by the drafters was mainly due to the ‘vagueness’ of the terms.¹⁶² In elaborating the drafting Committee’s approach in transposing the UDHR into the Convention, a member of the Committee noted that the approach pursued was not to ‘refer to all the provisions of the article in question but only to those specifying the content of the freedom’.¹⁶³ Moreover, while the ECtHR has considered ‘reputation’ claims under Article 8 of the ECHR in some cases, it has definitively ruled that ‘reputation’ and ‘private life’ are conceptually distinct.¹⁶⁴ Even for cases that implicate ‘reputation’ to be considered under the right to private life, the Court has set a higher threshold of seriousness, i.e. the harm to reputation must be one capable of causing prejudice to private life.

(b) Privacy and Its Zones of Protection

The right to privacy provisions of UN human rights treaties are couched in a manner that appears to detach the umbrella term ‘privacy’ from specific zones or grounds of protection – i.e. ‘family’, ‘home’ and ‘correspondence’ – that it normally embraces. The way the provisions are formulated gives the impression that these terms are not covered under the umbrella term ‘privacy’. This has been a source of confusion, and has been a subject of differing interpretations, including by the HR Committee. In an unprecedented interpretation, the Committee, for instance, has applied the term ‘home’ to cover tenancy rights.¹⁶⁵ A more recent decision similarly held that eviction from one’s home engages Article 17 because the measure presents a risk of homelessness.¹⁶⁶ GC 16 does not provide any clarification beyond stating that the term ‘home’ is to be understood to cover the place where ‘a person resides or carries out his usual occupation’.

¹⁶¹ See Tanya Alpin and Jason Bosland, ‘The Uncertain Landscape of Article 8 of the ECHR: The Protection of Reputation as a Fundamental Rights?’ in Andrew Kenyon (ed), *Comparative Defamation and Privacy Law* (Cambridge University Press, 2016) 265.

¹⁶² See Gloria Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer, 2014) 38, citing Carlos Ruiz, *La Configuración Constitucional del Derecho a la Intimidad* (1992) 99.

¹⁶³ Quoted in Jacques Velu, ‘The European Convention on Human Rights and the Right to Respect for Private Life, The Home and Communications’ in Arthur Robertson (ed), *Privacy and Human Rights* (Manchester University Press, 1973) 15-16.

¹⁶⁴ See *Karako v Hungary* (ECtHR, Application No. 39311/05, 28 April 2009) [22-13].

¹⁶⁵ See, e.g., HR Committee, *Dušan Vojnović v Croatia* (Communication No. 1510/2006, 30 March 2009).

¹⁶⁶ See HR Committee, *Kalamiotis et al v Greece* (Communication No. 2242/2013, 3 January 2017) [12.4] [12.8]

Such exceedingly broad interpretations of ‘home’ appear to be influenced by the case law of the ECtHR, which has long addressed similar cases under Article 8 of the Convention.¹⁶⁷ Perhaps in cognizance of this overstretched approach, the Court routinely reminds that there is nevertheless no right to be provided with a home/housing under Article 8. But, even this caveat raises a question. If there is no right to be provided home – i.e. a positive right to home, it is impliedly recognizing a ‘negative’ right to home. A right not to be evicted from one’s home technically would mean a negative freedom of home. To be sure, the Court has on several occasions entertained cases relating to search and seizure under Article 8, which concern the classic right to the privacy of home.¹⁶⁸

The term ‘family’ has also been interpreted by the Committee broadly to include family rights such as the right of foreigners not to be separated from their families by an expulsion order under immigration regulations.¹⁶⁹ But this interpretation is well beyond the usual understanding of privacy. The Committee’s GC 16 has not adequately clarified the meaning of these terms either. It simply provides that the term ‘family’ must be given broad interpretation to include ‘all comprising family as understood in the society of the State party concerned’.¹⁷⁰ Like in case of ‘home’, the approach of the Committee might have been influenced by the case law of the ECtHR. The Court has on numerous occasions treated cases involving expulsion orders under the ‘family life’ proviso of Article 8, although a separate ‘right to family’ is guaranteed under Article 12 of the Convention.¹⁷¹ The Court treats Article 12 as a *lex specialis*, and proceeds to consider a case under Article 12 only when it finds no violation under Article 8.¹⁷² The Committee has also increasingly adopted a similar approach of applying ICCPR’s Article 23 on right to marry/family alongside Article 17 in matters that relate to ‘family life’.¹⁷³ But it is worth noting that the Court’s now established practice of considering the two provisions together has some precedent. During the drafting of the ECHR, both provisions were considered together, with almost absolute focus to Article 8.¹⁷⁴ This might have influenced the current practice. But whether a similar path should be taken by Committee, without any such justification, is questionable.

¹⁶⁷ See, e.g., *Chapman v The United Kingdom* (ECtHR, Application No. 27238/95, 18 January 2001) [99].

¹⁶⁸ See, e.g., *Rachwalski and Ferenc v Poland* (ECtHR, Application No. 47709/99, 28 July 2009).

¹⁶⁹ See, e.g., HR Committee, *Al-Gertani v Bosnia and Herzegovina* (Communication No. 1955/2010, 6 November 2013).

¹⁷⁰ See GC 16, above n 155, [5].

¹⁷¹ See, e.g., *Uner v The Netherlands* (ECtHR, Application No. 46410/99, 18 October 2006).

¹⁷² *Hamalainen v Finland* (ECtHR, Application No. 37359/09, 16 July 2014) [96].

¹⁷³ See, e.g., HR Committee, *D.T. v Canada* (Communication No. 2081/2011, 29 September 2016); see also Sarah Joseph and Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Materials and Commentary* (Oxford University Press, 3rd ed., 2013) [16.24].

¹⁷⁴ See William Schabas, *The European Convention on Human Rights: A Commentary* (Oxford University Press, 2015) 582-584.

Scholarly interpretations are also divergent, reflecting the general confusion about the present makeup of the provision. Volio, for instance, writes that Article 17 of the ICCPR protects both ‘privacy and the family, home, correspondence, honour and reputation’.¹⁷⁵ Another instance of the confusion is that mere reference to the term ‘family’ under Article 17, a provision mainly addressing privacy, led to the assumption that it relates to the right to form a family, a right separately guaranteed under Article 23 of the Covenant.¹⁷⁶ Kalin and Kunzli write that Article 17 protects ‘the right to live together within a family’. This view sees Article 23 as a mere supplement to Article 17 of the Covenant. Sartor notes rightly that Article 17 of the ICCPR embodies a ‘cluster of rights’ but wrongly suggests that the right to privacy stands in this cluster distinctly than the others such as the right to correspondence.¹⁷⁷

Nevertheless, it appears to be the case that references to ‘privacy’, ‘home’, ‘family’ or ‘correspondence’ aim to cover zones of privacy protection rather than to provide for individuated distinct rights to privacy, home, family *and* correspondence.¹⁷⁸ The ‘home’, ‘family’ and ‘correspondence’ must be seen as spheres of privacy protection – or ‘institutional structures’ as Nowak calls them.¹⁷⁹ When one refers to these terms within the context of privacy, they designate privacy of home, family and correspondence. As such, no distinct protection exists for these zones of privacy protection. The term home under Article 17, for instance, does not protect the right to home for two plain reasons. One is that the right to housing is far removed from privacy interests, and second such right is protected under the International Covenant on Economic, Social and Cultural Rights (ICESCR) [Art 11], and the UDHR (Art 25). In one isolated occasion, a case concerning eviction, the HR Committee ironically held that the sanctioned eviction interfered with the author’s ‘right to the privacy of his home’.¹⁸⁰

With increasing migration of people’s personal lives to the digital space, privacy protection of the home must extend to these new spheres. Traditional privacy protection of individuals’ personal effects in their homes must now cover aspects of personal effects now situated in digitalized accounts. This is also in accord with emerging initiatives such as IBRs, considered in chapter 3, that embody a right to the

¹⁷⁵ See Fernando Volio, ‘Legal Personality, Privacy and the Family’ in Henkin (ed), above n 123, 192.

¹⁷⁶ See Walter Kalin and JorgKunzli, *The Law of International Human Rights Protection* (Oxford University Press, 2009) 14.

¹⁷⁷ See Giovanni Sartor, ‘Human Rights and Information Technologies’ in Roger Brownsword et al (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press, 2017) 440.

¹⁷⁸ Of a similar view see, ‘Privacy in the Digital Age: A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights’ (ACLU, March 2014) 32.

¹⁷⁹ See Manfred Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary* (NP Engel, 2005) 378. For a similar holding, in the context of ‘correspondence’, see Tallinn Manual 2.0, above n 159, 189, footnote 417.

¹⁸⁰ HR Committee, *Petr Gatilov v Russia* (Communication No. 2171/2012, 30 August 2017) [9.4].

‘inviolability of electronic systems, devices and domiciles’.¹⁸¹ As Nowak notes, the right to privacy of home under Article 17 covers a broad range of interests including protection against ‘forced or clandestine trespassing’ as well as ‘digital surveillance’ through listening devices and hidden camera.¹⁸² The increasing reliance on cloud computing services has made the cloud a ‘digital home’, worthy of protection under Article 17.¹⁸³

The same is true with the term ‘family’ which, in several cases, has been applied to protect the right to family life. It is to be noted that none of UN human rights treaties that embody the right to privacy contain the term ‘family life’, except the CRPD. And when the CRPD refers to ‘family life’, which is explicitly mentioned in Article 8 of ECHR, it refers explicitly to the right to marry and form a family.¹⁸⁴ But, the right to family is recognized under Article 23 of the Covenant, and under Article 10 (1) of the ICESCR. In that sense, the meaning of the term ‘family’ within the privacy provision should be different from the ‘right to marry and form a family’. A more appropriate construction of the term – in the context of digital privacy – should be right to privacy of family life. In the present realities of the Internet, family lives of individuals are represented in the digital sphere, and equally merit protection under Article 17.

It is more straightforward with respect to ‘correspondence’ in the digital context. It essentially concerns secrecy of digital communications although it initially was meant for ‘written letters’.¹⁸⁵ The term ‘correspondence’ must also be understood in the context of the right to privacy of correspondence. Similar understanding must be extended to these terms in the context of digital communications. The Committee is yet to examine cases that directly concern privacy of correspondence in the digital context. But it remains to be seen to what extent the case law of the ECtHR would inform its decisions. This is because the Court has made a number of decisions that read a far-reaching ‘right to respect for correspondence’ based on Article 8.¹⁸⁶

But there are reasons to suggest the ill-formulation, and the mis-drafting in between, of privacy vis-à-vis its zones of protection might have been partly a result of drafting and redrafting. A June 1947 draft of the UDHR – the third draft considered by the

¹⁸¹ See *Italian Declaration of Internet Rights* (2015) art 7.

¹⁸² Nowak, above n 179, 400.

¹⁸³ Cf Mark Zuckerberg, ‘A Privacy-Focused Vision for Social Networking’ on Facebook (6 March 2019) <<https://bit.ly/2TmiQWv>> (noting the need for a digital equivalent to the ‘living room’ to protect privacy in social media).

¹⁸⁴ See CRPD, above n 112, art 23(3).

¹⁸⁵ See Nowak, above n 179, 401; see also Tallinn Manual 2.0, above n 159, 189, footnote 417.

¹⁸⁶ See, e.g., *Golder v The United Kingdom* (ECtHR, Application No. 4451/70, 21 February 1975) (See particularly the Separate Opinions of Judges Zeika and Gerald). [The Court held that any measure that impedes someone from initiating correspondence interferes with the ‘right to correspondence’. This far-reaching decision borders the right to free speech, which perhaps embraces spirit of such a right].

drafting Committee – was relatively accurate in its use of the umbrella term privacy. It read:

The privacy of the home and of correspondence and respect for reputation shall be protected by law.¹⁸⁷

This formulation was accurate in applying the umbrella term privacy for the protection of specific zones of privacy protection – i.e. home and correspondence. It had removed term ‘family’ for unknown reason, but it perhaps was because ‘family’ receives protection under another provision of the Declaration (Art 16). Similarly, an earlier draft version of Article 8 of ECHR reflected a more accurate version of the right to privacy: ‘[...] the right to privacy in respect of family, home and correspondence’.¹⁸⁸ One can argue that had these earlier fairly accurate formulations of the right to privacy were adopted, expansive interpretations of the right to privacy would not have ensued.

Overall, the expansive interpretive approach of the ECtHR seems to be influencing the Committee. In addition to reference by the Committee to the case law of the Court, its European members might also bring to the table recipe of the jurisprudence. But the question is whether this is warranted and to what extent. The Court’s expansive interpretation of Article 8 might have grown out of the specific contexts in which the Court operates or the CoE in general. For one, the way in which Article 8 is structured, particularly the terms ‘private and family life’ may have invited a broader interpretive approach. That the Court’s jurisdiction does not embrace socio-economic rights like the right to housing perhaps encouraged an expansive approach. The Court has applied the notion of ‘private life’ in relation to areas that normally fall under other socio-economic rights such as the right to health, right to work and even right to a clean and healthy environment.¹⁸⁹

But when one considers that the Court has addressed issues relating to bodily and psychological integrity, e.g. rape and domestic violence, under the rubric of ‘private life’, one wonders to what extent that such an overly elastic approach should be relied upon by the Committee.¹⁹⁰ The Convention already guarantees a right to

¹⁸⁷ See Mary Glendon, *A World Made New: Eleanor Roosevelt and the Universal Declaration of Human Rights* (Random House, 2001) 283.

¹⁸⁸ See ‘Preparatory Work on Art 8 of the European Convention on Human Rights’ [DH (56) 12, 1956] 6, footnote 2.

¹⁸⁹ For a summary of case law on this, see ‘Guide on Art 8 of the European Convention on Human Rights: Right to Respect for Private and Family’ (CoE, April 2017) 21-22, 24, 26.

¹⁹⁰ Note, though, that the Court’s expansive approach under Art 8 has already attracted widespread criticism. See, e.g., Lord Sumption, ‘The limits of Law’ (27th Sultan Azlan Shah Lecture, Kuala Lumpur, 20 November 2013) 7-8 [noting how the Court ‘went well beyond interpretation, and well beyond the language, object or purpose’ of the ECHR to create ‘new rights’ relating to, inter alia, ‘law of landlord and tenant’ and questions best addressed in a ‘social convention’ out of a ‘perfectly

liberty and security of person, which even the Committee, based on relevant provisions of the ICCPR, interpreted to cover attacks against bodily and psychological integrity.¹⁹¹ The Court also held on many occasions that these four zones of protection are ‘autonomous interests’, privacy being one such interest. The concern with this approach is that the provision would lose one underlying notion that binds various interests together that is privacy.

(c) Privacy and Limitation Clauses

Article 17 of the Covenant does not provide a fully-fledged ‘limitation clause’ that stipulates conditions under which the right could be restricted. The importance of a limitation clause is that it is a key in ascertaining the scope of the right. A vaguely formulated clause opens the door for wider constructions of the conditions where restriction is permissible. The only phrases that could be seen through the lens of ‘limitation clause’ are the terms ‘arbitrary’ and ‘unlawful’. If these were to be solely relied on to assess the legality of certain restrictions, measures that are neither arbitrary nor unlawful would not amount to interference with the right to privacy. But again, the meaning of these terms, particularly the term ‘arbitrary’, is not entirely clear. During the drafting of Article 12 of the UDHR, the term ‘arbitrary’ was controversial – and alternative terms such as ‘unreasonable’ – were suggested by delegates.¹⁹²

The High Commissioner’s 2014 Report on the right to privacy appears to play down the lack of an explicit limitation clause by pointing to the guidance offered by the Siracusa Principles on the meaning of the terms ‘arbitrary’ and unlawful’ under the ICCPR.¹⁹³ The Siracusa Principles, however, provide no guidance on these two notions but provide a rather complex set of interpretive principles relating to limitations.¹⁹⁴ This is, of course, notwithstanding the question of whether these Principles are authoritative enough to warrant reference.¹⁹⁵ Instead, the Committee’s jurisprudence has offered some clarification on the meaning of the term ‘arbitrary’ both under the right to privacy and right to liberty and security of person provisions. But, when it comes to the right to privacy, the Committee has not been consistent in

straightforward provision’ (i.e. Art 8) which was intended to protect ‘private and family life, the privacy of the home and of personal correspondence’].

¹⁹¹ See HR Committee, *General Comment 35: Article 19 (Liberty and Security of Person)*, 112th sess, UN Doc CCPR/C/GC/35 (16 December 2014) [3].

¹⁹² See Morsink, above n 148, 137.

¹⁹³ See *Report of the High Commissioner for Human Rights: The Right to Privacy in the Digital Age*, UN Doc A/HRC/39/29 (30 June 2014) [22].

¹⁹⁴ See ‘Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights’ (American Association for the International Commission of Jurists, 1988) part I.

¹⁹⁵ The Siracusa Principles were not formally adopted by the UN, but the former Commission on Human Rights tacitly endorsed them when, inter alia, it assigned UN symbols and circulated them to member States. See UN Doc E/CN.4/1985/4.

the way in which it interpreted the conditions for restriction. In some instances, it relied upon the organic limitation clauses of 'arbitrary and unlawful',¹⁹⁶ while in many others it applied the less organic three-part tests of legality, legitimate aim and necessity.¹⁹⁷

This lack of coherence meant that the problem of scope remains unresolved. A former UN Special Rapporteur on Human Rights and Counter-terrorism, Scheinin, (creatively) suggested that despite lack of a proper limitation clause under Article 17 of the ICCPR, the terms 'unlawful' and 'arbitrary' fulfil the requirements of the 'in accordance with law' – i.e. legality and 'legitimate aim and/or necessary in a democratic society' respectively.¹⁹⁸ However, some States like the US reject the reliance by the HR Committee of any limitation clauses other than the organic clauses of 'arbitrariness' and 'unlawfulness'.¹⁹⁹ This uncertainty and interpretive inconsistency underlines the need for explicit and authoritative limitation clause that demarcates the scope of the right to privacy.

Background documents indicate that there were initial proposals to incorporate a fully-fledged limitation clause within Article 17 of the ICCPR benchmarked after Article 8(2) of the ECHR.²⁰⁰ The political compromises that clouded the overall drafting of the Covenant led, however, to the rejection of the proposals without much discussion. The US delegation had even proposed a general limitation clause similar to one provided for in Article 29(2) of the UDHR.²⁰¹ The majority held that State parties are best placed to prescribe grounds under which the right to privacy could be restricted based on their unique domestic circumstances.²⁰² This reason behind the rejection of a limitation clause does not, however, fully provide the complete story when one considers that other Covenant provisions were equipped with such a clause. Why would States agree for a limitation clause for the right to assembly, but not for the right to privacy, unless the omission in the latter case was a result of an apparent lack of concern to privacy?

The ICCPR does not also contain a general limitation clause of a kind provided under UDHR which applies to all rights guaranteed under the UDHR. Article 29(2) of the UDHR reads:

¹⁹⁶ See, e.g., HR Committee, *I Elpidia v Greece* (Communication No. 2242/2013, 26 February 2014).

¹⁹⁷ See, e.g., HR Committee, *A.B. v Canada* (Communication No. 2387/2014, 16 March 2017).

¹⁹⁸ See *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, Martin Scheinin, UN Doc A/HRC/13/37 (28 December 2009) [16].

¹⁹⁹ See 'United States Response to OHCHR Questionnaire on the 'Right to Privacy in the Digital Age' (2014) <<https://bit.ly/1FNq6r4>>

²⁰⁰ See Nowak, above n 179, 381-382.

²⁰¹ See Maya Randall, 'The History of the Covenants: Looking Back Half a Century and Beyond' in David Moeckli et al (eds), *Human Rights Covenants At 50: The Past, Present and Future* (Oxford University Press, 2018) 13.

²⁰² Ibid; see also Bossuyt, above n 132, 347.

In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.

While this has partly remedied the lack of a clearer limitation clause within Article 12 of the UDHR, it is not unfortunately repeated in the ICCPR. Although the resistance to including a proper 'limitation clause' within Article 17 of the ICCPR was due to political impasse of the time, the omission of a general limitation clause of a kind found in UDHR is a clear reflection of the haphazard drafting of the provision.

(d) The Extraterritorial Scope of Art 17 ICCPR

The fourth problem of scope relates to the extraterritorial scope of the right to privacy. The question of whether international human rights law in general and the ICCPR in particular apply extraterritorially has been contentious. The issue stems from the ambiguous way in which Art 2 of the ICCPR is framed. Art 2(1) partly reads as follows:

Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant [...]

Some States, particularly the United States, argued that this provision circumscribes the scope of States' human rights obligations to respect and protect the rights of individuals that are within their territory *and* jurisdiction.²⁰³ According to this literal interpretation of the jurisdictional clause, States owe no human rights obligations vis-a-vis individuals outside their geographic borders. In the context of the right to privacy, this reading would mean that States would not be held accountable for unlawful foreign digital surveillance activities.

This interpretation has been rejected by the HR Committee in its case law and concluding observations as well as GC 31.²⁰⁴ In GC 31 adopted in 2004, the Committee held that Covenant rights apply extraterritorially, and States owe an obligation to 'respect and ensure to all persons who may be within their territory and to all persons subject to their jurisdiction'.²⁰⁵ In practice, this means that State

²⁰³ See Marko Milanovic, 'Human Right Treaties and Foreign Surveillance: The Right to Privacy in the Digital Age' (2014) 56 *Harvard International Law Journal* 81, 102-108.

²⁰⁴ See, e.g., GC 31, above n 33; HR Committee, *Sergio Euben Lopez Burgos v Uruguay* (Communication No. R.12/52, 29 July 1981); note also that the ICJ has affirmed the extraterritorial scope of the ICCPR more generally. See, e.g., *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, [2004] ICJ Reports 136.

²⁰⁵ *Ibid*, [10].

obligations extend to anyone within the power or effective control of that State Party, even if not situated within the territory of the State party.²⁰⁶

In the years since the adoption of GC 31, the Committee has consistently affirmed this position in a number of concluding observations. But this primarily concerned the extraterritorial application of Covenant rights in the non-digital context. It was only in the wake of the Snowden revelations that the Committee considered the extraterritoriality of Art 17 in the context of digital communications. In a 2014 concluding observation on the periodic report of the United States, it held that the right to privacy applies extraterritorially, especially when a State party engages in foreign surveillance.²⁰⁷ This position has later found some expression, as shall be noted in chapter 5, in the UN Privacy Resolutions.

Notwithstanding the above affirmations of the HR Committee (and UN Privacy Resolutions), the issue remains controversial. As noted above, the US position on this point relies very much on rigid textual reading of Art 2 of the ICCPR. And, in the absence of political will, the Committee's position is unlikely to resolve the contention. While the US position is now a minority view, it should not be a reason to underestimate the extent of the controversy. This is mainly because of the unique position the US holds in the global Internet governance more broadly, and particularly, in being home to major actors involved in the provision and ownership of Internet infrastructures, products and services.

In part, the non-binding nature of GC 31 (and concluding observations) appears to lend weight to argument that the meaning of a clear provision cannot be altered, and more so, through soft law. This means that apart from political will, the problem of scope regarding Art 17 ICCPR should be addressed through a mechanism that carries higher normative force. As shall be argued in chapter 6, the best way to address this is by codifying the position of the HR Committee as well as other bodies and the growing State practice on the extraterritoriality of the ICCPR — especially the right to privacy — in UNGA Declaration. Such Declaration, while enjoying all the benefits of 'softness', it would place the extraterritoriality scope of Art 17, in the context of digital communications, on a firm legal basis.

2 The Curious Case of (Internet) Corporations

The second major normative gap in the international law of privacy concerns the lack of clear normative guidance on the human rights obligations/responsibilities of technology companies. The primary obligation in human rights law lies on States, and as such non-State actors owe no direct human rights obligations in human rights law.²⁰⁸ It is through the general duty of States to 'protect' that private actors are held

²⁰⁶ Ibid.

²⁰⁷ See *Concluding Observations of the HR Committee: The United States of America* (23 April 2014).

²⁰⁸ See GC 31, above n 33, [8].

to account for human rights infringements. This obligation, as shall be explored in chapter 5 in greater details, involves putting in place the requisite legal and institutional framework to regulate the conduct of private actors. But, the increasing influence that transnational corporations exercise over individuals has raised the question of whether the latter should be held to account directly under human rights law. This is more so in the case of Internet corporations such as Google and Facebook that wield tremendous power over the digital lives of their billions of users.

Recent revelations that mass digital surveillance has been carried out by governments in concert with these Internet businesses cast doubt on whether States could genuinely ensure respect for the right to (digital) privacy by private actors. As highlighted in chapter 1, the lack of a direct human rights obligation of corporations, particularly in the area of privacy is partially addressed through data privacy law. Progressive data privacy legislation in Europe regulates the behaviour of Internet corporation, and even guarantees some enforceable data subject rights. While the scope of data privacy legislation is more nuanced, it essentially imposes direct obligation on corporations. But the absence of an enforceable international data privacy framework, considered in chapter 2, means that the gap in international human rights law vis-à-vis Internet corporations remains unaddressed.

The question of how best to envisage the possible human rights obligations of transnational corporations has been controversial. A major UN attempt in this field was the adoption in 2003 of the 'Norms and Responsibilities of Transnational Corporations'.²⁰⁹ These norms had envisaged 'periodic reporting' and 'verification' by the UN as monitoring mechanisms.²¹⁰ Because these 'norms' were framed in terms of strict 'obligations', they were not well received by stakeholders particularly corporations.²¹¹ This later forced the former Commission to retract these norms, and the matter received little attention for a while until the possibility of a 'soft law' measure was considered. The only applicable norms currently at the international level are the Ruggie Principles adopted by the HR Council in 2011.²¹²

The Guiding Principles do not strictly introduce new human rights obligations on businesses but rather 'elaborate' already existing State obligations in international human rights law. Para 12 of the Guiding Principles states that the 'corporate responsibility of businesses to respect human rights' emanate, *inter alia*, from the international bills of human rights which includes the ICCPR and the UDHR. The

²⁰⁹ See Sub-Commission on the Promotion and Protection of Human Rights, *Norms and Responsibilities of Transnational Corporations and other Business Enterprises with regard to Human Rights*, UN ESCOR, 55th sess, 22nd mtg, Agenda item 4, UN Doc E/CN.4/Sub.2/2003/12/Rev.2 (13 August 2003).

²¹⁰ Ibid, [16].

²¹¹ Ibid, [4]; see also Hurst Hannum, 'Reinvigorating Human Rights for the 21st Century' (2016) 16 *Human Rights Law Review* 409, 427-428.

²¹² See Guiding Principles on Business and Human Rights, above n 35.

human rights ‘responsibilities’ of businesses are four: (1) to refrain from infringing human rights; (2) to prevent infringement of human rights; (3) to mitigate impact of measures that impinge on human rights; and (4) to remedy violations of human rights. The practical utility of these Principles in addressing the role of Internet businesses vis-à-vis the right to privacy is limited. For one, the Principles being soft law, and hence bereft of any legally binding force, make them less effective.

The UN currently is in the process of translating these soft laws into a binding instrument. The HR Council has in 2014 created an open-ended ‘Inter-governmental Working Group’ to craft a ‘binding international legal instrument’ within the purview of international human rights law to regulate the activities of transnational corporations and other business enterprises.²¹³ While this might address the first concern by introducing an enforceable hard law, it appears not to adequately respond to the second concern. The Working Group has so far held several sessions but reports of the Group reveal that the discussions have not considered the case of Internet businesses.²¹⁴ The focus rather was on the depletion of natural resources and its impact on the rights of workers and vulnerable groups such as indigenous peoples, children and disabled persons.²¹⁵

A ‘zero draft’ has recently been released by the Working Group for substantive negotiation by States.²¹⁶ The draft mostly reads like a version of the Ruggie Principles in treaty form. Unlike a preceding document released by the Working Group that sought to impose direct obligations on corporations,²¹⁷ this is mainly addressed to States. Considering that the retraction was due to opposition from some States and business organizations,²¹⁸ the prospect of an instrument being adopted seems doubtful. It is also worth noting, in this regard, that the Council’s Resolution that creates the Working Group was curiously voted against by the US and the UK, along with other 12 countries.

The negative votes of the US and the UK do not come as surprise given their strongly held view that even the little disputed obligation of States to ‘protect’

²¹³ See *Elaboration of an International Legally Binding Instrument on Transnational Corporations and other Business Enterprises with respect to Human rights*, HRC Res 26/9, 26th sess, Agenda item 3, UN Doc A/HRC/RES/26/9 (14 July 2014) [1].

²¹⁴ See, e.g., *Report on the Second Session of the Open-ended Intergovernmental Working Group on Transnational Corporations and other Business Enterprises with respect to Human Rights*, UN Doc A/HRC/34/47 (4 January 2017).

²¹⁵ *Ibid*, [32-33], [65].

²¹⁶ See ‘Legally Binding Instrument to Regulate, in International Human Rights Law, the Activities of the Transnational Corporations and Other Business Enterprises’ (Zero Draft, 16 July 2018) <<https://bit.ly/2Ly1nT0>>

²¹⁷ See ‘Elements of the Draft Legally Binding Instrument on Transnational Corporations and Other Business Enterprises with respect to Human Rights’ (September 2017) sec 3.2 <<https://bit.ly/2fF5crq>>

²¹⁸ See Doug Cassel, ‘The Third Session of the UN Inter-Governmental Working Group on a Business and Human Rights Treaty’ (2018) 3 *Business and Human Rights Journal* 277, 281.

against abuses by third parties is limited, and not grounded in customary international law of human rights.²¹⁹ But it is still striking that the Resolution was adopted by 20 to 14 votes, with 13 abstentions.²²⁰ Almost all States who voted in favour of the Resolution were developing countries. Even some of the States like Russia that initially voted in favour of the Resolution have since opposed a treaty on business and human rights.²²¹ Reports of the Working Group also reveals that the level of participation, both from States and private actors, during the drafting of the instrument was limited. For instance, only a few States made submissions while no civil society working in the field of (digital) rights participated.²²²

Moreover, the process appears to be moving without any heed to the ongoing discussion at the UN on the 'right to privacy in the digital age', which is, as considered in chapter 4, gradually addressing the role of corporations under the right to privacy. The likelihood of such an instrument being adopted, in the face of such widespread lack of enthusiasm as well as possible resistance from businesses, appears to be low. This makes more uncertain the possibility of clear and strong international normative standards that determine the nature of responsibilities that Internet businesses owe in respecting and protecting the right to digital privacy of their users.

B Institutional-Structural Gaps

The second type of gap in international privacy law is institutional and structural. The current regime for the monitoring of human rights treaties relies on panels of independent experts organized in the form of committees, working groups and special procedures. When it comes to privacy, the monitoring of the right to privacy is undertaken mainly by the HR Committee and other treaties bodies such as the Committees that monitor CRPD, ICRMW and CRC as well as the Working Group that oversees the UN Guiding Principles.²²³ The UNSRP also has some role in the promotion and protection of the right to digital privacy.²²⁴

²¹⁹ See, e.g., 'Letter from David Bethlehem, Legal Advisor to UK's Foreign and Commonwealth Office, to John Ruggie, Special Representative of the Secretary General on Human Rights and Transnational Businesses and Other Business Enterprises' (9 July 2009); 'Observation of the United States on General Comment 31 of the Human Rights Committee' (December 2007) [10-18], [27].

²²⁰ See HRC Res 26/9, above n 213, annex.

²²¹ See Cassel, above n 218, 283.

²²² See details at <<https://bit.ly/2IemLOR>>; see also *Report on the Third Session of the Open-ended Intergovernmental Working Group on Transnational Corporations and other Business Enterprises with Respect to Human Rights*, UN Doc A/HRC/37/67 (24 January 2018).

²²³ See *Human Rights and Transnational Corporations and other Business Enterprises*, HRC Res 17/4, 17thsess, Agenda item 3, UN Doc A/HRC/RES/17/4 (16 June 2011) [6].

²²⁴ See *The Right to Privacy in the Digital Age*, HRC Res 28/16, 28thsess, Agenda Item 3, UN Doc A/HRC/RES/28/16 (26 March 2015).

But these human rights bodies operate in a framework that does not permit development of a robust regime for the protection of digital privacy. The Committees and Working Groups are composed of experts that work part-time. The HR Committee, for instance, is a Committee of 18 part-time experts who meet only three times per year, and only for four weeks each time.²²⁵ And, these part-time experts are expected to review State periodic reports (and adopt concluding observations), examine individual communications, develop GCs, hear reports of Rapporteurs on follow-up of views and concluding observations. Add to that the frequent reshuffle of members of the Committee, due to term limits and other factors, which affects development of a coherent rights jurisprudence.²²⁶ Interpretive inconsistencies, discussed above, regarding ‘home’ as well as the application of ‘arbitrariness’ are partly results of this institutional problem. What may follow from this state of affairs is that the Committee is not able to examine individual communications, periodic reports or GCs as rigorously as could be done with better resources. The broad range of Covenant rights that the Committee must address further works against full and proper examination of certain matters that implicate rights such as the right to privacy.

This adds to the broader challenge that these bodies do not have the power to pronounce legally binding decisions that impose sanctions against States found to be in breach of privacy rights. The HR Committee – like other Committees – is tasked under the ICCPR to adopt mere unbinding ‘views’ and ‘concluding observations’ under the individual communications and reporting procedures respectively. The SRP’s mandate is also only to promote the right to privacy through various mechanisms and to offer recommendations to the HR Council for the better protection of the right to privacy.²²⁷ The other relevant platform is the HR Council’s Universal Periodic Review (UPR) mechanism, which also has similar institutional limitations. But, vesting the HR Committee, as shall be argued in chapter 6, with the power to make binding decisions would not necessarily improve the protection of human rights. But it is reflective of the larger institutional-structural problem in the international law of privacy.

These institutional weaknesses translate into two practical challenges that reduce the effectiveness of the UN treaty monitoring framework. One is that the level of compliance by States found to be in violation of privacy rights is bound to be lower. States are likely to give deaf ears to non-binding views of the HR Committee, openly reject recommendations offered at the UPR or through concluding observations.²²⁸ This has, of course, occurred in practice. The level of State compliance with the views

²²⁵ See ICCPR, above n 1, art 28.

²²⁶ Of a related view, see Steiner, above n 115, 28-29.

²²⁷ HRC Res 28/16, above n 224, [4].

²²⁸ Of a related view, see Martin Sheinine, ‘The International Covenant on Civil and Political Rights’ in Geir Ulfstein et al (eds), *Making Treaties Work: Human Rights, Environment and Arms Control* (Cambridge University Press, 2007) 66.

of the Committee has, for instance, been generally low. In its 2015 report to the UNGA for instance, the Committee complained that ‘many’ State parties have failed to implement views adopted under the Optional Protocol.²²⁹ Similar non-compliance tendencies have been detected at the UPR. Studies have shown that two years after the review process commenced States had acted only on 40% of the recommendations given.²³⁰ Moreover, only 43% of the recommendations were accepted by States under review at the 14th session of the second cycle.²³¹

Secondly, the lack of discretion to pronounce binding and enforceable decisions against recalcitrant States also has the effect of limiting recourse by individuals whose privacy rights have been violated. Partly, this is because there are relatively effective regional courts that are empowered to issue enforceable decisions in Europe and the Americas. It is conceivable that Europeans would be more inclined to resort to, for example, the ECtHR than a rather powerless Committee to seek remedy against their States.²³² This explains why individuals and civil society groups mount several successful legal challenges in the wake of the Snowden revelations against mass digital surveillance before these European courts, not the HR Committee. It is also interesting to note that most digital privacy cases against European governments considered by the Committee, highlighted below, have initially been submitted to either the former European Commission on Human Rights or the ECtHR but declared inadmissible. This lends weight to the argument, then, that European authors filed complaints with the UN Committee (mainly) because their cases were declared inadmissible by the more effective regional bodies.

To summarize, the overall ‘cooperative framework’ that animates the UN human rights system renders human rights monitoring bodies’ roles to be merely advisory rather than judicial. But the problem is not solely the lack of authority to issue legally binding decisions. Indeed, the way forward in strengthening the UN privacy system lies in rebuilding its central dialogical approach. Chapter 6 returns to the way in which the existing regime based on cooperative dialogue must be entrenched and enhanced in the digital age.

C Jurisprudential Gaps

The third major limitation of the current international regime for the protection of the right to digital privacy is jurisprudential, which flows from the normative and institutional limitations considered above. Not only are normative texts vague and

²²⁹ See, e.g., *Annual Report of the Human Rights Committee to the General Assembly*, UNGAOR 70th sess, UN Doc A/70/40 (April 2015) [40].

²³⁰ See, e.g., Roland Chauville, ‘The Universal Periodic Review’s First Cycle: Successes and Failures’ in Hilary Charlesworth and Emma Larking (eds), *Human Rights and the Universal Periodic Review: Rituals and Ritualism* (Cambridge University Press, 2015) 93.

²³¹ See Universal Periodic Review (2013) 1 *Human Rights Monitor Quarterly*, 27.

²³² Of a related view, see Steiner, above n 115, 34.

ill-conceived but also the jurisprudence developed around these norms by a rather weak institutional framework has been thin and stagnant. A closer look at the practices of the UN Committees that monitor relevant human rights treaties such as the ICCPR, CRPD, ICRMW and CRC as well as the HR Council and Working Group installed to monitor the UN Guiding Principles reveal that a coherent and progressive digital privacy jurisprudence is yet to emerge. This section provides some highlights of the jurisprudence, or the lack thereof, on digital privacy to illustrate the jurisprudential dearth. The discussion explores first privacy jurisprudence, or the lack thereof, of relevant UN treaty bodies, and second, HR Council (and associated) bodies such as the UPR and Special Procedures.

1 Treaty Body Jurisprudence

(a) Case Law

Cases that implicate the right to privacy in the digital context have been few and far between in the international fora. Cases relating to the right to privacy under the ICCPR are considered mainly by the HR Committee. The other treaty bodies that monitor the CRPD, ICRMW and CRD are yet to consider digital privacy cases. At the time of writing, there was one privacy case considered by the Committee that monitors the CRPD but it concerned physical privacy, and was ultimately declared inadmissible *ratio temporis*.²³³ The required number of declarations recognizing the competence of Committee that monitors the ICRMW has not been achieved means that the individual communications procedure under Article 77 of the Convention has not yet entered into force.²³⁴ The Committee that monitors CRC is also unlikely to consider digital privacy cases anytime soon as its Optional Protocol on Individual Communication has only 42 State parties.²³⁵

Another possible avenue for consideration of (digital) privacy cases is the complaints procedure of the HR Council which allows lodgement of complaints concerning 'consistent patterns of gross and reliably attested violations of human rights'.²³⁶ Mass digital surveillance by governments and corporations of the scale revealed by Snowden might arguably meet the threshold to be scrutinized by the Council. But there is no record of such complaints so far, unsurprisingly, because the threshold appears to invite mostly gross human rights violations such as torture, enslavement and enforced disappearance.

The case law of the HR Committee, which is best placed to address digital privacy, is also yet to arrive. Most privacy cases adjudged by the HR Committee concern the

²³³ See HR Committee, *Kenneth McAlpine v United Kingdom* (Communication No. 6/2011, 13 November 2012).

²³⁴ See details at <<https://bit.ly/2tJeeeu>>

²³⁵ See details at <<http://indicators.ohchr.org/>>

²³⁶ See *Institution Building of the United Nations Human Rights Council*, HRC Res 5/1, 5th sess, 9th mtg, UN Doc A/HRC/RES/5/1 (18 June 2007) [85].

right to ‘family life’ of foreigners facing expulsion orders, the right to not to be subjected to unreasonable search and seizure or interference with the secrecy of prisoners’ correspondence.²³⁷ A review of the Committee’s case docket results in only four cases relating to privacy that centre around digital communications such as the Internet and telecommunications as well as disclosure of personal information.²³⁸ Even these cases touch on digital privacy only peripherally. More often, the Committee has reviewed these cases in the context of reputation/honour than privacy per se. And where some of these cases concern digital privacy, the Committee has barely addressed them in full context, and as such the decisions are not preceded by thorough examination.

(b) Concluding Observations

Concluding observations are another source of jurisprudence in the UN human rights framework. The observations are basically concluding views of the treaty bodies after periodic reports of State parties are reviewed, and an interactive dialogue is held with the State under review. A typical feature of concluding observations is that, after a paragraph that briefly outlines concerns regarding a given piece of national law or practice that impinges on provisions of the relevant human rights treaty, the relevant treaty body urges the State party to ensure that the law or the practice is aligned to the treaty. Often, States are called upon to provide remedies, amend laws to make them in accord with the relevant human rights instrument and provide an independent oversight mechanism, for example, for surveillance measures.

Digital privacy has relatively received frequent attention through concluding observations at the HR Committee in contrast with the case law.²³⁹ Since its early days – and more so since the Snowden revelations, the Committee has adopted concluding observations that relate to wiretapping of telephones,²⁴⁰ data privacy,²⁴¹

²³⁷ See, e.g., HR Committee, *Al-Gertani v Bosnia and Herzegovina* (Communication No. 1955/2010, 6 November 2013); *Marouf v Algeria* (Communication No. 1889/2009, 29 April 2014).

²³⁸ See HR Committee, *I.P. v Finland* (Communication No. 450/1991, 26 July 1993); *Antonius Cornelis Van Hulst v The Netherlands* (Communication No. 903/1999, 15 November 2004); *Nabil Sayadi and Patricia Vinck v Belgium* (Communication No. 1472/2006, 29 December 2008); *H.S. v Australia* (Communication No. 2015/2010, 13 May 2015). No individual communication alleging violation of the ICCPR through surveillance has been made to the Committee. See Shany, below n 244 (note that Shany is currently a member of the Committee).

²³⁹ It to be noted that no privacy related concluding observations has been adopted by the other treaty bodies, except one on the right to family life by the Committee that monitors the CRPD. For a list of Concluding Observations by the Committee, see <<http://bit.ly/2fUo4lZ>>

²⁴⁰ See, e.g., *Comments of the HR Committee: Russian Federation* (26 July 1995) [19]; *Concluding Observations of the HR Committee: Jamaica* (19 November 1997) [20]; *Concluding Observations of the HR Committee: Poland* (29 July 1999) [22]; *Concluding Observations of the HR Committee: The Netherlands* (25 August 2009) [14]; *Concluding Observations of the HR Committee: Bulgaria* (19 August 2011) [22].

domestic laws that authorize warrantless and excessive surveillance²⁴² and more recently mass digital surveillance.²⁴³ A recent independent survey by a member of the HR Committee reveals that concluding observations relating to digital surveillance have increased by 25% since the Snowden revelations.²⁴⁴ Concluding observations are not, however, structurally best placed to expound and give content to the right to privacy provision of the relevant human rights treaties. The inherent limitation of the reporting procedure – and hence concluding observations – is that these observations, unlike case law, do not examine a particular scenario in the light of the specific human rights in question, and as such they add little to the development of jurisprudence on digital privacy. The brief nature of concluding observations have also robbed them of jurisprudential significance.

(c) General Comments

The other sources of jurisprudence in international human rights law are GCs adopted by the relevant treaty bodies. These comments are meant to elaborate content of human rights and as such, they are sometimes referred to as ‘restatements’ or ‘authoritative interpretations’ of the treaty provisions.²⁴⁵ GCs are drafted based on the jurisprudence developed by the relevant treaty body particularly from its concluding observations on periodic reports submitted by State parties.²⁴⁶ The primary purpose of GCs is to offer guidance for States in the course of complying with their human rights treaty obligations particularly in their periodic reports.

GCs relating to digital privacy have so far been adopted by the HR Committee and the Committee on the Rights of the Child.²⁴⁷ But it is GC 16 of the HR Committee that

²⁴¹ See, e.g., *Concluding Observations of the HR Committee: Sweden* (2 April 2009) [18]; *Concluding Observations of the HR Committee: Hungary* (16 November 2010) [6]; *Concluding Observations of the HR Committee: France* (13 July 2008) [22].

²⁴² See, e.g., *Concluding Observations of the HR Committee: Poland* (31 October 2016) [39]; *Concluding Observations of the HR Committee: France* (17 August 2015) [12]; *Concluding Observations of the HR Committee: New Zealand* (28 April 2016) [15-16].

²⁴³ See, e.g., *Concluding Observations of the HR Committee: The United Kingdom of Great Britain and Northern Ireland* (17 August 2015) [24]; *Concluding Observations of the HR Committee: The United States of America* (23 April 2014) [22].

²⁴⁴ See Yuval Shany, ‘Online Surveillance in the Case Law of the Human Rights Committee’ (The Hebrew University of Jerusalem Center for Cybersecurity Research, 13 July 2017) available at <<https://bit.ly/2MECR7m>>

²⁴⁵ See Tyagi, above n 119, 285, 302.

²⁴⁶ See, e.g., ICCPR, above n 1, art 40(4)

²⁴⁷ But GCs adopted by the latter address digital privacy only peripherally. The GC on the HIV/AIDS and the Rights of the Child, for instance, emphasizes the need to respect and protect the privacy of medical data of the child. See Committee on the Rights of the Child, *General Comment 3: HIV/AIDS and the Rights of the Child*, 32 sess, UN Doc CRC/GC/2003/1 (17 March 2003) [6], [20], [24], [29], [40(c)]. Note, though, that the Committee has just initiated a process towards a new GC on ‘children’s rights

offers some guidance on the right to (digital) privacy although it was adopted as far back as 1988 and written in truncated forms. It addresses the right to digital privacy in two levels. First, it provides that the right to privacy of correspondence must be protected de jure and de facto, and surveillance is prohibited under Article 17.²⁴⁸ Second, the GC addresses privacy of personal data to some degree. It provides that States' positive obligation under Article 17 includes the regulation by law of automated collection and processing of personal information both by the public and private sectors.²⁴⁹ This can be taken to mean that Article 17 requires States to pass data privacy legislation.

Furthermore, the GC briefly reflects four principles of data privacy law.²⁵⁰ The principle of 'data security' is implicit when the Comment states 'information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it'. The GC's stipulation that information concerning a person's private life must not be 'used for purposes incompatible with the Covenant' mirrors the 'use limitation principle'. The 'principle of data subject participation' is also partially envisaged under the GC where it empowers data subjects to ascertain the identity of the person who holds data on them and what information. The GC's proviso allowing data subjects to request rectification of incorrect information about them held by third parties highlights the 'principle of data quality'.

GC 16 has three basic limitations, however. One is that it recognizes only some of the basic data privacy principles, and even those reflected in the GC are not adequately elaborated.²⁵¹ This is mainly due to the truncated nature of the comment. Second, GC 16 – as for other GCs – is not a legally binding document, and as a result it is difficult for individuals to invoke provisions of the Comment to challenge privacy violations. Third, the Comment was adopted by the HR Committee in 1988, before modern technologies including the Internet are introduced or entered the mainstream. This reduces its pertinence to new threats to privacy posed by rapid technological advances. Recent calls and initiatives for a new GC are prompted by this outmoded state of the present GC.²⁵²

But the jurisprudence of the HR Committee to date, as noted above, appears to be too thin to lead to a new GC. It is not also straightforward whether the Committee

in relation to the digital environment' which, as hinted in a concept note, will consider the right to privacy. See <<https://bit.ly/2UnSFeO>>

²⁴⁸ See GC 16, above n 155, [8].

²⁴⁹ Ibid, [10].

²⁵⁰ Ibid.

²⁵¹ Of a similar view, see Lee Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 *International Journal of Law and Information Technology* 247, 253.

²⁵² See, e.g., Report of Scheinin, above n 198, [19], [74]; Report of the High Commissioner, above n 193, [10]; ACLU, above n 178, 3-10 and annex of a Draft GC.

could simply develop a new GC based on, say, draft proposals tabled by civil society groups or even on its own accord drawing on comparative (case) law. Also unclear is how/if a new GC would improve the protection of digital privacy or more generally induce better State behaviour. As shall be discussed in chapter 5, a GC is amongst the various types of soft law explored as the best way of addressing the ‘normative gap’ in the international privacy law. But the adoption of a new GC without any reform in the institutional arrangements will not result in substantial progress in global privacy protection.

2 Jurisprudence of HR Council Bodies

The dearth in privacy jurisprudence is also present when it comes to HR Council bodies. One is the UPR mechanism. It is a recent human right monitoring mechanism within the HR Council that reviews human rights performance of all UN member States irrespective of ratification of any of the human rights treaties.²⁵³ The review mechanism relies, like the bulk of the UN human rights monitoring system, on ‘cooperative and interactive dialogue’ and is devoid of any remedial procedure.²⁵⁴ The ultimate consequence for ‘persistent non-cooperation’ is that the Council would pass a decision or resolution condemning the non-cooperative State.²⁵⁵ When it comes to the review of States in relation to the right to digital privacy, there is little to be said. The review process, which is now in its the third cycle, has so far reviewed quite a few countries regarding their digital surveillance practices post-Snowden.²⁵⁶ Inherent structures of the UPR mechanism, as well as the *modus operandi* of the Council, however, makes it an unlikely candidate to address concerns regarding digital privacy more directly. The fact that reviews are often made by high-level government delegates meant that little could be anticipated of the UPR in elaborating the right to privacy in the digital context and holding States to account for violations.

A second potential source of privacy jurisprudence under the HR Council is the work of the Working Group that monitors the Ruggie Principles. However, a survey of the Working Group’s reports suggests that there is little to be said. A 2016 report of the Working Group, for instance, focuses on the ‘human rights impacts of agroindustry operations, particularly the production of palm oil and sugarcane, on indigenous peoples and local communities’.²⁵⁷ An earlier report from 2014 even

²⁵³ For details on the UPR mechanism, see <<https://bit.ly/1dSvPEw>>

²⁵⁴ See HRC Res 5/1, above n 236, [33-38]; see also *Human Rights Council*, GA Res 60/251, 60th sess, Agenda items 46 and 120, UN Doc A/RES/60/251 (3 April 2006) [5(e)].

²⁵⁵ *Ibid.*

²⁵⁶ See, e.g., ‘Australia: Report of the UPR Working Group’ (13 January 2016) [136] cum ‘Australia: Addendum to the Report of the UPR Working Group’ (29 February 2016) [28]; ‘United States of America: Addendum to the Report of the UPR Working Group’ (14 September 2015) [14-15]; ‘India: Report of the UPR Working Group’ (17 July 2017) [161.145].

²⁵⁷ See *Report of the Working Group on the Issue of Human Rights and Transnational Corporations and other Business Enterprises*, UN Doc A/71/291 (4 August 2016).

indicated that its areas of priority for the future will be promoting the incorporation of the Guiding Principles in the policy framework of ‘international institutions.’²⁵⁸

The Guiding Principles have recently been adapted by Global Network Initiative (GNI), a civil society organization that promotes privacy and free speech on the Internet, to be applied by the technology sector. GNI’s ‘Principles on Freedom of Expression and Privacy’, adaptations of the Ruggie Principles, outline general norms that could voluntarily be followed by technology companies.²⁵⁹ Of major Internet companies, Google, Microsoft and Yahoo! have accepted the principles and undergo independent reviews of their systems, processes and policies for the protection of freedom of expression and privacy.²⁶⁰ The review is made by ‘accredited assessors’ that conduct the assessment based on the assessment criteria and report to GNI Board, which is composed of various stakeholder representatives, for review and determination.²⁶¹ That the review relies on good faith self-reporting by some corporations means that it can only be a supplementary mechanism of holding corporations into account. GNI’s early work had, indeed, drawn criticism, particularly due to lack of robust assessment mechanisms.²⁶² In sum, there currently exists no concrete jurisprudence on the human right responsibilities of Internet businesses.

The SRP is the other HR Council body with a potential to progressively develop international privacy jurisprudence. But, added with the largely ‘promotional’ role of UN special procedures — and partly because the SPR was appointed only in 2015, the mandate is yet to contribute towards filling the jurisprudential gaps. Reports of the SRP have yet to offer intellectual guidance on the scope and meaning of the right to privacy in international law. The mandates work thus far has focused primarily on creating a number of ‘task forces’ dealing with specific aspects of the right to privacy.²⁶³ And, the outcome of these task forces, and the way in which they would address the jurisprudential gaps remains unclear. The only tangible outcome so far has a draft recommendation released by the task force working on the theme ‘privacy and health data’.²⁶⁴ While this draft may later evolve into an international soft law, it does little in filling the jurisprudential gaps addressed in the thesis. As it

²⁵⁸ See *Report of the Working Group on the Issue of Human Rights and Transnational Corporations and other Business Enterprises*, UN Doc A/HRC/26/25 (5 May 2014) [84], [87].

²⁵⁹ See ‘Principles on Freedom of Expression and Privacy’ (Global Network Initiative, 2008) <<https://bit.ly/2FKiCwQ>>

²⁶⁰ See ‘Global Network Initiative: 2015 Annual Report’ (2015) 4.

²⁶¹ See details at <<https://bit.ly/2HSY3EB>>

²⁶² See, e.g., Sarah Joseph, ‘Social Media, Political Change and Human Rights’ (2012) 35 *Boston College International and Comparative Review* 145, 184.

²⁶³ See, e.g., *Report of the Special Rapporteur on the Right to Privacy, Joseph Cannataci*, UN Doc A/72/43103 (19 October 2017).

²⁶⁴ *Draft Recommendation on the Protection and Use of Health-Related Data* (Mandate of the United Nations Special Rapporteur on the Right to Privacy – Task Force on Privacy and the Protection of Health-Related Data, June 2019).

currently stands, the draft outlines a range of principles applicable to processing of health-related personal data.

IV CONCLUSION

This chapter argued that international human rights law is currently ill-equipped to respond to the ‘privacy problem’ in the digital age. Mainly due to political controversies that clouded the drafting of relevant standards –and exacerbated by poor drafting, the human right to privacy framework exhibits several weaknesses. The chapter examined the principal normative, institutional, and the resultant jurisprudential gaps. This attests to the need for a progressive development of existing privacy standards to adapt them to the digital age. Nevertheless, recent developments at the UN reveal an ambivalent approach as to whether existing standards require some form of updating or translation.

Post-Snowden revelation discussions at the UN proceed from the assumption that the right to privacy in international human rights law is fit for purpose in the digital age. The problem, or rather gap, is in the domestic law and practices of States.²⁶⁵ Resolutions of the UNGA and the HR Council on the ‘right to privacy in the digital age’ routinely call upon States to ensure that their national laws and practices comply with international human rights law. This viewpoint maintains that mere abstract high-level general principles provided in the UDHR and the ICCPR are adequate to set international standards. Latent in this supposition is the idea that present international privacy norms set forth under the UDHR (and the ICCPR) are eternal principles that apply across changing times.²⁶⁶ No changes in technology or other developments to date are believed to render these principles obsolete.

A more benign interpretation of this assumption is that these ‘eternal principles’ will just have to be applied to a new set of circumstances by, for example the HR Committee, evolutive interpretation. Seibert-Fohr, a former member of the Committee, argues that there is no ‘blind spot’ in the international law of privacy and what is lacking is national-level regulation.²⁶⁷ She suggests that the Committee’s

²⁶⁵ See, e.g., *Report of High Commissioner for Human Rights: The Right to Privacy in the Digital Age*, UN Doc A/HRC/39/29 (3 August 2018) [58] (noting that ‘the international human rights framework provides a strong basis for shaping the responses to the manifold challenges arising in the digital age’).

²⁶⁶ See, e.g., Gordon Brown (ed), *The Universal Declaration of Human Rights in the 21st Century: A Living Document in A Changing World* (Open Book Publishers, 2016) 14, 25, 29; Paul Lauren, *The Evolution of International Human Rights: Visions Seen* (University of Pennsylvania Press, 3rd ed, 2011) 226 (stating the UDHR is targeted at the future); William Schabas (ed), *The Universal Declaration of Human Rights: The Travaux Préparatoires* (Cambridge University Press, Vol. I, 2013) xxiii (stating that the drafters of the UDHR were ‘sensitive’ to the evolving nature of human rights).

²⁶⁷ Anja Seibert-Fohr, ‘Digital Surveillance, Meta Data and Foreign Intelligence Cooperation: Unpacking the International Right to Privacy’ (April 2018) <<https://bit.ly/2GSm3FP>>

‘evolutive interpretation’ has allowed it to ‘confront new challenges and keep human rights protection alive and effective based on the existing legal framework’. As this chapter has demonstrated, that is not really the case. Not only is the (international) human right to privacy framework replete with normative ‘blind spots’²⁶⁸ but also that the HR Committee, strapped by structural shackles, has not been able to develop a robust digital privacy jurisprudence.

This suggests that gradual normative progression is both possible and desirable in the human rights movement. As Alston notes, ‘gradualism’ is an inherent characteristic of the international human right system.²⁶⁹ The UDHR also hints the gradualist nature of rights protection, stating:

*‘states shall strive [...] to promote respect for these rights and freedoms by progressive measures, national and international’.*²⁷⁰[Emphasis added]

Such progressive measures arguably include gradual development of international human rights norms. This is, indeed, reflected partly in the privacy provisions of post-ICCPR human rights instruments.²⁷¹ The CRPD and the ICRMW, for instance, appear to be progressive, to some degree, especially in suggesting inclusion of modern forms of ‘communication’ as new media of correspondence.²⁷² The Conventions, in so doing, follow other progressive regional instruments such as the EU Fundamental Rights Charter of 2000.²⁷³ The CRPD also addresses protection of data privacy at some length.²⁷⁴ With the adoption of Optional Protocol to the CRC on the Sale of Children, Child Prostitution and Child Pornography, the CRC has also progressed to protect the right to (digital) privacy of child victims of abuse, particularly in the context of criminal proceedings.²⁷⁵ Considering limitations of the present regime explored in this chapter, there is a need to reimagine international human right to privacy framework to make it better equipped in the digital age. Subsequent chapters further explore the question of how best to meet this need.

²⁶⁸ Cf Tobin, above n 26, 44 (describing ‘blind spots’ in human rights treaties as ‘issues that were overlooked or unanticipated in the drafting process but that are essential to the effective operation of the relevant provision and thus require the development of an appropriate interpretive response’).

²⁶⁹ Philip Alston, ‘Beyond Them and Us: Putting Treaty Body Reform into Perspective’ in Alston and Crawford (eds), above n 115, 522.

²⁷⁰ See UDHR, above n 1, preamble.

²⁷¹ Note, though, that these Conventions also backtrack in some respects, one instance being the CRPD intriguingly omits ‘home’ from the zones of privacy protection.

²⁷² See CRPD, above n 112, art 22 (1); see also ICRMW, above n 112, art 14.

²⁷³ See *Charter of Fundamental Rights of the European Union*, proclaimed on 7 December 2000, [2000] OJ C 326/393 (entered into force 1 December 2009) art 7.

²⁷⁴ See CRPD, above n 112, art 22 (2) cum art 31(1). For more, see ch 2.

²⁷⁵ See *Optional Protocol to the CRC on the Sale of Children, Child Prostitution and Child Pornography*, opened for signature 25 May 2000, 2171 UNTS 227 (entered into force 18 January 2002) art 8(1(e)) cum [6] of the preamble; see also a recent UN Resolution affirming this right, *Rights of the Child: Information and Communications Technologies and Child Sexual Exploitation*, HRC Res 31/7, 31st sess, Agenda item 3, UN Doc A/HRC/RES/31/7 (23 March 2016).

CHAPTER 2 — DIGITAL PRIVACY AND BOUNDARIES OF UNITED NATIONS' DATA PROTECTION FRAMEWORK

I INTRODUCTION

This chapter turns to consider boundaries of the UN data protection framework in securing digital privacy. In undertaking this regime analysis, it seeks to show the extent to which present data privacy standards supplement the human right to privacy framework. Unlike the much-developed European data privacy regime, the origins of the UN data privacy framework are closely related to the human rights system. Early UN work in the field of data privacy emerged at the Teheran Conference in 1968 on the occasion of the 20th anniversary of the UDHR. Held merely two years after the adoption of the ICCPR, the Conference was seized with issues surrounding 'scientific and technological developments' and their impact on human rights, particularly the right to privacy.

In his opening address at the Conference, the then UN Secretary-General, U Thant, set the tone of the Conference with a rhetorical question of whether the 'right to a minimum of privacy' could be protected in the face of 'ever-present listening and seeing electronic devices'.²⁷⁶ This was followed by a Resolution that called upon the UN to conduct studies on the impact of modern technological developments on the right to privacy, a point later reiterated in the Proclamation of Teheran at the conclusion of the Conference.²⁷⁷ After decades of protracted process, visions of the Conference were translated into the UN Data Privacy Guidelines adopted by the UNGA in December 1990. The Guidelines are the principal UN instruments in the field of data privacy to date.

This chapter argues that UN data protection framework is normatively outdated, highly fragmented, and devoid of clear institutional arrangements to be considered an important source of international privacy law. A characteristic feature of the UN data privacy system is that it is made up of highly dispersed rules embodied in a number of instruments. In addition to the Data Privacy Guidelines, present UN data privacy rules are also to be found in other instruments, including major human rights treaties and a range of soft law instruments adopted by various specialized and related agencies of the UN. Drawing a parallel to the human right to privacy framework, the chapter further locates factors for the present weak structure of the

²⁷⁶ Address Delivered by the Secretary-General of the United Nations, U Thant, in Commemoration of the Twentieth Anniversary of the Adoption of the Universal Declaration of Human Rights (Teheran, Islamic Republic of Iran, 22 April 1968).

²⁷⁷ *Human Rights and Scientific and Technological Developments*, Resolution XI, adopted at the Teheran Conference, 25th plenary mtg (12 May 1968) [2(a)]; see also *The Proclamation of Teheran*, UN Doc A/CONF.32/41 (13 May 1968) [18].

UN privacy framework in Cold War political controversies and the overall apathy towards privacy at the UN. The chapter concludes that the gradual prominence of data privacy themes in the ongoing UN privacy discourse bears a potential of reviving and modernizing the UN data privacy framework.

With a view to properly appreciate limits of the UN data protection framework, comparative references are made in this chapter to the relatively developed data protection regime of the EU and the CoE.

II BACKGROUND TO UNITED NATIONS' DATA PROTECTION FRAMEWORK

UN initiatives in the field of data privacy began relatively early, shortly after the human right to privacy was enshrined in a binding treaty. These initiatives were, however caught up in protracted processes of negotiation, and a major UN data privacy instrument was adopted long after regional organizations enacted influential instruments that set the tone of data privacy law worldwide. Ideological differences that resulted in a weak regime for the protection of the human rights to digital privacy, considered in chapter 1, have had similar negative impact on the data privacy framework. This, in part, has to do with the human rights origins of the data privacy framework. As noted above, UN efforts in the field of data privacy were set in motion in the context of human rights as the UN moved to renew the commitment pledged by States with the adoption of the UDHR. But the overall reluctant approach to the privacy in the UN system has compounded the effects of the ideological factor. An overview of these historical episodes offers context to fully bring out the limits of the current international data privacy regime.

A The Cold War Effect

As the UN began to consider the impact of 'scientific and technological developments' on human rights in the wake of the Teheran Conference, the debate was divided along the North-South and the East-West ideological lines.²⁷⁸ Countries in the South/East camp which mostly included developing countries insisted on the need to emphasis on the socio-economic benefits of scientific and technological discoveries whereas those in the North/West bloc, mainly industrial nations, argued for priority to be given to the negative impact of these technologies on human rights particularly, the right to privacy.²⁷⁹ These divisions could be seen partly as reverberations of the broader debate on the 'generation of human rights' that divided States between those that argued for the priority of civil and political rights

²⁷⁸ See Sadako Ogata, 'Introduction: United Nations Approaches to Human Rights and Scientific Developments' in Christopher Weeramantry (ed), *Human Rights and Scientific and Technological Development* (United Nations University Press, 1990) 3-4.

²⁷⁹ See Moses Moskowitz, *International Concern for Human Rights* (Oceana Publications, 1974) 14-15.

– i.e. first generation rights – and those that put thrust on socio-economic and cultural rights – i.e. ‘second generation rights’.²⁸⁰

Despite initial references to (data) privacy as one area deserving of further study post-Teheran,²⁸¹ ideological divisions later pushed the matter to the edges. The South/Easter bloc led by the Soviet Union pushed, instead, for an international instrument that emphasised on the use of modern technologies for positive ends. This later led to the adoption by the UNGA of the ‘Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Mankind’ in 1975.²⁸² The Declaration slightly diverted the question of human rights particularly privacy, and directed its focus on the need to gear technological innovations to positive economic ends.²⁸³ The Declaration was initially recommended by a group of experts assembled by the Secretary-General, but the expert’s recommendation appeared to have had more emphasis on human rights.²⁸⁴

The Declaration’s reference to human rights in general and privacy in particular is slightly remote. It, for instance, requires States to take all measures including legislative measures to prevent the use of modern technologies particularly by State organs in a manner or for purposes that limit the rights recognized in the UDHR and the ICCPR.²⁸⁵ The right to privacy, one of the main areas initially identified for further study, and possible international legal response, also similarly received lesser attention. The Declaration states partly:

All states shall take measures [...] to protect [all strata of the population] from harmful effects of the misuse of science and technological developments including their misuse to infringe upon the rights of the individual [...] particularly with regard to respect for privacy [...].²⁸⁶ (Emphasis Added).

Unlike States’ widely accepted human rights obligations in international law both to ‘respect’ and ‘protect’, this provision appears to recognize only an obligation to ‘protect’, i.e. a positive obligation, and hence no obligation to ‘respect’, i.e. negative

²⁸⁰ See Edmundson, above n 113, 173-74.

²⁸¹ See, e.g., *Human Rights and Scientific and Technological Developments*, GA Res 2450 (XXIII), 1748th plenary mtg, UN Doc A/RES/2450(XXIII) (19 December 1968) [1(a)].

²⁸² *Declaration on the Use of Scientific and Technological Progress in the Interest of Peace and for the Benefit of Mankind*, GA Res 3384 (XXX), 2400th plenary mtg, UN Doc A/RES/3384(XXX) (10 November 1975).

²⁸³ See Christopher Weeramantry, ‘Science, Technology and the Future of Human Rights’ (1986) 13 *India International Centre Quarterly* 41, 47.

²⁸⁴ *Existing and Proposed Texts which could be used in the Drafting of a Further International Instrument on Human Rights and Scientific and Technological Developments*, Commission on Human Rights, 33rd sess, Item 8 of provisional agenda, UN Doc E/CN.4/1233 (16 December 1976) [2], footnote 2, quoting UN Doc E/CN.4/1199 (1975) [4-5].

²⁸⁵ See GA Res 3384 (XXX), above n 282, [2] cum [8-9].

²⁸⁶ *Ibid*, [6].

obligation, is to be read into the provision. Implicit in this wording is that the Declaration sought to absolve States, and their agents, from any responsibility for violation of human rights, including privacy. The general emphasis on 'sovereignty' and 'international peace and security' further reinforces that point. Of course, one of the constant controversies in human rights standard setting has been that human rights and the attendant monitoring mechanism would undermine the domestic jurisdiction of States. This traditional argument seems to have led the East/South bloc to shift the attention of the momentum set in Teheran.²⁸⁷

Ideological fault lines featured more clearly during voting on the Declaration. Unsurprisingly, States in the North/West bloc boycotted the Declaration, and they finally abstained during the voting.²⁸⁸ It appears that the effort on the part of the North/West bloc to successfully push the cause of human rights was frustrated by the overwhelming majority of the South/East camp which was made up of several countries from Asia, Africa, East Europe and the Middle East. To vent their frustration the western bloc resorted to a politically motivated Resolution on the mistreatment of mentally ill persons in imprisonment in east European countries.²⁸⁹ This was part of the trend at the time by which western countries reportedly used human rights as a stick to beat socialist countries.²⁹⁰ Ogata observed that due to the ideological conflict, the Western camp had lacked enthusiasm to push for human rights initiatives during this time.²⁹¹

Perhaps, the inability to pursue a tangible (data) privacy agenda at the UN seems to be the reason for western countries to focus more on a regional approach to data privacy through the CoE and the Organization for Economic Cooperation and Development (OECD) where there exists considerable ideological convergence among member States. Indeed, in the context of human rights, Cassese writes that the Cold War confrontation had led (western) States to agree upon measures at the regional level where there frequently is greater homogeneity.²⁹² Soft law was the other alternate path taken to bypass the impasse of the Cold War period.²⁹³ The adoption ultimately of the UN Data Privacy Guidelines best illustrates this point.

Reverberations of Cold War politics were also felt during the drafting of other UN data privacy instruments. One instance was during the drafting of United Nations Educational, scientific and Cultural Organization (UNESCO) instruments relating (data) privacy, considered in section III below. At least in the context of the 'Universal Bio-ethics Declaration', recourse was made to a Declaration as opposed to

²⁸⁷ See Hiroko Yamane, 'Impacts of Scientific and Technological Progress on Human Rights: Normative Response of the International Community' in Weeramantry (ed), above n 278, 91.

²⁸⁸ See Ogata, above n 278, 4.

²⁸⁹ Ibid, 5-6.

²⁹⁰ See Cassese, above n 125, 300.

²⁹¹ Ogata, above n 278, 4.

²⁹² See Cassese, above n 125, 198.

²⁹³ Ibid.

a treaty due to two reasons according to Kirby who was involved in the drafting process. One is relevant in this context. A binding treaty should be considered, it was agreed by the time, at a later stage once States have deliberated and consulted on the Declaration, like in the case of the UDHR which later was translated into two covenants.²⁹⁴ The obvious resistance towards stringent human rights commitment among many States appears to have dictated a soft law approach.

In sum, the successful lobbying of the South/Eastern bloc and the lack of enthusiasm among western countries had further reduced the possibility of a major UN data privacy initiative. All the UN could achieve after two decades of prolonged process was mere Guidelines.²⁹⁵ A soft law instrument that provides only high-level principles of fair information practices, with no effective machinery of monitoring, is thus a result of the political compromise, one that had to be struck between ideological foes of the time.

B The (Data) Privacy Inattention Effect

Yet, the Cold War effect alone does not fully explain the weak structures of the UN data privacy regime. A reluctant approach to the privacy agenda entrenched in UN processes is equally responsible for the lack of a robust data privacy regime. This problem was more visible within the former Commission on Human Rights under whose aegis the work on the UN Data Privacy Guidelines was carried out. The Commission, for instance, was not able to closely consider various studies on the subject conducted under the auspices of the Secretary-General between 1968 and 1976.²⁹⁶ This had forced the UNGA to issue a Resolution expressing 'regrets' over the delay in considering the matter by the Commission in due time.²⁹⁷ Although the official excuse was 'lack of time', divergence of priorities among States appears to have been the principal factor in dragging the agenda item.

Even before the actual work on the Guidelines began, States had made it clear that all that they are willing to consider was a 'general guideline' that could guide States in legislating at the national level.²⁹⁸ Yet the work on these guidelines did not begin until 1980, and the first draft was submitted only four years later.²⁹⁹ Several drafts of the Guidelines were circulated among member States to achieve some level of consensus before they were finally adopted in 1990.³⁰⁰ Reports suggest that most

²⁹⁴ See Michael Kirby, 'Human Rights and Bioethics: The Universal Declaration of Human Rights and UNESCO Universal Declaration of Bioethics and Human Rights' (2009) 25 *Journal of Contemporary Health Law and Policy* 309, 320.

²⁹⁵ See UN Data Privacy Guidelines, above n 29.

²⁹⁶ See Yo Kubota, 'The Institutional Response' in Weeramantry (ed), above n 269, 113-114.

²⁹⁷ See *Human Rights and Scientific and Technological Developments*, GA Res 3149 (XXVIII), 2201st plenary mtg, UN Doc RES/3149(XXVIII) (14 December 1973).

²⁹⁸ See Kubota, above n 296, 119-119.

²⁹⁹ Ibid.

³⁰⁰ Ibid.

States were disengaged during the drafting process, and seldom did they respond to queries.³⁰¹ Even members of the Sub-Commission on the Prevention of Discrimination and Protection of Minorities, a subsidiary of the former Commission under whose auspices the UN Data Privacy Guidelines were prepared were said to withhold their opinion on studies and reports submitted to them in the interest of 'moving along the agenda'.³⁰²

This is indicative of the lack of enthusiasm at the time for privacy in general and the Guidelines in particular. Resistance to the Guidelines was also shown by UN specialized agencies such as the International Labour Organization (ILO), as well as by the International Criminal Police Organization. An aspect of this resistance was that these organizations had requested exemption from the application of the Guidelines to their operations.³⁰³ Given that these agencies are inter-governmental, where membership is at the State level,³⁰⁴ it may well be that the ideological differences witnessed within the UN were also present in these organizations.

The (data) privacy inattention effect is also latent in the way how the substance of the data privacy instruments was crafted. In the case of the Data Privacy Guidelines for instance, relatively better and privacy protective initial versions of the Guidelines were later substantially watered-down. A number of rules or principles embodied in the Secretary-General's 1974 Report, which later partially were integrated with the guidelines prepared by Joinet,³⁰⁵ are absent in the current version. Of principles included in the initial version of the Guidelines include the following: stringent requirements for collection of personal information including prohibition of collecting hearsay and subjective information, legal responsibility of computer manufacturers and software developers regarding security of information systems, specific rules on damages and penalties for violation of the rules, requirement for judicial control of automated decision-making, extraterritorial protection and specific obligations of national data protection authorities which included monitoring developments in the technology sector that may affect the right to

³⁰¹ Ibid, 119.

³⁰² See Kathrine Brennan et al, 'The Fortieth Session of the UN Sub-Commission on Prevention of Discrimination and Protection of Minorities' (1989) 11 *Human Rights Quarterly* 295, 312.

³⁰³ See Wayne Madsen, *Handbook of Personal Data Protection* (Macmillan Publishers, 1992)194.

³⁰⁴ Note, however, that the ILO's Governing Body has a unique tripartite membership structure in which employer and employee representatives participate alongside States. See *ILO Constitution* (1919) art 7.

³⁰⁵ Note that Louise Joinet, appointed by the Sub-Commission as a Special Rapporteur, drafted the final version of the Guidelines, after replacing Nicole Questiaux. The latter was responsible for the preparation of the initial reports and studies for the Sub-Commission that eventually led to the UN Data Privacy Guidelines. See Edward Lawson (ed), *Encyclopedia of Human Rights* (Taylor & Francis, 2nd ed, 1996) 1195-1196.

privacy.³⁰⁶ These norms and principles were later eliminated from the final version of the Data Privacy Guidelines. There is no reason to suggest that these rules were rolled back due to political compromises, not least because the Guidelines were soft law. A more plausible conjecture then is that the overall lack of attention to the privacy is liable. Had there been a firm commitment to introduce a robust data privacy instrument, would these rules have been eliminated?

In the ultimate analysis, the human rights origins of the UN data privacy framework, added to the ideologically divided era during which the process was set in motion, appeared to have opened the door for ideological factors to negatively influence the present shape of the UN data privacy framework. Ideological differences, and the need for political compromises needed to narrow these differences, appear to be the primary factor for the current normatively and institutionally weak framework for the protection of data privacy. In considering the lack of express reference to the right to privacy in the Helsinki Final Act – a document often seen as lessening the Cold War, one wonders if the right to privacy was particularly disadvantaged. The Act, which of course is not a legally binding instrument, enshrines the agreement of States to respect human rights particularly freedom of expression, freedom of religion and other group rights but privacy rights are omitted.³⁰⁷

Indeed, while the signing of the Helsinki Final Act has had an impact in ‘shoring up’ the human rights agenda, its signing by the Soviets was merely of symbolic gesture, rather than a genuine commitment to human rights.³⁰⁸ This observation corresponds to the instances of ‘drafting inattention’ that plagued the human right to privacy highlighted in chapter 1. But more generally, it reinforces the point that the UN has generally been reluctant in consistently considering the issue of whether new threats to privacy dictate an international legal response. The UN has not pursued a clear and coherent approach when it comes to international protection of (data) privacy. While the ongoing UN privacy discourse increasingly adopts a unifying approach that touches on important aspects of privacy, including data privacy, it still exhibits a level of selectivity in its choice of themes, as shall be examined in chapter 4. The UN approach so far has been haphazard and piecemeal that cumulatively left a patchy international data privacy regime in contrast with progressive regional approaches in Europe, and recently in Africa.

³⁰⁶ See *Uses of Electronics which may Affect the Rights of the Person and the Limits which Should be Placed on such Uses in a Democratic Society*, Report of the UN Secretary-General, UN Doc E/CN.4/1142 (31 January 1974) [320] cum [92].

³⁰⁷ *The Helsinki Final Act: Conference on Security and Cooperation in Europe Final Act* (OSCE, 1 August 1975) sec VII.

³⁰⁸ See Rosemary Foot, ‘The Cold War and Human Rights’ in Melvyn Leffler and Odd Westad (eds), *The Cambridge History of the Cold War* (Cambridge University Press, Vol. 3, 2010) 459.

III FALLING INTO DISUSE: EXCESSES AND GAPS OF UNITED NATIONS' DATA PRIVACY FRAMEWORK

Propelled mainly by historical factors outlined above, the present regime for the protection of data privacy exhibits a number of normative and institutional gaps. This section examines the scope of data privacy protection under the UN framework, and highlights two of its major weaknesses: (a) problems of substance and approach; (b) problems of institutionalization. A caveat is, however, in order: since existing rules are scattered across various instruments, the discussion in this section is limited to those that are universal in scope, and those containing key UN data privacy norms.

A Problems of Substance and Approach

Normative weaknesses of the present framework relate mainly to three issues. One is the 'problem of normative dispersion' in that existing data privacy norms are a mere patchwork of rules dispersed across various instruments. As shall be shown below, this has significantly lessened their effectiveness and accessibility. Second, existing data privacy norms are embodied in a set of exceedingly soft law instruments which not only reduced their normative strength but also played a role in their lower practical utility. While soft legalization is an effective tool of international lawmaking, its overuse in the data privacy field had little value or has been counterproductive. Third, existing UN data privacy rules are normatively inferior to their regional counterparts, because of which the desirable level of protection has been minimal. Not only were more protective norms watered-down during the drafting process but also that lack of proper attention at the UN to data privacy over the past four decades has rendered existing standards obsolete. Particularly so in the light of significant developments in the field of data privacy law at national and regional levels since.

1 Dispersive Approach to Data Privacy

Present international data privacy norms are scattered across various sets of instruments. Not only are these norms scattered in various instruments but also that each instrument is often detached from other related instruments. One finds no unified and comprehensive UN instruments that regulate the processing of personal information and, as such, protect data privacy. Most norms appear to have come about under specific circumstances, and hence in insolation with already existing norms. This patchwork of rules is a result of piecemeal, uncoordinated and sporadic approaches to data privacy pursued by the UN and its agencies. It can also be attributed to the general apathy towards issues of privacy, as highlighted in chapter 1, that has been rampant in the UN standard setting processes in the past few decades. What follows considers this pervasive fragmented approach to data privacy at the UN. Based on their legal nature and scope, diffuse UN data privacy

instruments/norms can be grouped into four categories: 'universal/general', 'domain/subject-specific', 'agency-level' and 'human rights instrument-based' data privacy instruments and/or norms.

(a) Universal/General Standards

The UN Data Privacy Guidelines are the primary general data privacy instruments with a universal scope of application. The Guidelines stipulate a set of principles of information practices as 'minimum guarantees' to be enacted by States and international organizations.³⁰⁹ These guarantees are basically high-level principles of data privacy comparable to most domestic and regional data privacy principles. Key data privacy principles contained in the Guidelines include: principles of 'lawfulness and fairness', 'accuracy', 'purpose specification', 'interested-person access', 'non-discrimination' and 'security'.³¹⁰ The Guidelines further provide for rules on transborder data flows between countries with 'comparable' data privacy safeguards and on the need for an independent data protection authority.³¹¹ A hallmark of the Guidelines is that the 'procedures' for the implementation of these guarantees is left to States so long as they are based on the Guidelines' 'orientations'. Added to the soft law nature of the Guidelines – and hence lack of binding force, this leaves a significant latitude to States in translating the Guidelines into domestic legislation. As shall be noted later in this chapter, this broad latitude has lent weight in the ultimate disregard of the Guidelines by almost all States in domestic lawmaking.

Other more general UN Internet governance instruments also fall in this category. A set of Conference outcome documents adopted following the World Summit on Information Society (WSIS) held in 2003 and 2005, are one such example that slightly touch on data privacy. These instruments, however, address data privacy only peripherally and indirectly. One finds mere affirmation of privacy rights, and no data principles are articulated as such. The Geneva Declaration of Principles, for instance, simply affirms the need to protect 'data and privacy'.³¹² Similarly, the accompanying document – the Geneva Plan of Action – merely 'encourages' research in the field of e-health to ensure respect for the right to privacy especially in the context of international transfer of health data.³¹³ The Tunis Commitment – a final act of the Tunis WSIS of 2005 – does not make any reference to privacy at all but its accompanying document, the Tunis Agenda, emphasises the need for the protection of 'personal information, privacy and data'.³¹⁴ Beyond the peripheral – and at points, inaccurate references such as 'data and privacy', these UN instruments do not

³⁰⁹ UN Data Privacy Guidelines above n 29, part A.

³¹⁰ Ibid, arts 1-5, 7.

³¹¹ Ibid, arts 8-9.

³¹² *The Geneva Declaration of Principles* (WSIS, 12 December 2003) [35] cum [58].

³¹³ *The Geneva Plan of Action* (WSIS, 12 December 2003) [18] cum [12(f)].

³¹⁴ *The Tunis Agenda for the Information Society* (WSIS, 18 November 2005) [39] cum [42].

engage with relevant UN instruments that deal with (data) privacy, including the UN Data Privacy Guidelines.

(b) Domain/Subject-specific Standards

The second category of the UN data privacy framework includes ‘subject/sector-specific’ data privacy norms/instruments. A more recent example is ‘UN Fundamental Principles of Official Statistics’, which stipulates a set of principles that must be observed in undertaking official statistics. Of these principles, the relevant data privacy principle is provided in Principle 6 which states that ‘individual data collected by statistics agencies must be strictly confidential and used exclusively for statistical purposes’.³¹⁵ Another instrument is the ‘UN Principles and Guidelines on Access to Legal Aid in Criminal Justice Systems’, whose relevant data privacy principle provides that ‘privacy and personal data protection’ of children must be protected in the course of criminal proceedings and appropriate law must be enacted to that effect.³¹⁶ That these UN Principles address specific subjects, and nuanced in scope means they are not typical data privacy instruments.

(c) Agency-level Standards

Data protection and information disclosure policies of specialized and related agencies of the UN belong to the third category of the UN data privacy framework. These policies, particularly the data protection policies, are introduced in response to the request by the UNGA to pay due attention to technological developments and the impact that they pose to human rights.³¹⁷ The UN Data Privacy Guidelines also provide the ‘enabling law’ for the adoption of agency-level data protection policies by ‘governmental international organizations’ based on the Guidelines for internal and external purposes.³¹⁸

UN instruments in this category are of different variety in terms of their scope and as well as legal nature. While some are directly framed in human rights language – thereby reflective of the human rights genesis of the UN data privacy system, others have the common data privacy tone. Whereas some are sector-specific, a good case in point being the ILO Code of Practice, explained further below. The more recent intra-agency data protection policies, as shall be considered below, are notably reflective of European data privacy standards.

Intra-agency data protection policies: several UN agencies have adopted agency-level data protection instruments in the past few years. Examples in this regard are the policies adopted by the United Nations Higher Commission for Refugees (UNHCR)

³¹⁵ See Fundamental Principles of Official Statistics, above n 31.

³¹⁶ See *UN Principles and Guidelines on Access to Legal Aid in Criminal Justice Systems*, GA Res 67/187, 60th plenary mtg, UN Doc A/RES/67/187 (20 December 2012) [54] cum [58(b)].

³¹⁷ See *The Use of Scientific and Technological Developments in the Interest of Peace and Social Development*, GA Res 3150 (XXVIII), 2201st plenary mtg, UN Doc RES/3150 (XXVIII) (14 December 1973) [5].

³¹⁸ See UN Data Privacy Guidelines, above n 29, part B.

and the International Organization for Migration (IOM). The UNHCR Policy explicitly states that it is adopted as a response to the UN Data Privacy Guidelines which require, as noted above, international-governmental organizations to apply the Guidelines in the course of their operations, albeit with some adjustments.³¹⁹ The Policy embodies widely accepted data privacy principles and data subject rights with some level of details.³²⁰ The IOM Data Protection Manual is the other internal instrument developed by a related UN agency, which – like the UNHCR Policy – envisages progressive data privacy standards.³²¹ But unlike the UNHCR Policy, the UN Data Privacy Guidelines do not appear to be its inspirations. Adopted a few years after the ICPDPC made the initial call for an international data privacy instrument, the Manual sought to contribute to the ‘discussion’ (re)started by the Conference.³²²

With the increasing global attention to (data) privacy, it is likely that other UN agencies that control and process vast personal information in the course of their operations such as the World Health Organization may develop similar intra-agency policies. In a more recent attempt to create harmonization among these agency-level instruments, UN High-Level Committee on Management has adopted a set of data privacy principles as ‘basic framework’ for UN agencies in the course of processing personal data.³²³ But the intra-agency scope of these policies reduces their value in international law.

Information disclosure policies: a related development is that some of these agencies have adopted information disclosure policies that further complement the data protection policies. While mainly aimed to facilitate access to information retained by the agencies, information disclosure policies often embody ‘exceptions’ to disclosure when the requested access to personal information would invade ‘privacy interests’ of concerned persons. The Information Disclosure Policy of the United Nations Development Program (UNDP), for instance, prohibits disclosure of ‘personal information’ relating to ‘staff and consultants’ of the UNDP, including information pertaining to ‘personal medical information and personal communications’.³²⁴

But, on top of their intra-agency and hence narrow scope, these policies often provide for circumstances where the impinged disclosure could be permitted for

³¹⁹ Ibid; Cf UNHCR Data Protection Policy, above n 32, [1.1].

³²⁰ See UNHCR Data Protection Policy, above n 32, sec 2-7.

³²¹ See ‘Data Protection Manual’ (IOM, 2009).

³²² See Richard Perruchoud, ‘Foreword’ in IOM Data Protection Manual, Id; Cf Montreux Declaration, above n 40.

³²³ See ‘Personal Data Protection and Privacy Principles’ (UN High-Level Committee on Management, 11 October 2018).

³²⁴ See ‘Information Disclosure Policy’ (UNDP, 1996) (as amended in 2017) art 15(b). Cf ‘Information/Document Access Policy’ (ITU, 2016) art 3.1; ‘Directive on Information Disclosure’ (WFP, 2010) art 3(iv).

overriding ‘public interest’ reasons regardless of risks of privacy invasion.³²⁵ Moreover, the ‘privacy exceptions’ often are couched in a manner less reflective of a genuine desire to protect privacy rights. For instance, UNDP’s policy prohibits disclosure because it would ‘violate his or her rights, or invade his or her privacy’, thereby suggesting that privacy is worthy of protection not because it is a ‘right’. This seems to have the objective of distancing the organization from any obligation, in human rights terms, which would have otherwise been the case had the privacy been stated in human rights language.³²⁶ These limit the potential of internal information disclosure policies of UN agencies in serving as a source of international data privacy law.

Domain-specific instruments: A variant of agency-level UN data privacy instruments/norms takes the form of domain/subject-matter policies. For instance, the ILO – a specialized agency of the UN – has taken steps in adopting a ‘non-legal soft law’ instrument on the data privacy of workers.³²⁷ The ‘Code of Practice on the Protection of Workers’ Personal Data’ particularizes widely accepted data privacy principles and data subject rights to the labour sector.³²⁸ The aim of the Code is to provide ‘guidance’ to States in enacting national legislation, and to other actors to take them into account while preparing work-related agreements.³²⁹ Although adopted 7 years after the UN Data Privacy Guidelines, the Code of Practice makes no reference to the Guidelines but to other regional instruments such as the EU Data Protection Directive and the CoE Data Protection Convention.³³⁰ This is one of the instances that reflect not only the sectoral and disjointed nature of UN efforts in the field of data privacy, but also that UN has been complicit in undermining its own instruments. But as shall be highlighted later in this chapter, the ILO Codes of Practice have had some significance, particularly recently, in shaping judicial decisions at the regional level in relation to worker data privacy.

³²⁵ Ibid, art 16.

³²⁶ It is worth pointing out that whether international organizations, including inter-governmental organizations such as UN specialized and related agencies, are bound by international human rights has been part of the broader ‘human rights and non-State actors’ debate. Recent proliferation of agency-level data privacy instruments is primarily driven by, as noted earlier, the call made in the UN Data Privacy Guidelines, but it may arguably be associated with their positive obligation in international human rights law. See more in ch 5.

³²⁷ In discussing the diversity of soft laws in international lawmaking, Chinkin refers to ‘Codes of Practice’ as ‘non-legal soft law’, as a subcategory of soft law. See Christine Chinkin, ‘Normative Development in the International Legal System’ in Dinah Shelton (ed), *Commitment and Compliance: The Role of Non-Binding Norms in the International Legal System* (Oxford University Press, 2000) 28.

³²⁸ ‘Code of Practice on the Protection of Workers’ Personal Data’ (ILO, 1997).

³²⁹ Ibid, [2].

³³⁰ Ibid, preamble [1].

(d) Human Rights Instrument-based Standards

In the fourth category, one finds data privacy principles embedded in some UN human right treaties. A good case in point is the CRPD. The Convention, for instance, requires State parties to ensure protection of ‘personal, health and rehabilitation information of persons with disabilities’.³³¹ Details of this proviso are furthered in a separate provision.³³² While requiring State parties to collect reliable information for purposes of formulating sound policies in the interest of disabled persons, the Convention attaches a number of requirements that must be complied with in the course of collecting and maintaining such statistics. It requires such processes to (i) comply with data privacy principles to ensure privacy and confidentiality of the data; and (ii) comply with internationally accepted norms and principles.³³³ The first requirement latently assumes the existence of data privacy law in State parties – and if there is none already, such law to be adopted. It is interesting to note that first general proviso is provided alongside the underlying privacy provision of the Convention, which is verbatim to Article 17 of the ICCPR.³³⁴

To an extent, the convention on enforced disappearance also touches on data privacy themes although it does not provide for a specific right to privacy like the CRPD. The Convention addresses (data) privacy themes in two levels. At a higher level, it provides that ‘collection, processing, use and storage of personal information including medical and genetic data’ of a disappeared person shall not infringe human rights, fundamental freedoms or human dignity.³³⁵ The ‘purpose specification principle’ is implied when it states that personal medical and genetic data collected or transmitted for the purpose of searching a disappeared person must not be used or made available for a different purpose.³³⁶

The value of these data privacy provisions is the potential of inspiring domestic data privacy legislation, perhaps one with specific focus on persons covered in the respective instrument. But they are another manifestation of the fragmented and incoherent UN approach to data privacy.

Data privacy themes, in human rights language, figure also in a series of instruments adopted by the UNESCO. Indeed, one mandate of the UNESCO is to ‘further universal respect for human rights’,³³⁷ and this has translated into several instruments relating to data privacy. Of UNESCO instruments, relevant to data privacy is the Universal Declaration on Human Genome and Human Rights of 1997.

³³¹ CRPD, above n 112, art 22 (2).

³³² Ibid, art 31.

³³³ Ibid, art 31(1).

³³⁴ Ibid, art 22(1).

³³⁵ *International Convention for the Protection of All Persons from Enforced Disappearance*, opened for signature 6 February 2007, 2716 UNTS 3 (entered into force 23 December 2010) art 19(2).

³³⁶ Ibid, art 19(1).

³³⁷ *UNESCO Constitution* (16 November 1945) (as amended) art I (1).

The Declaration, endorsed later by the UNGA in 1998, aims at safeguarding, among other human rights, privacy of genetic data in the course of genetic research.³³⁸ It embodies a number of data privacy principles. It, for instance, implies the 'principle of lawful collection' when it mandates the need to solicit the consent of data subjects in the course of collecting and processing genetic information.³³⁹ The principle of 'data security' is patent in the Declaration where it requires that genetic data collected or being processed must be kept confidential, and any limitation thereof must be imposed only by law which is consistent with international human rights law.³⁴⁰

The Declaration has further been reinforced by another instrument, the 'International Declaration on Human Genetic Data' of 2003. The Declaration not only embodies broader data privacy principles but also addresses the right to privacy more directly. On top of emphasising the need for obtaining 'prior, free and informed consent' in the course of collecting and processing genetic data, it provides principles of 'purpose specification principle', 'use limitation principle', 'principle of data security', 'data subject participation principle' and 'principles of data quality'.³⁴¹ 'Privacy and confidentiality' are also touched on under Art 14 of the Declaration.

A latest UNESCO instrument in the field of data privacy is the Universal Declaration on Bio-ethics and Human Rights, adopted by the General Conference in 19 October 2005. This Declaration aims to protect human rights in medical research and stipulates universal ethical principles that States must translate into domestic legislation and to provide guidance to non-State actors. Of the ethical principles, one is that confidentiality of personal medical data shall be respected, and no data shall be used or disclosed for purposes than it was initially collected or consented for, except in accordance with international human rights law.³⁴² The latter phrase appears to invite the application of the widely agreed three-part tests of legality, necessity and legitimate aim in assessing requests for disclosure of personal data. But despite the framing of UNESCO instruments with human rights terms, the legal softness, and of course, the apparent nuanced scope, reduce their place in the international law of privacy.

(e) Perils of A Fragmented Approach

As the above survey of the current UN data privacy framework reveals, normative dispersion is prevalent. This fragmented approach to data privacy is problematic on many levels. A more obvious concern is that it results in redundancy of efforts when several UN bodies are involved not only in setting these norms but also in overseeing them. As will be considered later in this chapter, normative

³³⁸ *Declaration on the Human Genome and Human Rights* (UNESCO, 11 November 1997) preamble.

³³⁹ *Ibid*, art 5.

³⁴⁰ *Ibid*, arts 7 and 9.

³⁴¹ *International Declaration on Human Genetic Data*, (UNESCO, 16 October 2003) arts 8-9, 13, 15-16.

³⁴² *Universal Declaration on Bio-ethics and Human Rights* (UNESCO, 19 October 2005) arts 7 and 9.

fragmentation creates institutional dispersion, which in turn weakens the overall effectiveness of the UN data privacy framework in enhancing the protection of (data) privacy. The problem of normative fragmentation is, however, different from the sectoral and domain-specific approach to data privacy regulation, or at least in the form common in the EU data privacy regime.

The EU, which has the most advanced regime for the protection of data privacy, regulates the matter under various instruments. In addition to the General Data Protection Regulation (GDPR), there are sectoral data privacy instruments. A typical example is the e-Privacy Directive which particularizes data protection rules to the communications sector.³⁴³ Another example is the Data Protection Directive in the field of criminal proceedings and law enforcement which extends protection of data privacy to victims, suspects and witnesses of crimes.³⁴⁴ Processing of data by EU institutions is also regulated under a separate Directive.³⁴⁵ But, these instruments operate in a coherent and consistent manner, and that each is not completely isolated from the other. The dispersive approach is deeply fragmentary and almost each instrument is disjointed from the others.

Lack of a unified and coherent framework weakens the potential of the UN norms in ensuring uniform protection of data privacy. This is particularly the case when normative dispersion makes applicable rules invisible to relevant adjudicative bodies and data subjects. The HR Committee, for instance, has never refereed to either the UN Data Privacy Guidelines or other data privacy instruments in examining relevant individual communications and periodic reports of States. The lack of a clear and accessible framework of rules has the potential to bury even the patchy rules that guarantee rights of individuals from those who could oversee or invoke them in practice. The problem is that almost every fragmentary data privacy standard does not carry binding legal force, as shall be discussed below.

2 Problem of (Over) Soft Legalization

The second normative weakness of the UN data privacy regime flows from its exceedingly soft law approach. As shown in the discussion above, not only are data privacy norms diffuse but also that they are carried in soft law instruments. Except for the human right treaties noted above, almost all UN instruments are soft law instruments. The obvious concern with ‘soft legalization’ is that States are at liberty

³⁴³Directive (EC) 2002/58 of the European Parliament and of the Council of 12 July 2002 on the Protection of Privacy in the Electronic Communications Sector [2002] OJ L 201/37.

³⁴⁴Directive (EU) 2016/680 of the European Parliament and of Council of 27 April 2016 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 Offenses or the Execution of Criminal Penalties and on the Free Movement of such Data [2016] OJ L 119/89.

³⁴⁵Regulation (EU) 2018/1725 of the European Parliament and of Council of 23 October 2018 on the Protection of Natural Persons with regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices and Agencies and on the Free Movement of such Data [2018] OJ L 295/39.

simply to ignore these non-binding rules. At a more general level, excessive soft legalization threatens the international legal order. As Handl et al comment, there is often a concern that excessive soft legalization pursued due to current exigencies may weaken the international legal order.³⁴⁶ In part, the generally patchy structures of the international law of privacy are results of soft law approach to data privacy.

Excessive soft legalization also gives rise to practical concerns. A primary concern lies not just on the lack of legally binding force but the resultant loss of value in practice. As will be considered in chapter 5, soft law is the most pertinent candidate in reimagining the right to privacy in international law. But the excessive use of soft law tends to reduce the possibility of its rules in being implemented at the local level. Precisely this is the problem of the UN data privacy system due to its overly soft approach to legalization. The concern is compounded by the lack of a robust institutional machinery to oversee the implementation of soft rules by States. Where there are monitoring bodies, they are handicapped by structural problems, including lack of adequate monitoring authority. We return to this point later in this chapter.

As alluded to above, the primary concern with excessive soft legalization is that owing to the non-binding nature of soft laws, their legislative goal may not necessarily be met in practice. This, in turn, reduces their practical utility. An illustrative example, in this regard, is the practical utility of the UN Data Privacy Guidelines in meeting their objective of serving as a 'model law'. The overarching aim of the Guidelines is to provide a prototype for national-level legislation with a minimum set of data privacy guarantees. In adopting the Guidelines, the UNGA merely 'requested' governments on the one hand, and governmental, inter-governmental and non-governmental organizations on the other hand, to take into account and respect the Guidelines in their domestic legislation and in the course of their activities respectively.³⁴⁷ There is, however, little evidence to suggest that the Guidelines have actually been used as benchmarks in several countries that enacted data privacy legislation since the 1970s and 2000s. In fact, it is only rarely that even instruments adopted within the auspices of the UN invoke the Guidelines as an enabling universal data privacy instrument.

Studies have shown that the EU Data Protection Directive, adopted five years after the Guidelines, instead served as a benchmark instrument for national data privacy laws in Asia, Africa and Latin America.³⁴⁸ The surge in data privacy legislation since the early 2000s is mostly dictated by the 'adequacy' requirement of the EU Data Protection Directive. Countries with trade relations with the EU are indirectly forced

³⁴⁶ Guther Handl et al, 'A Hard Look at Soft Law' (1988) 82 *Proceedings of the Annual Meeting of the ASIL* 371, 377.

³⁴⁷ UN Data Privacy Guidelines, above n 29, [4-5].

³⁴⁸ See Graham Greenleaf, 'Data Protection in A Globalized Network' in Ian Brown (ed), *Research Handbook on Governance of the Internet* (Edward Elgar, 2012) 231.

to adopt a national data protection law that is proximate to European standards.³⁴⁹ To be sure, accession to the CoE Data Protection Convention is one of the factors that must be taken into account in the ‘adequacy’ decisions of the EU under the new Data Protection Regulation.³⁵⁰ Therefore, the recent proliferation of data privacy law worldwide is not, for the most part, a response to the rather universal UN Data Privacy Guidelines. Perhaps one exception is that the Guidelines, along with other regional instruments, were ‘overtly’ taken into account by the Spanish Constitutional Court in its landmark ruling of 2000 that consolidated the ‘right to data protection’ as a fundamental right.³⁵¹

One may well say that other soft law instruments, particularly the OECD Privacy Guidelines, have served as model law in a number of countries.³⁵² And of course, data privacy legislation in some OECD member States has been inspired by the Guidelines.³⁵³ But, this has to be considered in context. The successes of OECD instruments have a lot to do with the small membership of the organization, and the general ideological convergence among member States.³⁵⁴ This convergence, added to the principal ‘economic’ institutional goals of the OECD itself and its privacy guidelines,³⁵⁵ appears to have paved the way for the wider acceptance of the Guidelines in member States. On the contrary, the UN is a home for diverse panoply of States from all corners of the world that exhibit deep ideological, socio-economic and political divisions. In the face of such divergence – more so in an area like data privacy that has human rights at its core, States are free to ignore following the UN Data Privacy Guidelines. At the time of writing, over 120 countries have adopted, or are considering some form of bill largely based on European standards.³⁵⁶ This leaves around 70 States still without any data privacy law proper although they are required, or expected, to adopt one per the UN Data Privacy Guidelines.

³⁴⁹ For the influence in Africa, see Alex Makulilo, ‘The Context of Data Privacy in Africa’ in Makulilo (ed), above n 68, 18-19.

³⁵⁰ See *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data* [2016] OJ L 119/1, Recital 105.

³⁵¹ See Fuster, above n 162, 179, citing *STC 292/2000*, de 30 de noviembre de 2000 del Tribunal Constitucional.

³⁵² See *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD, 23 September 1980) (as updated in 2013).

³⁵³ See, e.g., *The Australian Privacy Act 1988* (Cth) preamble. Cf ‘Explanatory Memorandum Privacy Bill 1988’(Cth) [1988].

³⁵⁴ See Michael Kirby, ‘The History, Achievement and Future of the 1980 OECD Guidelines on Privacy’ (2011) 1 *International Data Privacy Law* 6, 11 (Note that the author was chair of the expert committee that drafted the OECD Privacy Guidelines).

³⁵⁵ *Ibid*, 8

³⁵⁶ See, e.g., Graham Greenleaf, ‘Global Analysis of Data Privacy Laws and Bills’ (2017) 145 *Privacy Laws and Business International Report* 14, 14-18, 24.

The drafting of the UN Data Privacy Guidelines was, of course, influenced by European data privacy instruments, especially the CoE Data Protection Convention, which was adopted in 1981 while the Guidelines were still in gestation. What is more, the primary drafter of the Guidelines, Joinet, was, as noted above, a French data protection official and was involved with the drafting of data protection instruments of both CoE and OECD;³⁵⁷ so European marks in the Guidelines were inevitable. But the Guidelines do also embody some privacy-protective rules that are not to be found in European instruments, or even OECD Guidelines. For instance, the Guidelines' 'principle of accuracy' requires data controllers to make regular accuracy checks, the 'principle of purpose specification' requires publicity of the purpose of the data collection/processing, the 'principle of interested third party access' requires the data subject to be informed of the recipients of data concerning him, and more importantly the Guidelines mandate the application of the principles to International organizations.³⁵⁸

If States especially those that pursued the European approach really had the aim of introducing more human rights friendly instrument, the UN Data Privacy Guidelines would have been a good starting point, or at least an additional benchmark. Arguably, the primary legislative motive rather was more economic, or perhaps of mere capitulation. But the soft law nature of the Guidelines, added to the economic incentives of taking the European path, seems to have played a role in limiting the practical utility of the Guidelines.³⁵⁹

Yet not only did the Data Privacy Guidelines fail in their mission to serve as a 'model law' for national legislation but also regional instruments enacted subsequently do not appear to consider them. The EU Directive of 1995, and its recent replacement, the Regulation, do make reference to CoE Convention but not to the Guidelines which are actually universal in scope.³⁶⁰ The Asia-Pacific Privacy Framework follows suit, and notes that it rather relied upon the OECD Privacy Guidelines.³⁶¹ The absence of any reference to the UN Data Privacy Guidelines is significant given that they are universal instruments well positioned to serve as enabling law for regional and national legislation. Whether this disregard of the Guidelines was a deliberate (in)action is unclear, but it is clear that it played a role in further undermining the practical utility of the Guidelines and puts them off the global map of data privacy lawmaking. This does not, however, provide the complete explanation for the high isolation of the Data Privacy Guidelines. As shall be considered later in this chapter, the UN and its relevant bodies also contributed in throwing the Guidelines into disuse.

³⁵⁷ See his profile at <<http://bit.ly/2lwQFiL>>; see also Kirby, above n 354, 9.

³⁵⁸ UN Data Privacy Guidelines, above n 29, [2-4] cum part B. For more on this, see Bygrave, above n 69, 52-53.

³⁵⁹ Of a related view, see Bygrave, above n 70, 53.

³⁶⁰ See, e.g., GDPR, above n 350, recital 105.

³⁶¹ See *APEC Privacy Framework* (2014) preamble, [5].

The UN's exceedingly soft law approach further cast on the extent of attention given to the privacy agenda. Uninterrupted but again disjointed resort to soft legalization, and without ever making efforts towards progressive development of international data privacy law is problematic. More so when one considers the established pattern of gradual transition to hard law in other areas of international regulation. Soft law often serves as a precursor to and a way of short-circuiting hard law.³⁶² In line with this tradition, several UN soft law instruments including 'Guidelines' have been translated into – or have formed an important part of – subsequent hard laws in the same area. An example is the 'Guidelines on Environmental Impact Assessment of 1987' which were later incorporated substantially into the 'Convention on Environmental Impact Assessment in a Trans-border Context of 1991'.³⁶³ This has not materialized in the case of the Data Privacy Guidelines. On the contrary, what we have now – as noted have – is a partially watered-down 'lite' version of the Guidelines.

At times, the limited practical utility of the Data Privacy Guidelines – and equally other relevant data privacy instruments, is attributed to the timing of the adoption of the Guidelines. This viewpoint holds that the Guidelines were adopted (in 1990) long after the OECD Privacy Guidelines (1980) and the CoE Data Protection Convention (1981) had served as benchmark for national legislation in many countries.³⁶⁴ In short, that the Guidelines were late-comers means not much domestic legislation left to inspire. But two obvious reasons cast doubt on this conclusion. First, owing to the limited memberships of both the OECD and CoE, there were over a hundred States (probably including some European States) without a fully-fledged data privacy law by the time the Guidelines were adopted. And, the doors for accession to CoE Data Protection Convention to non-member States opened up only recently, in 2008.³⁶⁵ That OECD Privacy Guidelines are also soft law instruments meant that its members are at liberty not to follow the Guidelines, but they did (mostly) in practice anyway.³⁶⁶ Perhaps, the generally wider reception of the OECD Privacy Guidelines was also facilitated by other structural-institutional push factors, including the underlying Convention that created the organisation. Kirby notes, in this regard, that the Privacy Guidelines 'on the whole, have been taken seriously by the countries that are parties to the OECD Convention'.³⁶⁷

Second, most data privacy pieces of legislation enacted since the late 1990s and early 2000s, especially in Africa and Asia as well as partly in Latin America, as noted above, are largely influenced by the EU Data Protection Directive of 1995, which is

³⁶² See Leo Gross, *Essays on International Law and Organization* (Springer, Vol. I/II, 2014) 176.

³⁶³ *Convention on Environmental Impact Assessment in a Transboundary Context*, opened for signature 1 March 1991, 1989 UNTS 309 (entered into force 10 September 1997).

³⁶⁴ De Hert and Papakonstantinou, above n 89, 282.

³⁶⁵ See Committee of Ministers Decision CM/Del/Dec/2008 (2 July 2008) 1031/10.2.

³⁶⁶ Kirby, above n 354, 11.

³⁶⁷ *Ibid.*

more progressive, and detailed in its regulatory patterns, than the OECD Guidelines. Therefore, the 'timing of adoption' argument cannot persuasively explain away why the UN Data Privacy Guidelines failed in spurring data privacy legislation. Instead, a host of factors, including the soft law nature of the Guidelines is to blame for their resultant limited impact.

Overall, added to the low normative quality of UN data privacy standards considered in what follows, the excessive soft law path taken by the UN has significantly limited the practical utility and efficacy of UN data privacy norms globally.

3 Problem of Juridical Quality

The UN data privacy framework has a problem of normative inferiority in contrast with its regional counterparts. This problem of normative quality has two dimensions. First, UN data privacy norms are restricted to generic and high-level provisions. Second, UN data privacy standards are by and large outmoded in comparison to progressive developments elsewhere. What follows considers these two points.

Existing data privacy standards are formulated in a characteristically generic manner. Unlike the regulatory nature of data privacy legislation, present data privacy standards are contained in high-level data privacy principles. The only exception is the recent intra-agency policies of UN specialized and related agencies, which relatively reflect the substance of modern data privacy instruments. A common challenge associated with the overly brief and general nature of, for instance the UN Data Guidelines, opens the door for conflicting interpretations.³⁶⁸ This is exacerbated by the lack basic interpretative aides in the Guidelines. This in turn impacts transposition into law by States of the principles of the Guidelines and create divergent implementation of the rules. Basic weaknesses of this sort are no less significant in causing uncertainties in the application of the Guidelines. But more generally, the high-level nature of UN data privacy instruments means that intricate regulatory details of data privacy law will not be provided. The data privacy framework being less holistic would mean that legislative goals will not be met.

A similar observation applies in equal force to the other UN data privacy instruments discussed in section III. In relation to genetic data for example, the CoE has a progressive regime than relevant UNESCO instruments. It regulates the matter through a binding instrument, the Convention on Human Rights and Bio-medicine of 1997.³⁶⁹ The Convention, which currently has 29 State parties, recognizes the right

³⁶⁸ See Keller, above n 86, 350.

³⁶⁹ *Convention on Human Rights and Bio-medicine*, opened for signature 4 April 1997, 164 ETS (entered into force 1 December 1999).

to privacy in the context of health data and envisages grounds of limitation identical to ones provided in Article 8(2) of the ECHR.³⁷⁰ The Convention further requires State parties to pass implementing domestic legislation and to provide remedial measures such as injunctions, compensation and even sanctions.³⁷¹ The Convention is elaborated in additional protocols that touch on data privacy in the context of biomedical research and genetic testing.³⁷²

The second aspect of juridical quality is that UN data privacy norms have now become obsolete in the light of significant developments worldwide. Modern data privacy principles, data subject rights and the corresponding obligations of data controllers, processors and data protection authorities that evolved over the years are absent in many of UN instruments. This concerns also those UN instruments introduced relatively recently. Little reforms have occurred at the UN to revitalize already existing norms in light of new developments in the digital age, and to make them fit for purpose. Not only is legislative reform lacking but also progressive development through the existing but dispersed institutional arrangements.³⁷³ This stands in stark contrast to the continued reform introduced in most regional systems, including the EU, CoE and even the African Union (AU) which has recently unveiled a comprehensive data protection instrument.³⁷⁴ The European data privacy framework has particularly been under continuous reviews that introduced a number of progressive data privacy standards.³⁷⁵

With no major reforms so far, and uncertain future reforms in the horizon, it is safe to state that the UN framework especially the Data Privacy Guidelines are slightly 'obsolete' as they stand.³⁷⁶ In the ultimate analysis, the fact that the UN data privacy framework is already outmoded compared to European law means that its role in shaping the progressive development of international law in the area of data privacy is limited. The pending UN discourse on right to privacy touches on data privacy themes to a degree. But the influence of UN data privacy standards is not to be felt. As shall be examined in chapter 4, substantive elements of Resolutions adopted as part of the discourse bear more of, as they should, European marks of data privacy law.

³⁷⁰ Ibid, art 26 cum art 5.

³⁷¹ Ibid, art 23.

³⁷² See, e.g., *Additional Protocol to the Convention on Human Rights and Biomedicine Concerning Biomedical Research*, opened for signature 25 January 2005, 195 CETS (entered into force 1 September 2007) art 25 cum art 13(2)(iv); *Additional Protocol to the Convention on Human Rights and Biomedicine Concerning Genetic Testing for Health Purposes*, opened for signature 27 November 2008, 203 CETS (entered into force 1 July 2018) art 16 cum art 13(d).

³⁷³ See below on the problem of institutional dispersion.

³⁷⁴ See *AU Convention on Cybersecurity and Personal Data Protection Convention* (June 2014) ch II.

³⁷⁵ See, e.g., GDPR, above n 350, arts 33, 25, 35; see also *Modernized Data Protection Convention*, above n 63.

³⁷⁶ Of a related view, Cristina Casagran, *Global Data Protection in the Field of Law Enforcement: An EU Perspective* (Routledge, 2016) 217.

B Problems of Institutionalization

The dispersive approach to data privacy protection, discussed above, is worsened by deep institutional and structural gaps in the UN data protection framework. The principal setback is the lack of clear institutional arrangements for overseeing the implementation of existing data privacy norms. Owing to the dispersed nature of existing norms, the monitoring responsibility falls on various bodies. The institutional arrangement for the monitoring of existing data privacy rules is as fragmented as the rules are. The other institutional weakness is that these various bodies tasked to monitor scattered information rules lack the requisite monitoring capacity that would allow them to ensure adequate respect for and protection of data privacy. This section considers these two limitations.

1 Institutional Fragmentation

Present institutional arrangements in the UN data privacy framework are devolved among several UN bodies. Data privacy principles embodied in human right treaties, for instance, are overseen by the respective treaty bodies. The Committee on the Rights of Persons with Disability Persons, although yet to apply data privacy principles embodied in the Convention, is responsible for adjudging individual communications, examine periodic reports of State parties and even adopt GCs on relevant provisions of the Convention.³⁷⁷ The UNESCO instruments relevant to data privacy similarly are monitored by the International Bio-ethics Committee and the Inter-governmental Bio-ethics Committee.³⁷⁸ In contrast, the CoE's counterpart to the UNESCO Declarations, the Convention on Human Rights and Bio-medicine, is supervised by a dedicated Steering Committee which further benefits from the 'advisory' role of the ECtHR.³⁷⁹ Indeed, the ECtHR has adjudged several cases that touch upon the Convention were considered, and to that extent, it could be said that provisions of the Convention are also indirectly enforceable by the ECtHR.³⁸⁰

The institutional problem is slightly different when it comes to the UN Data Privacy Guidelines, which leaves matters of implementation to national governments. The 'model law' nature of the Guidelines naturally means that no central monitory body is envisaged. But the soft law nature of the Guidelines, as noted above, makes it easy for States to undermine the requirements of installing a national body to overseeing legislation enacted based on the Guidelines. The former UN Commission on Human Rights had put in place a 'follow-up' procedure by which the Secretary-General

³⁷⁷ See CRPD, above n 112, art 34.

³⁷⁸ See, e.g., Declaration on the Human Genome and Human Rights, above n 338, art 24; see more details at <<http://bit.ly/2mlyFCb>>

³⁷⁹ See Human Rights and Bio-medicine Convention, above n 369, art 29.

³⁸⁰ For a summary of cases where principles of the Convention have been considered, see Pere Vilanova, 'The Right to Privacy in the Case Law of the ECtHR' (Proceedings of the High-Level Seminar on International Case Law in Bioethics: Insight and Foresight, 2016) 21 et seq.

would monitor the implementation of the Guidelines by States and international organizations.³⁸¹ At a practical level, the follow-up procedure was symbolic in that States and international organizations would simply be requested to provide information/updates on the progress of implementing the Guidelines to the Secretary-General, and the latter would prepare reports based on the information so received. What makes this a symbolic procedure is that States or even international organizations would simply report compliance, even without taking any measure. Or at worse, they may not even reply to the requests of the Secretary-General.

While the follow-up essentially was a tentative monitoring mechanism, it still had the potential to push the adoption of domestic law based on the Guidelines' 'orientations'. But the UN had not tapped into this potential, and the procedure was abandoned without any success. Various reports of the Secretary-General suggest that procedure was not taken seriously. A 1998 report, for instance, states that no information has been provided by States as to whether they have translated the Guidelines into national legislation.³⁸² But the Commission decided a year later to terminate the follow-up procedure because 'the applicable guidelines are progressively being taken into consideration by States'.³⁸³ Instead, it instructed the Secretary-General to focus on ensuring the implementation of the Guidelines by relevant UN organs. This comes as a rather striking decision because most data privacy laws adopted in the 1990s, as noted above, including the EU Directive of 1995 are barely based on the UN Data Privacy Guidelines.

It is clear that the 'follow-up procedure' was meant to be a temporary procedure. Little has, however, followed it in terms of creating a proper monitoring body, be it by salvaging existing ones or installing a new one. A more pertinent monitory body, at least for overseeing the UN Data Privacy Guidelines, would have been the HR Committee, regardless of its institutional weaknesses discussed in chapter 1. This is for two reasons. One is that the Committee is responsible for overseeing the ICCPR a major binding multilateral treaty that guarantees the right to privacy to which data privacy is one area of protection. The genealogical link between the Data Privacy Guidelines and the ICCPR, as discussed at the outset, lends weight to this point. The Committee could even justify basing its data privacy jurisprudence on the UN Data Privacy Guidelines by holding that they constitute 'authoritative interpretations' of the ICCPR's privacy provision. As will be considered in the context of post-Snowden

³⁸¹ See *Question of the Follow-up to the Guidelines for the Regulation of Computerized Personal Data Files*, Commission on Human Rights Decision 1995/114 (8 March 1995); see also *Human Rights and the Follow-up to the Guidelines for the Regulation of Computerized Personal Data Files*, Commission on Human Rights Decision 1997/122 (16 April 1997).

³⁸² See *Question of the Follow-up to the Guidelines for the Regulation of Computerized Personal Data Files: Report of the Secretary-General prepared Pursuant to Commission Decision 1997/122* (18 November 1998) [5].

³⁸³ See *Human Rights and the Follow-up to the Guidelines for the Regulation of Computerized Personal Data Files*, Commission on Human Rights Decision 1999/109 (28 April 1999).

UN Privacy Resolutions in chapter 4, the ‘authoritative interpretation’ argument draws from earlier doctrinal arguments that the UDHR is an ‘authoritative interpretation’ of the UN Charter’s human rights provisions – and hence creates binding legal obligations against States.³⁸⁴ That the UN Data Privacy Guidelines are adopted through the Resolutions of the UNGA, like the UDHR, the ‘authoritative interpretation analogy’ seems plausible.

Second, the Committee has taken steps to embrace data privacy principles, to some degree, through its GC 16 and concluding observations, as discussed in chapter 1. These principles are not, however, articulated fully and as such are incomplete. The UN Data Privacy Guidelines would have assisted by supplementing and further stimulating the Committee’s data privacy jurisprudence. In examining States’ periodic reports or considering individual communications under the Covenant, the Committee could invoke principles of the Guidelines in assessing compliance with the privacy provision of the ICCPR. This is also unlikely to raise a question of legitimacy since the Guidelines, as a soft law adopted by consensus, apply – or are at least addressed – to all member States of the UN. But, the Committee has never made a reference to the Guidelines.

Ironically, the Committee often refers to and sometimes relies upon the case law of the ECtHR on data privacy issues. For instance, in the recent case of *N.K. v The Netherlands*, the Committee drew substantially from the decision of the Court in the case of *S. and Marper v UK*, which concerned concerns collection and storage of cellular samples in the criminal context.³⁸⁵ In contrast, the ECtHR’s reference to the HR Committee’s jurisprudence is rare. When it has done so, it is often in a barely decisive manner. In the data privacy front, the UN Data Privacy Guidelines have been referred to in a recent Grand Chamber judgment of the Strasbourg Court in a case relating to the workplace surveillance of employees’ digital communication, but with no visible influence in the outcome.³⁸⁶ It is, however, interesting to note that this case has referred to and, to some extent, relied upon the ILO Code of Practice on the Protection of Workers’ Personal Data.³⁸⁷

In considering the termination of the monitoring by the Secretary-General, perhaps for the wrong reasons, and reluctance of treaty bodies to heed to the Data Privacy Guidelines, it is safe to state that the UN may have played the major part in throwing the Guidelines into disuse and practical futility. And of course, even most recent UN engagements with privacy in the wake of the Snowden revelations also

³⁸⁴ See Obed Asamoah, ‘The Legal Effect of Resolutions of the General Assembly’ (1965) 3 *Columbia Journal of Transnational Law* 210, 223.

³⁸⁵ HR Committee, *N.K. v The Netherlands* (Communications No. 2326/2013, 10 January 2018) [9.3-9.4] footnote 13-14, 22. It is also interesting to note here that while the author’s application to the ECtHR was initially declared inadmissible by the Strasbourg Court, the HR Committee found violation under Art 17 of the ICCPR.

³⁸⁶ *Barbulescu v Romania* (ECtHR, Application No. 61496/08, 5 September 2017) [37].

³⁸⁷ *Ibid*, [38-40].

have completely overlooked the Guidelines. All UN Privacy Resolutions make no reference to the Guidelines despite the fact that they purport to cover data privacy.³⁸⁸ Reports of the SRP do not sufficiently engage UN data privacy instruments. In his recent report to the HR Council, the Special Rapporteur ‘encourages’ countries recently adopting national data privacy law to ensure that the ‘minimum standards’ set out in the CoE Data Protection Convention are met.³⁸⁹ One would expect the UN Guidelines were referred to, instead, not least because they set minimum guarantees, and importantly are UN instruments.³⁹⁰ In this sense, the UN data privacy instruments, particularly Data Privacy Guidelines are ‘abandoned’ even by the UN itself.³⁹¹

In contrast, the institutional arrangements put in place in Europe are much advanced. The system by which each data privacy instrument is monitored is well tailored to avoid redundancy of efforts as indicated below in broad strokes. Moreover, although implementation of these instruments is largely local – i.e. undertaken by State parties under national legislation, the hard law nature of the data privacy instruments makes it compulsory to put in place the requisite institutional framework. At the most basic level, member States are required to install an independent national data protection authority to oversee the relevant legislation, and to entertain complaints from individuals. Additionally, European data subjects have the option of pursuing their claims in courts. Decisions of national data protection authorities are appealable to domestic courts.³⁹²

In the EU framework, layers of institutions are involved in enforcing and overseeing data privacy laws. The Court of Justice of the EU (CJEU), for instance, gets involved

³⁸⁸ A Resolution of the Human Council, however, breaks the trend, and mentions the UN Data Privacy Guidelines, which might in due course put the Guidelines in sight. See *The Right to Privacy in the Digital Age*, HRC Res 34/7, 34th sess, Agenda Item 3, UN Doc A/HRC/RES/34/7 (22 March 2017) preamble, [5].

³⁸⁹ Report of Cannataci, above n 158, [9]. See also *Report of the Special Rapporteur on the Right to Privacy, Joseph Cannataci*, UN Doc A/HRC/40/63 (27 February 2019) [47] (recommending UN member states to incorporate principles contained in Art 11 of Modernized CoE Convention).

³⁹⁰ The October 2017 report of the Special Rapporteur to the UNGA does refer to the Guidelines but in a clearly tangential manner after the OECD Guidelines (whose principles the report details) and the CoE Data Protection Convention. See *Report of Cannataci*, above n 263 (19 October 2017) [71-72]. A recent report of the OHCHR likewise notes that the CoE Data Protection Convention ‘can direct the design of adequate policy instruments’. See Report of the High Commissioner, above n 256, [28].

³⁹¹ Of a related point, see Casagran, above n 376, 217. In another report co-authored for the UNESCO, Cannataci notes that the UN Data Privacy Guidelines as being part of the international framework for the protection of privacy. See Joseph Cannataci *et al*, *Privacy, Free Expression and Transparency: Redefining their New Boundaries in the Digital Age* (UNESCO Series on Internet Freedom, 2016) 36.

³⁹² See, e.g., *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows*, opened for signature 8 November 2001, 181 ETS (entered into force 1 July 2004) art 1(4).

in individual cases when domestic courts refer cases for a preliminary ruling.³⁹³ A member State may also be sued by the European Commission before the Court for failing to respect EU legislation, including data protection legislation. It may even annul legislation found to violate fundamental rights including the right to data protection, based on action for annulment brought by the Commission, a member State or even individuals directly affected by a specific legislation.³⁹⁴ A more recent annulment decision by the Court was made against the Data Retention Directive whose ‘disproportionate’ retention obligations were found to violate the right to data protection recognized under the EU Charter.³⁹⁵

EU’s General Court also has a jurisdiction to hear and decide on cases brought by individuals against EU agencies or against regulatory instruments.³⁹⁶ Other supervisory mechanisms are also available. For instance, compliance with data protection rules by EU institutions is monitored by the Data Protection Supervisor.³⁹⁷ The ‘Data Protection Board’ under the GDPR also has some supervisory roles in ensuring harmonized application of data protection rules throughout the Union.³⁹⁸ That data protection is now a fundamental right in the EU also means that the Fundamental Rights Agency would also be involved in the web of the governance framework. Furthermore, the GDPR makes it mandatory to appoint ‘Data Protection Officers’ as internal supervisory authorities within each body engaged in the processing of personal data.³⁹⁹ These layers of monitoring bodies enable higher protection of data privacy rights of EU citizens. In the CoE, there is no supranational body tasked to enforce or monitor the Data Protection Convention. But there is arguably a possibility for individuals to invoke data privacy principles and rights of the Convention, when lodging complaints before the ECtHR. Since the ECtHR has considered many cases that concern protection of data privacy based on widely accepted data privacy principles, individuals could invoke the Convention directly before the Court.⁴⁰⁰

³⁹³ See, e.g., *Treaty of Lisbon, Amending the Treaty on EU and the Treaty Establishing the European Community*, opened for signature 13 December 2007 [2007] OJ C 306/1 (entered into force 1 December 2009) art 9F.

³⁹⁴ *Ibid.*

³⁹⁵ See *Digital Rights Ireland and Stetinger et alv Minister for Communication and et al* (C-293/12 and C-594/12) [2014] ECLI 238.

³⁹⁶ See e.g., *Treaty of Lisbon*, above n 393, art 9F.

³⁹⁷ See Regulation 2018/1725, above n 345.

³⁹⁸ See GDPR, above n 350, arts 68-76.

³⁹⁹ *Ibid.*, arts 37-39.

⁴⁰⁰ See Greenleaf, above n 59, 100. Recent examples of cases adjudged by the ECtHR that involved data privacy principles include *L.H. v Latvia* (ECtHR, Application No. 52019/07, 29 April 2014) [concerning processing of health data], *Uzun v Germany* (ECtHR, Application No. 35623/05, 2 September 2010) [Concerning processing of location data] Moreover, the ECtHR routinely makes reference to and relies upon Data Protection Convention 108.

In conclusion, the UN data privacy framework lags far behind when it comes to an institutional arrangement for monitoring implementation. The problem is not just in the lack of clearly designated monitoring bodies but also that already existing UN bodies such as treaty bodies have not been progressive in applying exiting norms in practice. The discontinuation of the 'follow-up' procedure, despite its limitations, further suggests the general reluctance, or lack of attention, at the UN towards data privacy as one area of protection. Now that UN data privacy standards are largely obsolete means that existing monitoring bodies like the HR Committee are better off to look across Europe, notwithstanding the question of competence that comes with it, until and unless the ongoing UN privacy discourse leads to a robust instrument of some sort.

2 Monitoring Challenges

The second institutional limitation relates to weak monitoring capacity of the various bodies tasked to oversee the plethora of UN data privacy standards. Like in the case of treaty bodies, the enforcement of UNESCO instruments falls in the hand of mostly part-time independent experts. The International Bio Ethics Committee, for instance, is a body of 36 independent experts elected by the Director General of the UNESCO for a four year term, and convenes at least once in a year.⁴⁰¹ The Committee is basically deliberative body that offers recommendations and advices to the UNESCO on matters of life sciences.⁴⁰² Unlike the European regime, there is no body with the power to make enforceable determinations on complaints lodged by individuals. Structural problems that beset treaty bodies such as the part-time nature of the role and frequent reshuffles add up to the lack of adequate monitoring powers. The CoE's Consultative Committee on Data Protection has only recommendatory roles,⁴⁰³ but the existence of the ECtHR provides a safety net. That is not the case in the UN data privacy regime.

Data protection policies of UNHCR and the IOM envisage relatively strong monitoring mechanisms. For instance, they mandate appointment of a 'Data Protection Officer' at the headquarters with the ultimate responsibility of oversight and 'Data Protection Focal Points' at each country office.⁴⁰⁴ Complaints against non-compliance with the policies could also be lodged to higher offices in the organizations' hierarchy, i.e. to the Inspect Generals Office under the UNHCR and the Office of Legal Affairs under the IOM Manuals.⁴⁰⁵ But the 'intra-agency' and essentially sectoral nature of these policies undercuts the potential of these instruments to serve as a truly international institutional framework.

⁴⁰¹ See details at <<http://bit.ly/2mIyFCb>>

⁴⁰² Ibid.

⁴⁰³ See Modernized Data Protection Convention, above n 64, art 18.

⁴⁰⁴ See UNHCR Data Protection Policy, above n 32, part 7.

⁴⁰⁵ See IOM Data Protection Manual, above n 319, principle 12.

The UN SRP is a newly added layer to the UN data privacy institutional arrangement. Its roles can generally be grouped into three: providing intellectual guidance, facilitating multi-level dialogue and monitoring developments on the right to privacy.⁴⁰⁶ On top of being a part-time role, the mandate's effectiveness in addressing the institutional deficit is hampered by a number of structural factors, including lack of resources and non-adjudicative nature of the role. That limits the potential of the mandate in filling the institutional void. But as shall be explored in chapter 6, its roles could be reoriented towards steering the already warmed-up the UN privacy discourse. The mandate can be tasked to chair the privacy forum where current and emergent privacy challenges are regularly discussed.

IV CONCLUSION

This chapter examined the boundaries of the UN data protection framework in protecting digital privacy. It demonstrated that the present UN framework suffers from deep normative fragmentation, lack of progressive privacy standards and a pertinent institutional machinery. These weaknesses of the data privacy framework are mainly by-products of Cold War politics and the UN's generally reluctant approach to privacy in general. The chapter further uncovered that relevant UN bodies have played a role in undermining practical value of the data privacy framework. The HR Committee's privacy jurisprudence, for instance, reveals no reference to UN data privacy standards. This adds to the thin privacy jurisprudence of the Committee developed under the ICCPR. The UN data privacy system, therefore, remain buried, and without any practical utility.

With the human right to privacy system yet to properly address data privacy themes – and with a rather parasitic and yet patchy data privacy framework, the case for a modern and comprehensive data privacy treaty may seem plausible. But the feasibility and desirability of a global data privacy treaty is doubtful. As argued in the introductory part of thesis, any hard legalization approach to digital privacy will meet stiff resistance from different corners. The best way forward is, as shall be shown in chapter 5, is to follow the unifying approach to privacy pursued in the ongoing UN privacy discourse. A soft law that brings under one roof various digital privacy norms, including key data privacy norms, will fill the missing data privacy piece in international law.

⁴⁰⁶ See HRC Res 28/16, above n 224, [4].

PART II: POSITIONING GLOBAL PRIVACY INITIATIVES IN INTERNATIONAL LAW

CHAPTER 3 — DIGITAL CONSTITUTIONALISM: DIGITAL PRIVACY AND PROMISES OF INTERNET BILL OF RIGHTS

I INTRODUCTION

This chapter examines the first of international initiatives that tend to envisage a progressive vision for the right to privacy: IBRs. It investigates the role of IBRs in reimagining the international law of privacy in the digital age. To that effect, the chapter considers the extent to which the new contours of the right to privacy envisioned in IBRs entrench, elaborate or clarify the right to privacy in international law, or even reinforce developing privacy norms. As shown in chapters 1 and 2, international privacy law is not largely fit for purpose in protecting digital privacy. This chapter discusses the role of IBRs in addressing weak structures of international privacy law. The argument develops on three levels:

First, this chapter demonstrates that the IBRs Project is unlikely to develop into a freestanding international law response to the ‘privacy problem’. This is mainly due to the diffuse and momentary nature of the overall IBRs Project, which further erodes the desirability and feasibility of a global IBRs. The adoption (and tabling) of IBRs legislation only in a handful of countries so far, and mainly in reaction to the shock of the Snowden debacle, adds little in terms of progressively developing an international IBRs. Conceptual ambiguities in many IBRs initiatives further weaken the ‘freestanding’ role of IBRs in international law.

Second, the chapter shows that the other possible role of IBRs is ‘contributory’ in that it may shape the methodological and normative directions of other ongoing reform initiatives. This flows from the characteristic feature of IBRs in cross-fertilizing developing privacy norms drawn from multiple sources. As this – and the next chapter on the ongoing UN privacy discussions – shall demonstrate, marks of IBRs, shoehorned through submissions of civil societies, are slightly visible in the series of UN Privacy Resolutions. However, the extent to which IBRs have so far informed the ongoing UN privacy discourse is, however, limited. This reduces the contributory role of IBRs in reimagining the international law of privacy.

Third, the chapter then argues that because IBRs is unlikely to result in anything tangible on its own or through cross-fertilization, the prime significance of IBRs is ‘catalytic’ by which its progressive vision shapes the form and content of a pragmatic approach to international privacy law. Chapters 5 and 6 explore how aspects of the IBRs may form part of such an approach, particularly in unpacking the scope and meaning of the right to privacy. As this chapter will show, the significance of IBRs initiatives lies in the way in which they reimagine the right to privacy in the

digital context. Most IBRs envisage the right to privacy in an elaborate manner, in contrast with vaguely charged privacy provisions of international law.

For the sake of convenience and to capture emerging terminologies in the literature, the chapter uses the terms IBRs, IBRs Project and digital constitutionalism interchangeably.⁴⁰⁷ Appendix 1 provides a full text of the Italian Declaration of Internet Rights for ease of reference.

II MAKING SENSE OF INTERNET BILL OF RIGHTS: ORIGINS, NATURE AND SCOPE

A Origins of IBRs as a Constitutional Project

The origin of the various initiatives for IBRs dates back to the early days of the Internet. With a typical declaratory tone, these initiatives sought to uphold the protection of human rights to the then expanding cyberspace. The unprecedented capabilities of information and communication technologies (ICTs) stirred concern that human rights would not adequately be protected in the new space. While the very nomenclature ‘bill of rights’ suggests the constitutional aim of these initiatives both in guaranteeing rights and setting limits to power, the initial choice of the terms was merely for symbolic purposes. Drawing on the English Bill of Rights (1689), the American Bill of Rights (1791) – and recently the ‘Magna Carta’ (1215), proponents of IBRs seek to symbolically assert human rights on the Internet, rather than to strictly enact them.⁴⁰⁸ In that sense, the IBRs Project may be taken as an attempt to offer a digital supplement to the global constitutionalization of human rights that took place after the Second World War. In the light of the new contexts of the digital space, it seeks to particularize the (international) human rights system to a set of rights and principles that require some unique rendition.

Unlike what its name might suggest, the ‘IBRs Project’ is not a unified and coherent digital rights movement. Rather, it is a collective label meant to capture a range of digital constitutionalism initiatives worldwide that often emerge in different contexts and fora.⁴⁰⁹ As shall be discussed below, these initiatives emerged in varying contexts and disparate processes but with some commonality of purpose. Recent judicial reference to these initiatives – and of course, the adoption of IBRs legislation in some jurisdictions – appear to gradually pull these initiatives towards a

⁴⁰⁷ See, e.g., Dennis, below n 413 (describing multi-level IBRs initiatives as digital constitutionalism).

⁴⁰⁸ See Rodotà, above note 50. The terms ‘Magna Carta’ has been used, in the context of IBRs, by inventor of the web Tim Berners-Lee in the wake of the Snowden debacle. See Jemima Kiss, ‘An Online Magna Carta: Berners-Lee Calls for Bill of Rights for the Web’, *The Guardian* (online), 12 March 2014, <<https://bit.ly/2wz93jL>>

⁴⁰⁹ For an early use of the terms ‘IBRs Project’ while discussing the IBRs initiative at the IGF, see Francesca Musiani, ‘The Internet Bill of Rights: A Way to Reconcile Natural Freedoms and Regulatory Needs?’ (2009) 6 *Scripted* 505, 505-506, 510-511.

coherent whole, however. The disunity of goals that epitomized its initial path is gradually lessening. This is further emboldened by the half-hearted embrace of the IBRs Project by various inter-governmental processes, including at the UN, the EU and the CoE.

The United States is sometimes considered a pioneer in adopting the first ‘bill of rights for the computer age’ for introducing the ‘Code of Fair Information Practices’ in 1973.⁴¹⁰ But the Code was merely a soft law that codifies data privacy principles which were then being enacted into law in some European countries, and as such, has little resemblance to typical IBRs considered in this chapter. Since the late 1980s, various actors including individual activists, media organizations, civil societies and academics have launched declarations of rights, principles and manifestos that claim rights on the Internet.⁴¹¹ Civil societies have particularly played a key role in championing IBRs since the early days of the web. The most influential IBRs initiative emerged at the IGF in 2006, which has since inspired, as shall be noted below, other similar initiatives at various levels. The Snowden revelations, however, came as an important milestone in the history of the IBRs Project. Not only did new typical exhortatory initiatives emerge but also that the IBRs have slightly changed its course, especially in terms of inspiring some concrete measures at national, regional and international levels.

In the years after the revelations, Brazil and Italy IBRs have enacted pieces of legislation that embody elements of IBRs. While these countries have long been supporters of IBRs at the IGF,⁴¹² the enactment of national IBRs legislation has barely been a course of action they envisioned. Similar initiatives are taking foot in other countries such as Cambodia, Nigeria, the Philippines and Guatemala. IBRs have also recently gained traction in some national and regional courts, as shall be considered later in this chapter. At the international level, IBRs are also slightly shaping the ongoing discussion at UN on the ‘right to privacy in the digital age’, where elements of IBRs informed, to a certain extent, the content of the latest Privacy Resolutions. As noted above, the IBRs Project postulates the right to privacy in a more nuanced, specific and sophisticated manner.⁴¹³ The chapter returns to discuss the way in which the right to privacy is articulated in IBRs documents after having discussed

⁴¹⁰ See Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (O'Reilly, 2000) 12; the text of the Code is available at <<http://bit.ly/1CVSjmd>>

⁴¹¹ Writing in 2014, Rodotà – who is one of the pioneers in the IBRs Project – reported the existence of at least 87 IBRs proposals worldwide. See Stephano Rodotà, ‘Towards a Declaration of Internet Rights’ on *European Area of Freedom, Security and Justice* (18 November 2014) <<https://bit.ly/2luWmxw>>

⁴¹² See, e.g., ‘Joint Declaration (of the Minister of Culture of Brazil and Undersecretary of Communication of Italy) on Internet Rights’ (The Second Internet Governance Forum, Rio de Janeiro, 12-15 November 2007) <<https://bit.ly/2qiWvuI>>

⁴¹³ See Dennis Redeker et al, ‘Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights’ (2018) 80 *International Communication Gazette* 302, 311.

immediately below common threads that tie the otherwise diffuse IBRs initiatives together.

B Locating Convergence in IBRs Initiatives

As noted above, the IBRs represents a diverse array of initiatives that often emerge in varying contexts, times and levels. This section seeks to locate areas of converge in the IBRs Project a view to provide a conceptual background against which its legal significance is examined. The discussion draws on a selection of IBRs initiatives, particularly those put forward post the Snowden revelations. This is precisely because the revelations have played a key role in the re-emergence of IBRs but also in lending some coherence to the IBRs Project. Despite the fragmented and diffuse nature of the IBRs Project, there are at least five common threads that tie most IBRs initiatives together, as considered below.

1 Evolutionary Project

The IBRs Project has generally been an *evolutionary* endeavour when it comes to its ultimate goals and purposes. While the original idea behind the project was to promote the protection of human rights on the Internet through non-binding advocacy instruments, this appears to be shifting over the years. Most of these initiatives emerged, as hinted above, originally as aspirational and declaratory documents aimed at influencing public policy. Unlike a typical legal instrument that gives individuals enforceable rights, IBRs were seen as tools of advocating for the respect, protection and enforcement of rights on the Internet. In launching an IBRs more recently, Article 19 – a civil society organization – for instance, notes that it is simply following the ‘honourable tradition within civil society and digital communities to draft and publish declarations, statements or principles on human rights and the Internet’, and based on ‘visionary and inspirational’ approach of the tradition.⁴¹⁴ Similarly, the IBRs initiative at the IGF, considered further below, originally sought to use the Charter of Internet Rights and Principles (IRP Charter) as a ‘rhetorical device’ that lays down an alternative vision for the Internet,⁴¹⁵ and to serve as an ‘advocacy and awareness raising’ tool.⁴¹⁶

However, this conventional aim of IBRs has been gradually changing in recent years. One apparent sign for this shift is the adoption into law of IBRs in some countries. Civil society initiatives are also showing similar sign of shift. At the 2014 IGF Istanbul meeting of the IBRs Dynamic Coalition – a group behind the launching of the IRP Charter, a member of the Coalition had, for instance, emphasised the need to

⁴¹⁴ See Barbora Bukovska and Niels ten Oever, ‘#InternetofRights: Creating the Universal Declaration of Digital Rights’ on *Article 19 Blog* (24 March 2017) <<http://bit.ly/2q5wji2>>

⁴¹⁵ See Marianne Franklin, *Digital Dilemmas: Power, Resistance and the Internet* (Oxford University Press, 2013) 143.

⁴¹⁶ See Jorgensen, above n 97, 369-370.

translate these initiatives into ‘legal standards’, to take the Charter beyond aspiration.⁴¹⁷ A suggestion of pushing the Charter to the ‘calm waters of the UN’ has also been made pointing to the desire of translating the Charter into a form of a multilateral instrument.⁴¹⁸

The shift towards a binding IBRs is also reflected in subsequent initiatives. One example is the European Digital Rights Charter, the name of which was even intended to be likened to the EU Fundamental Rights Charter.⁴¹⁹ The aim has been to present it to the European Parliament,⁴²⁰ and subsequently to be adopted as a binding instrument, perhaps as a digital supplement to the EU Charter – and hence enforceable by the CJEU.⁴²¹ Italy’s IBRs Declaration is a soft law, but the long-term aim has been to use the Italian Presidency of the EU at the time as an opportunity to pursue the issue of IBRs at the EU.⁴²² What makes this is remarkable is that the EU, as will be noted later, had, at some point, pondered the idea of IBRs. These developments attest to the evolution of the IBRs Project. One possible factor for this shift is the realization that threats to human rights in the digital age will not sufficiently be addressed through advocacy alone. While the net effect of this shift is yet to be seen, the increasing prominence of IBRs would gradually play a role in influencing law, policy and practice. The chapter returns to this point later.

2 Rights Novelty

A second characteristic feature is that most IBRs instruments set forth a set of quasi-novel human rights and principles. While most IBRs documents appear to affirm or adapt existing rights in the digital context, a set of novel rights that find no direct counterparts in the present human rights catalogue are also put forward. Some protagonists of the IBRs Project maintain that there are contextual factors unique to cyberspace, which the human rights regime needs to take into full account.⁴²³ IBRs initiatives, for example Article 19’s Declaration, emphasis the need to ‘create and articulate’ new rights for the digital age.⁴²⁴ The preamble of the Declaration affirms that there is a need to ‘explore and expand new human rights guarantees for the future’. The ‘right to Internet access’ is often seen as the only ‘new’ right

⁴¹⁷ See ‘The IRP Charter of Human Rights and Principles for the Internet: Five Years On’ (IRP Coalition Meeting Report: IGF 2014 Istanbul, 4 September 2014) <<http://bit.ly/1IL6lT9>>

⁴¹⁸ See Franklin, above n 415, 169,180.

⁴¹⁹ See ‘Charter of Digital Fundamental Rights of the European Union’ (2016).

⁴²⁰ See details at <<https://bit.ly/2q33dRf>>

⁴²¹ See European Digital Rights Charter, above n 419, art 23.

⁴²² See ‘Report of the Dynamic Coalition for Internet Rights and Principles’ (2015) 3.

⁴²³ See David Casacuberta and Max Senges, ‘Do We Need New Rights in Cyberspace? Discussing the Case of How to Define Online Privacy in an Internet Bill of Rights’ (2008) 40/41 *Enrahonar* 99, 99-100.

⁴²⁴ See Bukovska and Oever, above n 414.

propounded by the IBRs Project,⁴²⁵ but rights that appear to be carved as ‘subsets’ of existing rights are arguably new, or at least quasi-new rights as well.⁴²⁶ The exercise in novelty particularly concerns the right to privacy, which is often furthered into a subset of rights such as the ‘right to (use) encryption’, the ‘right of anonymity’ and ‘freedom from surveillance’. In providing specific privacy rights, IBRs appears to redefine the scope of the classic right to privacy based on the new realities of the digital age. This approach seemingly proceeds from the assumption that the respect for and protection of the right to privacy needed some rendition in the digital space.⁴²⁷

In the context of the right to privacy, for instance, the importance of encryption technologies – and hence the ‘right to *use* encryption’ – is often emphasised, including by UN human rights officers/bodies. The more recent argument was levelled by the former UN High Commissioner for Human Rights, Hussein, who remarked that since encryption is now widely used as a tool of protecting privacy in the digital age, it deserves protection.⁴²⁸ This viewpoint was later seconded by the inventor of the web, Berners-Lee, who reportedly claimed that encryption is now used by the ‘critical mass’ – and weakening it, therefore, would destroy the ‘modern way of life’.⁴²⁹ Reimagining the right to privacy in the digital age requires some level of specificity, but it would invite questions of legitimacy. This point is discussed further later in this chapter.

3 Momentary Project

A third defining feature of IBRs concerns the way in which they emerge. Most IBRs initiatives follow major historical junctures and are often momentary. Unlike conventional human rights documents that are often preceded by years of negotiation and drafting, most – if not all – IBRs are expressions of outrage at a particular incident, be it an invasive legislation or government and/ private sector

⁴²⁵ See Marianne Franklin, ‘Mobilizing for Net Rights: The IRPC Charter of Human Rights and Principles for the Internet’ in Jonathan Obar et al (eds), *Strategies for Media Reform: International Perspectives* (Fordham University Press, 2016) 85.

⁴²⁶ As should become clear, ‘subsets’ of the right to privacy considered here are slightly different from the ‘typology of privacy’ or ‘taxonomy of privacy’ discussed in the privacy literature. Bert-Jaap Koops et al, for instance, identify typology of privacies in national constitutions of nine countries such as ‘bodily privacy’ and ‘communication privacy’. See generally Bert-Jaap Koops et al ‘A Typology of Privacy’ (2017) 38 *University of Pennsylvania Journal of International Law* 438.

⁴²⁷ See Franklin, above n 425, 73-74 (stating the need for more ‘explicit rendering’ of human right to online situations).

⁴²⁸ See ‘Apple-FBI Case Could Have Serious Global Ramifications for Human Rights: Zeid’ (OHCHR Press Release, 4 March 2016) <<https://bit.ly/2H7vX4x>>.

⁴²⁹ See Matt Burgess, ‘Tim Berners-Lee: ‘We Need to Rethink the Web to Stop the Spread of Mean Ideas’’, *Wired UK* (Online), 11 April 2017 <<https://bit.ly/2oyapHE>>; a recent report of the Dutch government also emphasises the importance of encryption for the ‘functioning of society’. See Kieren McCarthy, ‘Dutch Govt Says No to Backdoors, Slides \$540k into OpenSSL Without Breaking Eye Contact’, *The Register* (Online), 4 January 2016, <<https://bit.ly/2EYKuNs>>

practices. A good case in point is the Snowden revelations. The momentary nature of IBRs is also to be traced in some of the national initiatives in Brazil and the Philippines where the process was triggered by the adoption of, or proposal for, legislation thought to be human rights unfriendly. These initiatives were soon abandoned, until the Snowden revelations came to light, particularly in Brazil to which the disclosures have had particular resonance. But the sporadic nature of the IBRs Project has limited its impact in shaping policy, law and practice. Perhaps, the recent recognition of IBRs by national and regional courts as well as by the ongoing UN privacy discourse may slightly address this particular point. But as this chapter shall show, this role of IBRs has not only been limited so far but is unlikely to have a significant role in reimagining the right to privacy in international law.

4 Norm Cross-fertilization

A tendency to build on progressive judicial decisions, domestic laws and emerging industry practices is the other attribute of IBRs. One finds a number of rights and principles in IBRs initiatives that have already been recognized in judicial decisions and laws at various levels. The influence of European (case) law is, in this regard, particularly significant. Examples are in order. One of the commonest (Internet) rights in IBRs documents is the ‘right to the confidentiality and integrity of information systems’ or also referred to as ‘IT basic right’.⁴³⁰ Before it widely featured in these documents, it was introduced by the German Constitutional Court in a 2008 decision.⁴³¹ The Court read this right within the broader ‘right to personality’ which is expressly recognized in the Basic Law of Germany.⁴³² The decision was based on the argument that the extant protection under either the right to inviolability of home or secrecy of telecommunication was not adequate to protect the right to privacy in the digital space. While this decision introduced, or carved out, a quasi-novel constitutional (digital) right, the idea behind this right already existed in European law. One finds, for instance, in European data privacy law provisions that require data controllers to put in place technical measures to ensure confidentiality of digital communications.⁴³³ The IBRs Project embraces this (European) right which, with the recent proliferation of data privacy legislation worldwide (based mostly on European standards), is being recognized in jurisdictions outside Europe.

Another example is the ‘right to information self-determination’, a right initially formulated by a decision of the German Constitutional Court in a 1983 decision,⁴³⁴

⁴³⁰ See Schulz and van Hoboken, below n 715, 37.

⁴³¹ See Bundesverfassungsgericht (2008) *BVerfG* 822.

⁴³² See *Basic Law of the Federal Republic of Germany* (1949) (as amended in 2014) art 2(1).

⁴³³ See, e.g., Directive 2002/58/EC, above n 343, arts 1, 4-5.

⁴³⁴ See Bundesverfassungsgericht (1983) *BVerfGE* 65.

which is now widely adopted in IBRs instruments.⁴³⁵ Like the ‘right to the confidentiality and integrity of information systems’, this right was also carved out by the Court from the classic right to personality and the right to dignity of the Basic Law. A more recent example is the ‘right to be forgotten’, a right declared by the CJEU but based on relevant provisions of EU data privacy law.⁴³⁶ The right is now commonplace in IBRs instruments.⁴³⁷ The benefit of this cross-fertilization approach is that it identifies best practices from different sources and projects them to a wider global audience. This opens the possibility of gradual recognition in national law and even international law. We return to this point later in this chapter.

5 Multi-Stakeholder Experimentation

Some IBRs documents are results of multi-stakeholder processes by which inputs are drawn from various stakeholders, including governments, civil society, academia and the technical community. The primary goal of a bottom-up, multi-level process is enhancing procedural legitimacy of the norms created through the process. The assumption is that an instrument that heeds to the views, inputs and concerns of relevant stakeholders is likely to be treated as legitimate.⁴³⁸ A multi-stakeholder approach must, however, be distinguished from the rather common ways of drawing input in national lawmaking processes such as ‘consultation’. While both seek to achieve procedural legitimacy by drawing from relevant interest groups, the latter appears to be entirely discretionary/advisory – and hence not all inputs may make their way into the final version of the outcome. The making of some IBRs appears to have followed the conventional public consultation mechanism, as opposed to a truly bottom-up, multi-stakeholder process.

The multi-stakeholder approach is often reinforced by crowdsourcing mechanisms. While the IBRs Project makes use of crowdsourcing in norm creation, it is only rarely that the drafting of IBRs ever started from scratch. Often, the crowdsourcing exercise builds on an initial draft – and in that sense, it resembles the traditional ‘public consultation’ in domestic lawmaking. The drafting of Italy’s Declaration, for instance, was undertaken by a Commission installed by the government, which then was released to gather inputs through crowdsourcing.⁴³⁹ In a similar vein, Article 19 has launched a hash tag campaign on Twitter, perhaps as a new variant of

⁴³⁵ See, e.g., Italy’s Declaration, above n 181, art 6; European Digital Rights Charter, above n 419, art 11 [note, however, the error in the heading of the article, ‘data protection and data sovereignty’ while the proper heading is used (wrongly) in art 12, the content of which concerns, inter alia, the right to encryption].

⁴³⁶ See *Google v Agencia Española de Protección de Datos (AEPD) v Mario Costeja González* (C-131/12) [2014] ECLI 317. Note that the EU’s GDPR expressly recognizes a broader ‘right to be forgotten’. See GDPR, above n 350, art 17.

⁴³⁷ See, e.g., Italy’s Declaration, above n 181, art 11.

⁴³⁸ See, e.g., Joanna Kulesza, ‘Protecting Human Rights Online: An Obligation of Due Diligence’ (New York University School of Law Jean Monnet Working Paper No. 24/14, 2014) 6.

⁴³⁹ See details at <<http://camera.civi.ci/>>

crowdsourcing mechanism, to gather input on the draft Declaration.⁴⁴⁰ But the prevalent digital divide, across geography, age and gender, undercuts the promises of crowdsourcing as a reliable medium to ensure popular participation. This state of affair, coupled with recent threats of online disinformation, further raises concerns regarding the legitimacy of a crowdsourced IBRs instrument. This point is further discussed later in this chapter.

C Miscellany of Legal Sources and Forms in IBRs

Despite the above highlighted commonalities, initiatives for IBRs take different legal forms and have multiple sources. The IBRs Project is, as noted above, a syndicate of initiatives launched at various levels, including by individual activists, civil societies, the private sector and national governments. IBRs also take various forms from a legal point of view. While many are launched as non-binding civil society policy briefs or mere advocacy instruments, others are adopted (or proposed) as a domestic legislation, be it in hard or soft law form. This section discusses this diversity in form and source to properly situate IBRs in the international law of privacy. The submission is that the diffusion in form hinders any possibility of IBRs developing into an international instrument in the long-run.

Initiatives for IBRs launched by civil society groups dominate the global IBRs landscape. The IRP Charter is perhaps the most influential of civil society IBRs initiatives. The genesis of the Charter was at the Tunis Summit on Information Society in 2005, a summit convened by the International Telecommunication Union (ITU). With the active support of the governments of Brazil and Italy, the Charter was developed at the Summit by the Dynamic Coalition of Internet Rights and Principles.⁴⁴¹ While the Coalition operates within the UN as part of the IGF, it essentially is a multi-stakeholder platform where the voice of non-State actors especially civil society groups is influential.

Article 19, a UK based civil society group, has recently launched two notable IBRs: the Universal Declaration of Digital Rights and the Global Principles on the Protection of Freedom of Expression and Privacy. The Global Principles primarily aim to offer an 'analytical framework' on the way how free speech and privacy rights reinforce each other.⁴⁴² But one finds useful articulation of (digital) privacy rights in the Global Principles, particularly in unpacking the respective role of States and Corporations vis-à-vis the right to privacy. The African Declaration of Internet Rights and Freedoms is another civil society IBRs initiative. The Declaration seeks to promote 'human rights standards in Internet policy formulation and

⁴⁴⁰ See the hash tag campaign at <<https://twitter.com/hashtag/InternetofRights>>

⁴⁴¹ See Jorgensen, above n 97, 353, 358-359.

⁴⁴² See 'Global Principles on the Protection of Freedom of Expression and Privacy' (Article 19, 2017); a more recent civil society initiative is 'International Declaration on Information and Democracy' (Reporters Without Borders, 2018).

implementation' in Africa.⁴⁴³ As shall be highlighted later in this chapter, the Declaration has recently drawn the attention of the AU's human rights monitoring body, signalling prospect of reference in its jurisprudence.

A number of countries have either adopted, or are currently considering legislation, that carries IBRs themes. The first country to adopt a law that touches on aspects of IBRs is Brazil. Launched in response to a draft cybercrime legislation perceived to be human rights unfriendly in 2009, it initially was seen as an experiment of building consensus before parliamentary deliberations.⁴⁴⁴ The process was stalled until the Snowden disclosure came to light, which was particularly scandalous to Brazil. The country's President at the time, who was a victim of the espionage, declared a 'constitutional emergency' that revived the law. However, despite the frequent reference to this Brazilian law as a 'bill of rights', its content barely resembles typical IBRs instruments examined in this chapter. This point is further considered later in this chapter.

Italy is the first country to adopt, albeit a soft law, an IBRs legislation in the strict sense of the term. Italy's Declaration of Internet Rights was initiated by the President of the Italian Chamber of Deputies after the Snowden revelations.⁴⁴⁵ But, the Italian IBRs experiment, as noted above, begun at the IGF in collaboration with Brazil. Nigeria has also been considering a draft IBRs legislation since the Snowden debacle. The Nigerian Digital Rights and Freedom Bill, adopted by the country's legislature but later denied Presidential assent,⁴⁴⁶ aims to 'ensure that offline rights apply online' and to ensure compliance with 'established rights and freedoms'.⁴⁴⁷ While the bill is meant to be a broader legislation, it embodies common digital rights including privacy rights and principles. Substantive aspects of the Bill as well as Italy's Declaration, are considered in the section below.

The essence of IBRs has also found some expression in inter-governmental processes. At the UN, IBRs themes are considered, to some degree, in the reports of UN Special Rapporteurs. Some reports of the former Special Rapporteur on Freedom of Expression, La Rue, have touched on aspects of IBRs. His 2013 report, for instance, notes that restrictions on the use of privacy enhancing technologies (PETs) such as encryption amount to interference with the right to privacy.⁴⁴⁸ He further suggested

⁴⁴³ 'African Declaration of Internet Rights and Freedoms' (2014).

⁴⁴⁴ See Carolina Rossini et al, 'The Strength and Weaknesses of the Brazilian Internet Bill of Rights' (Chatham House, 2015) 4.

⁴⁴⁵ See Rodotà, above n 411.

⁴⁴⁶ See Victor Ekwealor, 'Nigeria's President Refused to Sign Its Digital Rights Bill, What Happens Now?', *Techpoint.africa* (online), 27 March 2019 <<https://bit.ly/2UZhGRC>> [reporting lack of thematic focus and coverage of proposed topics in existing laws as the grounds for denial of presidential assent].

⁴⁴⁷ See *Nigerian Digital Rights and Freedoms Bill* (2016) part I (1).

⁴⁴⁸ See *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, UN Doc A/HRC/23/40 (17 April 2013) [71].

that everyone has the right to use any technological tool to ensure the security of his/her communication, and States owe a negative obligation of not interfering with such use, or to force disclosure of encryption keys.⁴⁴⁹ The former Special Rapporteur on Human Rights and Counter-terrorism, Emerson, has endorsed this reading of Article 17 of the ICCPR in his post-Snowden disclosures report. Emerson noted that the obligation of States under Article 17 of the ICCPR is to ‘respect’ the privacy and security of digital communication, further suggesting that no positive obligation exists in the context of secure communication.⁴⁵⁰ These statements essentially read a ‘right to *use* encryption’ in the classic right to privacy. To what extent these UN reports have informed, or been informed by, IBRs initiatives, is not entirely clear. Perhaps, the Special Rapporteurs’ assertion might have informed civil society IBRs as part of the overall cross-pollination of digital rights norms in the IBRs Project.

La Rue’s successor, Kaye, has also noted that Article 17(2) of the ICCPR embraces a right to be notified when cases of compelled disclosure of user data arise.⁴⁵¹ Kaye further noted that the obligation involves, among other things, ‘protecting’ the private sector development and provision of technical measures, products and services.⁴⁵² Unlike La Rue who read a right to use encryption mainly in the privacy provision, Kaye reads the right implicitly within the right to freedom of expression.⁴⁵³ One also recalls the remark of the former Higher Commissioner, noted above, suggesting that encryption, as an important tool of protecting privacy, deserves protection. But he did not go far to claim the existence of a right to encryption or that States have a corresponding obligation therewith.⁴⁵⁴ Overall, apart from such occasional and indirect references to IBRs, there is an apparent apathy at the UN towards IBRs in general.⁴⁵⁵ Not only did IBRs themes surface occasionally but also that the above noted reports of Special Rapporteurs barely engage with the various IBRs documents that correspond to their mandates. The lack of consistent

⁴⁴⁹ Ibid, [89].

⁴⁵⁰ See *Report of the Special Rapporteur on the Promotion and Protection of Human Rights while Countering Terrorism*, Ben Emerson, UN Doc A/69/397 (23 September 2014) [28], [58].

⁴⁵¹ See *Report of Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Freedom of Expression*, David Kaye, UN Doc A/HRC/29/32 (22 May 2015) [18].

⁴⁵² See *Report of Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Freedom of Expression*, David Kaye, UN Doc A/HRC/32/38 (11 May 2016) [86].

⁴⁵³ See Report of Kaye, above n 451, [29-35]; see also David Kaye, ‘Encryption and Anonymity Follow-up Report’ (Research Paper 1/2018, June 2018) [5-6].

⁴⁵⁴ In an interesting contrast, the SRP, Cannataci, treats ‘technical safeguards’ like encryption as extra-legal means of privacy protection – and in so saying, appears to suggest no right to *use* encryption exists under the right to privacy. See *Report of Special Rapporteur on the Right to Privacy*, Joe Cannataci, UN Doc A/HRC/31/64 (8 March 2016) [50].

⁴⁵⁵ Note that IBRs themes also figured occasionally at the HR Council, see Dixie Hawtin, ‘Internet Rights and Principles: Trends and Insights, in *Internet Rights and Democratization: Focus on Freedom of Expression and Association Online*’ (Global Information Society Watch, 2011) 52.

attention to IBRs by relevant UN bodies discount the possible role of IBRs in the progressive development of international privacy law.⁴⁵⁶

To summarize the above discussion, the sporadic and diffuse nature of the IBRs Project – added to the complex diversity of its legal sources and forms, undermine its role in the further development of privacy law at various levels. The lack of sustained consideration of IBRs in relevant inter-governmental processes, especially at the UN, further arrests its role in reimagining the international law of privacy in the digital age. The next section discusses the way in which the right to privacy is envisaged in IBRs instruments. In doing so, it seeks to explicate the substantive boundaries of the IBRs in articulating the right to privacy. As shall be shown, the way in which privacy is formulated in IBRs documents offer a progressive vision for the right to privacy in international law.

D The Right to Privacy in IBRs

In a 1989 piece ‘Why have a Bill of Rights?’, Justice Brennan of the US Supreme Court quips that ‘the utility of a bill of rights cannot easily be gauged before its contents are specified’.⁴⁵⁷ In that spirit, this section examines the way in which the content of the right to (digital) privacy is specified in IBRs initiatives. This provides the background against which the utility of IBRs in reimagining international privacy law can be gauged in section III.

IBRs instruments cover a broad range of human rights, including those that find counterparts in (international) human rights law, and those that do not. Of these human rights, the right to privacy holds a prominent place in almost every initiative for IBRs. Not only is the right to privacy envisioned in these initiatives but also that it is made so in a manner that specifies the right into what we might call a ‘subset of rights’. One, however, finds variations in the way in which the right to privacy is enshrined vis-à-vis those ‘subset’ of rights. Some IBRs documents provide a general right to privacy which then is specified into specific privacy rights,⁴⁵⁸ while others

⁴⁵⁶ Note that IBRs has also gained some traction in the CoE and EU. A CoE digital sector official, for instance, has signalled that the best forum to realize Berner-Lee’s idea of Magna Carta is the CoE, and indeed Council’s Internet Governance Strategy document (2016-2019) had embraced that idea, although nothing tangible has come out thus far. See Jan Kleijssen, ‘A Magna Carta for the Internet?’ on *LinkedIn Pulse* (17 September 2014) <<http://bit.ly/2qtNTOH>> cum See ‘Internet Governance Strategy (2016-2019)’ (CoE, 2016) [8]. At the EU, IBRs was considered, but not (yet) acted upon, at the European Parliament even before the Snowden debacle. See, e.g., ‘European Parliament Recommendation to the Council on Strengthening Security and Fundamental Freedoms on the Internet’, [2008/2160(INI)] (26 March 2009) [S and ac]; see also Nate Anderson, ‘New Internet Bill of Rights Contender Comes from...Pirates?’, *Arts Technica* (online), 12 December 2012 <<http://bit.ly/2iv6SDg>>

⁴⁵⁷ William Brennan, ‘Why Have a Bill of Rights?’ (1989) 9 *Oxford Journal of Legal Studies* 425, 425.

⁴⁵⁸ See IRP Charter, above n 98, art 8.

stipulate each subset of right as a freestanding right.⁴⁵⁹ As shall be discussed further below, the IBRs Project also draws the scope of privacy rights in a manner that, to some extent, clarifies the scope of the right and the corresponding obligations of duty-bearers, particularly technology companies.

Two subset of privacy rights are commonly envisioned in IBRs initiatives: the ‘right to use encryption technologies’ and ‘freedom from surveillance’.⁴⁶⁰ Most IBRs documents incorporate a ‘right to *use* encryption’ while a few others provide for a ‘right *to* encryption’.⁴⁶¹ The basic difference is that the former appears to envisage a negative freedom, allowing users to make use of those technologies. In practice, this simply would mean the right of individuals to use encryption tools such as Pretty Good Privacy. And as such, no positive obligation flows from this in a way that would require technology providers, or States, to avail those tools. But the latter, on the other hand, suggests a positive freedom that entitles a right to demand provision of encryption tools somehow.

In practical terms, the right *to* encryption would partly relate to emerging requirements in data privacy law worldwide towards privacy by design. Perhaps, what the IBRs Project does is that it frames aspects of this idea in a human rights language. In EU law, the principle of ‘data protection by design’ concerns the embedding of (data) privacy principles in the designing of information systems used in the processing of personal data. It is described as the idea behind the PETs.⁴⁶² To a certain degree, the notion of privacy by design captures recent industry practices of companies like Apple in providing encryption of data and ephemeral messaging services. As hinted above, the primary aspect of the right to *use* encryption technologies is the freedom to access and apply the technologies. But where the right includes an entitlement for secure products and services, it would be a right *to* encryption.

The other specific privacy right is the ‘right to online anonymity’. It involves the right not to be identified while surfing the Internet. While some IBRs documents provide this right as a freestanding right,⁴⁶³ others provide it alongside the right to use encryption.⁴⁶⁴ However, both anonymity and encryption technologies reinforce the right to privacy. While most anonymization technologies hide the identity of

⁴⁵⁹ See ‘Universal Declaration of Digital Rights’ (Article 19, 2017) arts 4-6.

⁴⁶⁰ See, e.g., IRP Charter, above n 98, art 8; see also African Declaration, above n 443, art 8; Article 19’s Declaration, above n 459, arts 5-6.

⁴⁶¹ See, e.g., European Digital Rights Charter, above n 419, art 12(2).

⁴⁶² Bert-Jaap Koops and Ronald Leenes, ‘Privacy Regulation cannot be Hardcoded: A Critical Comment on the ‘Privacy by Design’ Provision in Data Protection Law’ (2014) 28 *International Review of Law, Computers and Technology* 159, 159.

⁴⁶³ See, e.g., Article 19’s Declaration, above n 459, art 4.

⁴⁶⁴ See, e.g., IRP Charter, above n 98, art 8.

individuals at the different ends of the communication, encryption software help conceal the content of the communication.

‘Freedom from surveillance’ is another common privacy right in IBRs documents. The use of the term ‘freedom’ suggests a negative right, but its content appears to embrace a positive dimension as well. The freedom involves the right not to be subjected to arbitrary mass surveillance, interception and pervasive monitoring.⁴⁶⁵ Its positive dimension guarantees a right to ex post-facto notification to a person subjected to ‘targeted’ surveillance. Moreover, it involves the right to access laws and procedures that authorize surveillance. This right is an invention of post-Snowden IBRs initiatives meant directly as a response to revelations of mass surveillance practices of Five Eyes States.⁴⁶⁶ But it captures an important essence of the right to privacy which the above subsets of privacy rights do not seem to cover.

Privacy principles and norms that now are common in data privacy law are also provided in many IBRs documents. This means that despite the apparent ‘human rights’ tone of IBRs, the IBRs Project embraces, to some degree, aspects of the rather regulatory field of data privacy. Indeed, in the case of Brazil’s purported IBRs law, the privacy provisions were imported from the then draft data privacy legislation.⁴⁶⁷ Italy’s Declaration also embodies rights that relate to the protection of data privacy. It, for instance, embodies the ‘right to the protection of personal data’, ‘right to information self-determination’, and ‘right not to be subjected to decisions based on automatic processing of personal data’.⁴⁶⁸ With the increasing fusion of human rights language in data privacy legislation in the form of ‘data subject rights’, the unifying approach of the IBRs Project is not out of place. But because of the casuistic nature of data protection legislation, IBRs do not, and probably could not, go beyond providing enabling set of data privacy rights leaving the mechanical details of data protection to a secondary legislation.

The way these rights and principles are framed sometimes varies. The African Declaration, for instance, puts the right to privacy into the ‘right to personal data protection’, ‘right to anonymity’ and ‘right to (use) appropriate technologies to ensure private, anonymous and secure communication’.⁴⁶⁹ Whereas Article 19’s Declaration stipulates the right to privacy into the ‘right to anonymity’, ‘right to encryption’, ‘right to be free from surveillance’, ‘right to control data’ and ‘right to

⁴⁶⁵ Ibid; see also Article 19’s Declaration, above n 459, art 6.

⁴⁶⁶ For purposes of this thesis, the terms ‘mass surveillance’ represents practices of States, acting alone or with the assistance of technology companies, to gather intelligence including personal information of an entire or significant portion of a population in bulk. See more at: <<https://bit.ly/2MzKB8Y>>.

⁴⁶⁷ See Rossini et al, above n 444, 4.

⁴⁶⁸ Italy’s Declaration, above 181, arts 5-6, 8-9.

⁴⁶⁹ African Declaration, above n 443, art 8.

migrate and export data'.⁴⁷⁰ The other important variation is that not all of these privacy rights are explicitly recognized in some IBRs documents. For example, while Brazil's Marco da Civil Internet addresses the right to privacy at length, one finds no rights like the right to *use* encryption in the legislation.⁴⁷¹ The closest it comes is when it provides for the 'inviolability and secrecy of the flow of communications over the Internet' in Art 7(II).

Italy's Declaration does not similarly recognize a specific right to encryption technologies. It embodies, however, other rights such as the right to the 'inviolability of electronic systems, devices and domiciles' which may perhaps be taken to embrace aspects of the right to encryption.⁴⁷² Article 10(1) of the Declaration, although situated under the caption 'protection of anonymity', reflects the spirit of a right to *use* encryption technologies: anyone may 'communicate electronically using instruments, including technical systems, which (...) prevent the collection of personal data'. Considering encryption's primary role in making content data unreadable by third parties, this provision can be said to protect a right to *use* encryption. Nigeria's Bill exhibits similar variations. While it does not embody a specific right to encryption, it includes broadly termed rights like 'right to digital privacy'.⁴⁷³

The second issue concerns the way in which IBRs initiatives define the scope of the right to privacy. They do so by providing a limitation clause that rectifies the gap in international (human rights) law. As discussed in chapter 1, no proper limitation clauses are attached to the privacy provisions of both the UDHR and the ICCPR. Limitation clauses in many IBRs invariably adapt the widely accepted three-part standards of legality, legitimate aim and necessity.⁴⁷⁴ There are, of course, exceptions to this. The IRP Charter, for instance, merely provides a general limitation clause that resembles Art 29 of the UDHR.⁴⁷⁵ This lapse appears to be a result of the drafters' mechanical approach while adapting provisions of the UDHR to the digital context, article by article. The European Digital Rights Charter also refers back to Art 52 of the EU Fundamental Rights Charter which envisages requirements of legality, necessity and proportionality.⁴⁷⁶ As submitted in chapter 1, proper limitation clauses are key in ascertaining the scope of human rights, and thereby preventing overbroad restrictions by the State (and non-State actors).

⁴⁷⁰ But note that while the heading reads as 'right to encryption', the content adds the term 'use'. See art 5.

⁴⁷¹ *Brazilian Civil Framework for the Internet* (2014) ch I, art 3 (II and III), ch II, arts 7-8, section II. Of a similar view, see Schulz and van Hoboken, below n 715, 44.

⁴⁷² Italy's Declaration, above n 181, art 7.

⁴⁷³ Nigeria's Bill, above n 447, arts 3-11.

⁴⁷⁴ See, e.g., Article 19's Declaration, above n 459, art 21.

⁴⁷⁵ IRP Charter, above n 95, art 29 (b).

⁴⁷⁶ European Digital Rights Charter, above n 419, art 23.

The third important aspect of the IBRs Project relates to the way in which possible obligations of both States and non-State actors are envisioned in some IBRs documents. This mostly is framed along with each subset of privacy right. Article 19's Global Principles, for instance, articulate the content of the right to anonymity and encryption along with purported obligations that rest on States and corporations. Obligations of States and corporations regarding encryption, for example, include recognition by law the importance of encryption technologies, promotion of end-to-end encryption, promotion of digital literacy, repeal of laws that ban or restrict use or import/export of encryption technologies, and repeal of laws requiring backdoor access or escrow systems.⁴⁷⁷

Principle 8 further provides the conditions under which Internet corporations may be required to disclose user data, and an obligation to provide notification to users when such disclosure is made. Similarly, the conditions for access to, search and seizure of digital accounts of users are provided in the Global Principles, which involve judicial oversight and requirements of legality, necessity and proportionality.⁴⁷⁸ This attempt at articulating the possible role/obligations of Internet corporations vis-à-vis the digital rights, including privacy, would offer some guidance for future efforts of defining the role of both States and corporations vis-à-vis the right to privacy.

III THE ROLE OF INTERNET BILL OF RIGHTS IN REIMAGINING INTERNATIONAL LAW OF PRIVACY

If the nature and scope of the IBRs Project as a promising international privacy initiative is clearly laid out, the next step is to examine its role in reimagining current international law of privacy in the digital age. In analysing the role of IBRs, the discussion in what follows considers three potential roles for IBRs. First, it considers whether there is any chance of IBRs developing as an international legal response to the 'privacy problem'. Second, having rejected the possibility of a global IBRs, it goes to consider its contributory role by which it may shape the pending UN privacy discourse and beyond. Third, because the contributory role has a limited normative value, it then discusses the more promising 'catalytic role' of IBRs in shaping the course of practicable reforms.

A Freestanding Role: Hurdles for an International IBRs

One possible path for the IBRs Project to take is gradually evolving into a global instrument, perhaps in a treaty form.⁴⁷⁹ As highlighted at the outset, there has been

⁴⁷⁷ Article 19's Global Principles, above n 459, principle 7.

⁴⁷⁸ Ibid, principle 10.

⁴⁷⁹ For a brief discussion of whether a customary international law (of privacy) may grow out of IBRs, see section B below, but the short answer is no.

occasional calls for a sort of international IBRs. De Minico, for instance, suggested for an IBRs to be adopted by a ‘public supranational legislator’ based on input from the private sector.⁴⁸⁰ A different form of proposal has been Rodotà’s proposed ‘charter of rights for the Internet’ that a ‘crowd of judges’ in every jurisdiction would apply in addressing common questions of human rights on the Internet.⁴⁸¹ Beside ambiguities associated with these proposals considered in the introductory part of the thesis, any idea of a global IBRs faces a number of hurdles. Such hurdles emanate from the nature IBRs Project as whole, its normative content, the process through which it is made. What follows discusses these concerns that reduce the chance of IBRs developing into a freestanding international law response to the privacy problem.

1 Diffuse and Momentary Project

The diffuse and momentary nature of the IBRs Project is the primary obstacle in its gradual development into a global instrument. As considered in section II above, the IBRs Project has been from the outset a multi-level endeavour pursued at various levels, by different actors and at different times. IBRs are adopted into domestic law, launched as civil society advocacy instruments and even by individual activists. IBRs national laws adopted so far, for example in Italy, are soft law and hence of no legal force. Where they are adopted in a form of hard law – for example in Brazil, the degree to which they reflect the conventional substance of IBRs has been limited. This diffuse nature of the Project means that any hope for an international IBRs is slim.

Momentary nature of the IBRs Project in that it emerges in reaction to a given incident, and dies down gradually, further reduces the possibility of an international IBRs, or in even contributing towards other forms of reform. IBRs initiatives do not often linger after the hype around that particular phenomenon recedes, and as such, the underlying aim does not appear to shape the development of human rights in the digital context. Reflective of IBRs Project’s momentary nature is that it is also becoming a tool of political campaigns in some countries. In countries like the UK and New Zealand, political parties – including those in power– appear to find it politically advantageous to champion digital rights in their election manifestos.⁴⁸² But little seems to follow once the election season ended. The recent embrace of IBRs

⁴⁸⁰ See De Minico, above n 83, 19-30.

⁴⁸¹ See Rodotà, above n 50.

⁴⁸² See, e.g., ‘Protecting Your Data Online with a Digital Rights Bill’ (Liberal Democrats, 11 April 2015); ‘Change Britain’s Future: Liberal Democrat Manifesto’ (2017) 72; ‘Forward, Together: Our Plan for Stronger Britain and a Prosperous Future’ (The Conservative and Unionist Party Manifesto, 2017) 76-77, 79-80; ‘The Digital Democratic Manifesto’ (The Labour Party, August 2016); ‘Gareth Hughes MP: Government Must Do More to Close the Digital Divide’ (The Green Party of New Zealand, 3 February 2015).

by some technology companies is also a manifestation of the market-driven, and hence its momentary nature.

In that sense, IBRs initiatives may have become victims of what Raz calls 'reckless activism'⁴⁸³ of rights that follow some major events thought to be human rights unfriendly. But resort to rights activism without a sustained process damages the integrity of the international human rights system.⁴⁸⁴ This relates to the problem of 'rights inflation' or 'hypertrophy of rights' which occurs due to nomination of more human rights, thereby posing the risk cheapening the currency of the human rights.⁴⁸⁵ As shall be discussed further below, this particular point has also a bearing on the legitimacy of IBRs.

Overall, because of its deeply fragmentary and temporal nature, it is unlikely that an international instrument would come out of the IBRs Project.

2 Conceptual Ambiguities

Perhaps a result of the diffuse and momentary nature of the IBRs Project, most IBRs documents lack theoretical-conceptual clarity, particularly in the way how they formulate rights. This is the second factor that works against the possibility of IBRs becoming a freestanding global instrument on digital rights. The problem of conceptual ambiguity has two dimensions. First, many IBRs initiatives do not clearly provide the substantive content of rights, and corresponding obligations. Second, the IBRs Project often overlooks the institutional framework needed for the implementation of the envisioned (Internet) rights. Third, the IBR Project does not properly situate itself within the international human rights discourse. What follows is an examination of these conceptual-theoretical shortcomings of the IBRs Project.

Beyond recognizing a subset of privacy rights, most IBRs documents leave undefined the specific content of each subset of right, and the corresponding obligations. The right to *use* encryption best illustrates this point. Despite figuring in almost every IBRs initiative discussed above, what obligation flows from this right is rarely explicitly provided. It is not also straightforward on whom the corresponding obligations befall – i.e. States, businesses or even ordinary individuals. Whether the obligation of States, for instance, is merely a negative obligation or also a positive obligation is far from clear. Would, for instance, States be required to run awareness raising campaigns on secure communications, waive import/export tariff or roll back licensing requirements? Would the obligation of businesses involve providing end-to-end encryption by default or offering free device encryption services or install

⁴⁸³ Raz, below n 487, 228.

⁴⁸⁴ See Hannum, above n 211, 445.

⁴⁸⁵ See Posner, above n 127, 94; see also Michael Ignatieff, 'Human Rights as Politics and Idolatry' in Amy Gutmann (ed), *Human Rights as Politics and Idolatry* (Princeton University Press, 2001) 90; Griffin, above n 159, 205-206.

Transport Layer Security (TLS) such as https? Questions of these sort find little answer in most initiatives for IBRs, perhaps with the exception of Article 19's Global Principles which, as noted above, to some extent elaborates possible obligations that flow from some digital rights both on States and businesses.

Such conceptual ambiguities give rise to a number of questions. First, from a theoretical perspective, there can barely exist a right if no corresponding obligation could be discerned from the right stipulated. As elaborated in Hohfeld's analytical framework of rights, duty is a 'jural correlative' of a right which exists only when there is a right.⁴⁸⁶ This means, as put by Raz, it is only when a right leaves a corresponding obligation on others that it exists, and therefore, a right exists because it gives rise to duty(ies).⁴⁸⁷ Second, even when a corresponding obligation may be implied somehow, it would prove difficult to attribute it to a particular duty-bearer. This, in turn, makes it onerous for individuals whose rights are violated to attribute responsibility. Even more onerous in the digital realm where attribution is harder, and that violation could be committed by anyone with ill-will. What makes the above uncertainties more acute, in the IBRs context, is that no interpretive entities are envisioned in most IBRs initiatives, as will be discussed below.

Amnesty International, a human rights non-governmental organization, recently offered an expansive reading of States' positive obligations under the right to privacy in the context of encryption technologies. According to this reading, the obligation to 'protect' includes the obligation to raise awareness about Internet security issues, fixing security flaws and to 'facilitate' the use of encryption tools and services.⁴⁸⁸ This expansive interpretation can be problematic, however. For instance, what exactly 'facilitating' involves would also be controversial. Does 'facilitating', for example, involve import tariff exemption, or State subsidized provision of PETs? What would State obligation to 'fix security flaws' include? It is not, for instance, clear whether it comes into play only when the security flaw concerns State-operated computer systems or extends to the private sector as well.

Conceptual ambiguities inhere in other rights as well: 'freedom from surveillance'. The right to freedom from surveillance includes, for example under the IRP Charter, the right not to be tracked online. But the scope of this right is far from clear. For example, whether freedom from surveillance would require service providers not to block access to users using anti-tracking technologies or more generally to make their services interoperable is not clearly enunciated. Article 19's Declaration frames the 'right to be free from surveillance' to include a right to have access to information about policies on surveillance, and to be informed when a targeted

⁴⁸⁶ Wesley Hohfeld, 'Fundamental Legal Conceptions as Applied in Judicial Reasoning' (1917) *Yale Law Journal* 710, 710-714.

⁴⁸⁷ Joseph Raz, 'Human Rights in the Emerging World Order' in Rowan Cruft et al (eds), *Philosophical Foundations of Human Rights* (Oxford University Press, 2015) 221.

⁴⁸⁸ See 'Encryption: A Matter of Human Rights' (Amnesty International 2016) 3, 32-33.

surveillance has been authorized.⁴⁸⁹ But, the scope of the right to notification is unclear – is the notification to be given prior to or after the surveillance? No doubt, *ex ante* notification is implausible as it would defeat the very purpose of the surveillance once the target becomes aware that surveillance is underway. Perhaps, a right to notification, as repeatedly articulated by the ECtHR, seems more appropriate *ex post facto*, which would allow concerned users to lodge protest against the request.⁴⁹⁰

The second aspect of ambiguity concerns institutional arrangements for the implementation of IBRs. Most IBRs initiatives, save few exceptions such as the Brazilian and the Nigerian legislation/bill as well as the European Digital Rights Charter, overlook the institutional aspect of rights. At times, the IBRs Project relegates the task of building institutions and the implementation of IBRs to a separate ‘discourse’.⁴⁹¹ The underlying aim of most IBRs initiatives to ‘translate’ human rights in the digital context also appears to eliminate the conventional role of judicial bodies to ‘translate’ norms to particular circumstances, including in light of new conditions of the day. Notable protagonists of the IBRs Project suggest that there is no need for an institutional arrangement for IBRs as its provisions would be applied by a global ‘community of judges’ who, in the digital age, will have to address similar legal questions.⁴⁹² IBRs would serve as a ‘reference’ to these, to use Rodotà’s words, ‘crowd of judges’ in such cases.⁴⁹³

But this viewpoint raises more questions than it answers. For instance, it is not clear to which IBRs instrument would serve as a model or reference to the global community of courts unless one assumes it to be the IRP Charter of the IGF or Italy’s recent Declaration in the drafting of which Rodotà played a part. It is not also clear how this would work, in reality, as courts normally apply legislation of their own jurisdiction. Nor is Rodotà’s vision equivalent to the rather common practice of judicial dialogue among courts of various jurisdictions.

Centrality of an institutional framework for a rights regime cannot be overemphasized. As rights without corollary duties are hardly rights, rights without an institutional framework to enforce them would be mere declaratory statements. As Raz points out, despite recognition by the black letters of the law, rights without impartial, efficient and reliable institutions that oversee their implementation are not (human) rights.⁴⁹⁴ The role of an institutional monitoring is also latent in Hohfeld’s analytical framework of rights. ‘Power’, in addition to ‘right’, ‘privilege’ and

⁴⁸⁹ Article 19’s Declaration, above n 459, art 6.

⁴⁹⁰ See, e.g., *Ekimdzhiev v Bulgaria* (ECtHR, Application No. 62540/00, 28 June 2007) [90].

⁴⁹¹ See Casacuberta and Senges, above n 423, 105.

⁴⁹² See Rodotà, above n 50.

⁴⁹³ *Ibid.*

⁴⁹⁴ Raz, above n 487, 228; see also Brennan, above n, 457 (noting that without some effective means of vindication, legal rights become mere moral claims).

‘immunity’, is the other jural component, by which it refers, among others, to the discretion of the State more broadly. According to his thesis, when ‘rights’ are violated, or more precisely, when ‘duties’ are not discharged – a putative right holder can appeal to the ‘power’ of the State to enforce his/her rights.⁴⁹⁵ This reinforces the indispensable role of an institutional mechanism, be it a court, quasi-judicial body or even an administrative agency, to maintain the balance of the rights-duty correlative.

In summary, the conceptual-theoretical opacity of the IBRs Project throws doubt on its practicality as an international law response to the privacy problem.

3 The Desirability Dilemma

Regardless of conceptional questions surrounding IBRs, there are also doubts as to the desirability of a global IBRs. Is there a need for an international IBRs? What justifies such an instrument? The question of desirability relates to at least two issues. One is that the IBRs Project does not offer a compelling justification as to why IBRs is needed in addition to the already existing framework of rights in (international) law. It is not clear how, and where, the present framework fails to protect human rights in the digital environment, and to what extent these weaknesses will be addressed by IBRs. Whether the perceived limitations of the present rights protection regimes are that of normative weaknesses or enforcement challenges is not clearly articulated by proponents of the IBRs Project.

The underlying objective of serving as an advocacy instrument of some IBRs initiatives, for example the IRP Charter, partly addresses the first point as this objective does not necessarily rely on the existence of weaknesses in the present framework. But, the problem persists in those IBRs instruments whose objective appears to be more than raising awareness or influencing public policy. The concern is that rolling out human rights without sufficient certainty that they will influence practice defeats their pragmatic function.⁴⁹⁶ In considering the several gaps in the international regimes for the protection of (digital) privacy – addressed in chapters 1 and 2, the lack of coherent conceptual justification for a new or expansive set of human rights standards for the digital space in the IBRs Project diminishes its appeal.

Second, the desirability of IBRs is also to be called into question in the light of the current reality where already guaranteed human rights are constantly violated. On account of the fact that some IBRs initiatives tend to install a parallel rights regime, it is of little value to add a new catalogue of rights which would either face the fate of being undermined or not enforced at all. The implied justification, at times, for some of the (Internet) rights lends weight for an argument against an international IBRs.

⁴⁹⁵ Hohfeld, above n 486.

⁴⁹⁶ See Amy Gutman, ‘Introduction’ in Gutman (ed) above n 485, xi.

The imperative of a right to encryption, for example, is often based on the supposition that encryption technologies are relied upon by ‘human rights defenders, journalists and dissidents’.⁴⁹⁷ Given that a smaller section of society uses such technologies, a question of whether it is worthy of nomination as a right arises.

This further raises doubt on the exaggerated claims, noted above, that encryption is necessary for the ‘functioning of society’, and that prohibition/restriction of its use would ‘destroy modern way of life’.⁴⁹⁸ When one considers the unresolved controversies regarding socio-economic and cultural rights – both in rights theory and practice, ambitious ventures of the IBRs Project particularly in introducing seemingly new rights such as right to the Internet access or even to use encryption technologies further compounds the desirability concern.⁴⁹⁹ The desirability concern, therefore, underpins the need for a pragmatic approach that explicitly justifies a reform without the risk of looking too ambitious, and hence stirring controversy. Chapter 5 explores the propriety of such an approach in rethinking the scope of the right to privacy in the digital age.

4 Feasibility Challenges

Uncertainties about the desirability of an international IBRs further cloud the likelihood of a globally acceptable IBRs framework. The feasibility concern takes various forms. First, the essentially ‘western’ origin – and hence reflection of ‘western values’ – of IBRs, in the face of wider digital divide, raises the question of whether IBRs could draw sufficient support worldwide to supplement, or remedy, weaknesses of the international law of privacy. The sheer fact that IBRs such as Nigeria’s Bill and the African Declaration, or even Brazil’s Macro da Civil, are from the global south do not necessarily mean that they reflect values of those jurisdictions or are reflections of wider concern for (Internet) rights. Indeed, most IBRs initiatives outside Europe are directly influenced by the IBRs Project that emerged as a European initiative, as highlighted above.

IBRs initiatives like the African Declaration are largely replicates of Charters with origins in the western world. The African human rights system, for instance, does not expressly recognize a right to privacy,⁵⁰⁰ but the Declaration embodies a list of privacy rights imported from preceding IBRs documents. With the digital divide

⁴⁹⁷ See, e.g., Amnesty International, above n 488, 4, 31.

⁴⁹⁸ Cf Melissa de Zwart, ‘Privacy for the Weak, Transparency for the Powerful’ in Kenyon, above n 2, 244 (claiming that ‘encryption may need to become the new standard, replacing common law or statutory concepts of privacy which have proven too vague and too unenforceable’).

⁴⁹⁹ At center of the controversy was the strong views of western States that socio-economic rights are ‘new’ rights, albeit to western political thought, and therefore must not be made part of the international bill of human rights. See Burke and Kirby, below n 611, 32.

⁵⁰⁰ The only exception is the rather specialized treaty, the African Child Rights Charter. See *Charter on the Rights and Welfare of the Child*, opened for signature 11 July 1990, OAU Doc CAB/LEG/24.9/49 (entered into force 29 November 1999) art 10.

wider (and intersectional) in some parts of the world, concerns for (digital) rights are probably lower. Some States and regions would, as a result, show hesitance towards a global IBRs, or an instrument with IBRs touch. Perhaps, a reluctance of the AU towards IBRs, except for a recent side note of the AU's human rights body, in contrast with the support shown by the CoE and EU, suggests the lack of strong interest, or attention, in Africa. A few countries in Latin America have recognized the right of Internet access, a typical IBRs, including in their national Constitution,⁵⁰¹ but it is too early to pronounce wider appeal to IBRs in the region. In parts of the world where access to the Internet is still limited, and where other priorities are too many, there is an additional reason to resist IBRs, or at least not to take them as a matter of priority.

IBRs may still be pursued as an international measure regardless of the above feasibility concerns. And, they might be endorsed without drawing sufficient consensus, as sometimes is the case in international standards setting. But this often comes with risks. As Hannum points out, attempts by (western) activists to put in place new human rights, without efforts to draw consensus, generates a backlash in the rest of the world.⁵⁰² The backlash could take various forms but typically IBRs drawn with insufficient consensus will be taken less seriously. In the context of 'rights talk' in general – i.e. proliferation of human rights, Glendon notes that impracticable demands of more human rights will gather little audience.⁵⁰³ The more visionary but unrealistic demands are made, the less that such demands are taken seriously, and met in practice. In places where they obtain some audience, the lack of resources towards enforcement will dictate a hierarchy of rights.⁵⁰⁴ This concern partly extends to the IBRs Project whose demands for rights protection not only appears less realistic but also lacks clear conceptual basis.

Recent enactment of legislation in Brazil and Italy does not necessarily reflect a strong and genuine global interest in IBRs. In fact, the success in the adoption of both pieces of legislation must be seen in context, and with a measure of care. Brazil's Marco da Civil, despite frequent references to it as the world's first IBRs, its content barely resembles typical IBRs. As noted above, a right to encryption, for instance, is not explicitly guaranteed under the law. Other privacy protective provisions of the legislation such as data localization rules were later rolled back due to criticism from various corners.⁵⁰⁵ Similarly, its implementation Decree adopted in 2016 addresses

⁵⁰¹ See, e.g., *Constitution of Ecuador* (2008) (as amended), art 16; *Constitution of Mexico* (1917) (as amended), art 6.

⁵⁰² Hannum, above n 211, 412-413.

⁵⁰³ Mary Glendon, *Rights Talk: The Impoverishment of Political Discourse* (Free Press, 1991) 14.

⁵⁰⁴ See Dominique Clement, 'Human Rights or Social Justice? The Problem of Rights Inflation' (2018) 22 *International Journal of Human Rights* 155, 159.

⁵⁰⁵ See Carlos Souza et al, 'Notes on the Creation and Impacts of Brazil's Internet Bill of Rights' (2017) 5 *Theory and Practice of Legislation* 73, 86.

privacy only peripherally as its primary focus is net neutrality.⁵⁰⁶ Considering these nuances behind the legislation, Marco da Civil can be seen as a politically motivated legislative rebuff to the Snowden revelations. So, this raises the question of whether IBRs, in the true sense of the terms, stands a chance of being accepted fully as one device of adapting (international) human rights to the digital space.

5 Procedural and Substantive (II) Legitimacy

If a global IBRs somehow gets adopted – despite fundamental questions raised above, it would not circumvent the consequent question of legitimacy.⁵⁰⁷ This is particularly if such instrument were to be adopted through a process often deployed in the IBRs Project. The process through which most IBRs initiatives come about, and actors that take part in the process raise issues of legitimacy and competence. In many cases, IBRs initiatives often are results of a multi-stakeholder process where various stakeholders, including civil society, governments and the private sector participate in the drafting exercise. The multi-stakeholder process is, as noted above, also increasingly being supplemented by crowdsourcing. That these processes of drawing up legal instruments are largely new phenomena raises the question of whether both the processes and the outcome of these processes could be accepted as legitimate. The question centers around who gets to decide what claims become human rights, and what content that such rights should have. The procedural and substantive legitimacy of a given rights regime turns, to a greater degree, on the answer to these questions.

There is no single widely accepted body to make the above sort of determinations. Perhaps, the closest is what is often referred to as a ‘democratic political community’ or the ‘international community’.⁵⁰⁸ This is, of course, without losing sight of the fact that these notions are largely artificial constructs, and at times, their constitution is contested.⁵⁰⁹ Democratically installed legislative bodies and judicial bodies at the national, regional and international levels can be taken to satisfy the criterion of ‘democratic political community’.⁵¹⁰ At the national and regional levels, parliaments and courts of competent jurisdiction may constitute this body whereas bodies such as the UNGA may be the international equivalents.⁵¹¹ Alston refers to the UNGA as the final ‘arbiter’ in deciding what claims are worthy of nomination as human

⁵⁰⁶ Ibid, 86-88.

⁵⁰⁷ The meaning of legitimacy may vary depending on the context in which it is used. But in a more general sense used here, what is often regarded ‘legitimate’ is one that is ‘lawful, just and rightful’. See Christopher Morris, *An Essay on the Modern State* (Cambridge University Press, 1998) 102-103.

⁵⁰⁸ See Saladin Meckled-Garcia, ‘Specifying Human Rights’ in Cruft et al (eds), above n 476, 300.

⁵⁰⁹ See Alan Boyle and Christine Chinkin, *The Making of International Law* (Oxford University Press, 2007, 17.

⁵¹⁰ See Meckled-Garcia, above n 508, 302.

⁵¹¹ See John Shorupski, ‘Human Rights’ in Samantha Besson and John Tasioulas (eds), *Philosophy of International Law* (Oxford University Press, 2010) 357.

rights.⁵¹² The Assembly perhaps represents what we earlier referred to as the ‘democratic political community’ or the ‘international community’.⁵¹³ The process through which some IBRs were launched meet these requirements, particularly those anchored at the national level.

Brazil’s legislation, for instance, is said to be a ‘legitimate’ piece of law on account of the participatory multi-stakeholder legislative process.⁵¹⁴ And of course, it has been adopted by an elected Congress, as was the Italian Declaration. The legislative exercise in the other experiments have not been so. The participation during the making of the Italian legislation, for instance, was said not to be ‘extraordinary’, suggesting the limited level of participation.⁵¹⁵ Little is known to what extent the Nigerian, or other similar initiatives in the Philippines, have been inclusive. But, most civil society initiatives barely meet the requirements of legitimacy noted above, not least because they often result from casual processes with apparent little concern for diversity of views. There is a general agreement that most civil society groups are not ‘even minimally transparent or accountable’ and hence lack legitimacy.⁵¹⁶ Article 19’s Twitter hash tag campaign, for instance, has gathered limited reaction, and the project seem to have been abandoned altogether. This casts doubt on the legitimacy of a global IBRs churned out of such processes of norm creation.

As highlighted in section II above, the IBRs Project is often credited for successfully experimenting a ‘multi-stakeholder model’, reinforced through crowdsourcing, of norm creation. But the level of stakeholder representation is constantly contested in organizations that practice ‘multi-stakeholderism’.⁵¹⁷ Although the options of participation are formally open, participation is practically limited by several factors including funding constraints, lack of expertise or even organizational capacity.⁵¹⁸ The open-door approach also exposes the process to undue influence by some interest groups, be it governments, businesses or even civil society.⁵¹⁹ When one

⁵¹² Alston, below n 542, 607-608.

⁵¹³ In their separate opinions in *Namibia Case*, Judges Fouad Ammoun and Padilla Nero refer to the UNGA as ‘representative’ of the international community and an ‘organ of the international community’ respectively. See *Legal Consequences for States of the Continued Presence of South Africa in Namibia (Advisory Opinion)* [1971] ICJ Reports, 73, 112.

⁵¹⁴ See Rossini et al, above n 444, 7.

⁵¹⁵ See Elisabeth Ferrari, ‘Italy Issues a Declaration of Internet Rights – Now Let’s Improve It’ on *Center for Global Communication Studies Media Wire* (4 August 2015) <<https://bit.ly/2qqyLOB>>

⁵¹⁶ See Samantha Besson and Jose Marti, ‘Legitimate Actors of International Law-making: Towards a Theory of International Democratic Representation’ (2018) 9 *Jurisprudence: An International Journal of Legal and Political Thought* 504, 527, 537.

⁵¹⁷ See, e.g., Laura DeNardis and Mark Raymond, ‘Thinking Clearly About Multi-stakeholder Internet Governance’ (Paper Submitted at the 8th Annual GigaNet symposium, Bali, Indonesia, 21 October 2013) 10.

⁵¹⁸ See Jeannette Hofmann, ‘Multi-stakeholderism in Internet Governance: Putting a Fiction into Practice’ (2016) 1 *Journal of Cyber Policy* 29, 33.

⁵¹⁹ See Besson and Marti, above n 516, 528, 538.

considers the generally sporadic and momentary nature of the IBRs Project, fault lines of its multi-stakeholder experiments compound. If multi-stakeholder participation is not free from flaws in well-resourced organizations like the Internet Corporation for Assigned Names and Numbers (ICANN), the experiment in IBRs would probably be too flawed to be taken seriously.

Recent developments further cast doubt on the value of crowdsourcing mechanism. One is the advent of online disinformation that dilutes the flow of information. The open nature of crowdsourcing platforms inherently lacks accountability mechanisms to protect legitimate contributions from being burdened by web trolls and bots.⁵²⁰ This adds up to the already growing ‘technological ambivalence’ towards promises of the web as a platform of popular participation. The failure of the crowdsourced constitution-making process in Iceland best illustrates the ambivalence towards crowdsourcing initiatives.⁵²¹ With a failed experiment in a small country of homogeneous and highly literate population, would crowdsourcing succeed in a rather heterogeneous environment, like the international community, where legitimacy is even more needed?⁵²² Probably not.

Crowdsourcing also raises an issue of normative quality. In the absence a mechanism of quality control by which the merit of inputs is independently examined, the sheer aim of ensuring procedural legitimacy ends up producing a document that erodes substantive quality, and hence legitimacy. Indeed, the juridical quality of several IBRs instruments, both those crowdsourced from scratch and those presented for collaborative redrafting, is questionable on many levels. Article 19’s Declaration, for instance, incorporates a range of rights, including ones that find counterparts in neither of the preceding IBRs instruments nor international human rights law. The problem is not with the exercise in rights novelty but the conceptual ambiguity of these rights. The Declaration contains, among others, the ‘right to blog’, ‘right to create’, ‘right to share’, ‘right to digital protest’, ‘right to dissent, offend and be offended’, ‘right to hack’, ‘right to tinker’ and ‘right to run one’s own server’.⁵²³ Similarly, the European Digital Rights Charter, reportedly drafted initially by a group of German academics, civil society groups and politicians, is poorly drafted, and is even described as a ‘juridical disaster’.⁵²⁴ This

⁵²⁰ See Helen Landmore, ‘Inclusive Constitution-making: The Icelandic Experiment’ (2015) 23 *Journal of Political Philosophy* 166, 175.

⁵²¹ See Andrea Simoncini, ‘The Constitutional Dimensions of the Internet: Some Research Paths’ (EUI Working Papers, LAW 2016/16, 2016) 7-9.

⁵²² For a related point, see Landmore, above n 520, 188-189.

⁵²³ See Article 19’s Declaration, above 459, arts 7-10, 13-15; perhaps in anticipation of surprise with some of these extraordinary rights, readers are cautioned at the outset that some of the text could be ‘distressing’ to lawyers and advises ‘reader discretion’. See Id, prelude.

⁵²⁴ See Franz von Weizsäcker and Norman Schräpel, ‘Why We Should Support the “European Charter of Digital Fundamental Rights”’ on *Internet Policy Review Blog* (14 December 2016) <<http://bit.ly/2qBg12N>>

casts negatively on crowdsourcing as a viable means of enhancing substantive legitimacy.

The other concern relates to the intersectional digital divides, be it geographically, across age groups, gender or disability. Digital divide significantly discounts the promises of crowdsourcing as a reliable medium of ensuring popular participation. Unless crowdsourcing is supplemented by other means to gathering input, what ultimately finds expression in the IBRs would be views of a limited group of stakeholders. Indeed, some interest groups mainly businesses may pursue crowdsourcing, in addition to their offline lobbying strategies, to influence the outcome of the law-making process. And this is not far from reality, with businesses now increasingly advocating for IBRs that often are aligned with their business interests.⁵²⁵ In the ultimate analysis, the legitimacy of the process, and the method through which some IBRs were launched so far – both as domestic legislation and civil society initiatives – falls short.

To summarize the above discussion, the case for a global IBRs instrument is weak for a number of reasons. The diffuse and momentary nature of IBRs means that no major initiative that gradually develops into an international instrument is likely. But notwithstanding its diffusive approach, an international IBRs would face questions of desirability. There is no compelling reason why, and how, a global IBRs would be adopted by the international community. More so if the proposed IBRs is to be developed through a process that lacks legitimacy.

B Contributory Role: Prospects of Shaping Law and Practice

As the shown above, the freestanding role of the IBRs Project in reimagining international privacy law is limited, if not none. But will it have some contributory role through which it may shape the progressive development of privacy law and practice at various levels? This section addresses this question. The contributory role may occur in three mutually-reinforcing levels: informing and steering global privacy discussions, inspiring domestic legislation and inducing judicial and industry best practices. As this section will be show, this role of the IBRs Project is unlikely to be consequential, particularly in reimagining the right to privacy in international law.

1 Enriching Global Privacy Dialogues

One possible contributory role is that IBRs may help further the global privacy debate evoked by the Snowden and subsequent revelations. More particularly, the elaborate privacy rights espoused in IBRs may shape the further development of privacy law worldwide. This may occur in inter-governmental processes, where IBRs is not an entirely new subject. As highlighted in section II, the IBRs Project now

⁵²⁵ See section B below on such industry practices.

has been, to some degree, an agenda item before several inter-governmental organizations such as the HR Council, the EU and the CoE. In practice, marks of IBRs are also slightly visible in the ongoing UN privacy discourse. The series of UN Privacy Resolutions adopted in the wake of the Snowden revelations appear to reflect, as shall be explored in chapter 4, IBRs themes. The Privacy Resolutions, for example, ‘encourage’ Internet corporations to ‘enable secure communications’ and develop ‘technical solutions’ to protect their users against arbitrary and unlawful privacy interference.⁵²⁶ This proviso reflects elements of common rights espoused in IBRs such as the right to *use* encryption.

But the degree to which IBRs shapes, and probably will continue to do so, global privacy discussions is limited. This is because the pursuit of IBRs as an agenda in inter-governmental and multi-stakeholder platforms has been largely inconsistent and sporadic. Despite positive initial gestures to IBRs at the CoE, EU and the HR Council, there is little to suggest that it still is an agenda item. The role of IBRs in the pending UN privacy discourse has also been, or will probably continue be, limited. This is, however, dictated partly by the nature of the discourse. As hinted at the outset, the composition of the Privacy Resolutions exhibits hybridity and selectivity of norms which means limited place for IBRs themes. Add to that the inherent unsuitability of Resolutions in being sufficiently comprehensive. Thus, regardless of the political will to embrace IBRs, there is only so much that may ultimately form part of a Resolution. Perhaps, the best chance is that other reform efforts may exploit this positive gesture in developing a more focused approach. This point is further explored below in section C and, in more details, later in chapters 5 and 6.

2 *Shaping Lawmaking*

IBRs may also inspire the enactment of national IBRs legislation, and hence gradually (and cumulatively) enhance harmonized protection of privacy globally. One of the earliest IBRs, the IRP Charter, for instance, has inspired Brazil and Italy’s IBRs instruments, albeit unsurprisingly given the historical role of the two countries at the Dynamic Coalition.⁵²⁷ Of draft IBRs legislation, a draft tabled by New Zealand’s Green Party is benchmarked after the IRP Charter.⁵²⁸ The substance of IBRs initiatives in the Philippines,⁵²⁹ Guatemala,⁵³⁰ Cambodia⁵³¹ as well as the

⁵²⁶ See *The Right to Privacy in the Digital Age*, GA Res 71/199, 71st sess, Agenda item 68(b), UN Doc A/RES/71/199 (25 January 2017) [7].

⁵²⁷ See Report of the Dynamic Coalition, above n 422, 3.

⁵²⁸ See IRP Coalition Meeting Report, above n 417, 12; Cambodia’s IBRs initiative is also influenced by the IRP Charter. See Godwin, below n 531.

⁵²⁹ See ‘Launch of the Philippine Declaration on Internet Rights and Principles’ (Foundation for Media Alternatives, September 2015) <<http://104.236.169.13/FMA/?p=416>>

⁵³⁰ See ‘An Inclusive Dialogue for the Internet Bill of Rights in Guatemala’ (Web We Want Foundation, 27 January 2017) <<http://ow.ly/hvMx30c7zdC>>

recently adopted IBRs in Nigeria are also similarly shaped by earlier IBRs documents. But the value in the proliferation of national IBRs legislation is rather limited in terms of international privacy law. Not only is the recent adoption of and/ proposal for IBRs legislation restricted to a few countries but also in the usual momentary fashion. The apparent lack of persistence in the IBRs Project means nothing concrete is forthcoming in terms of global privacy law.

These geographically limited legislative measures so far further eschew the possibility for the gradual development of international customary norms on (digital) privacy. As Chinkin notes, the use by States of instruments produced by civil society groups like IBRs may facilitate creation of customary norms by pressuring compliance, and hence producing State practice.⁵³² The adoption of domestic legislation giving effect to IBRs would further reinforce the creation of a customary international law norm. But, the limited adoption of domestic IBRs legislation so far, and the lack of adequate use of civil society IBRs by States means that the possibility of IBRs-induced customary norm is unlikely.

In short, because only a few pieces of IBRs legislation are adopted thus far, the role of IBRs in inspiring domestic legislation, and hence gradually resulting in the development of customary IBRs applicable globally, is insignificant.

3 Stimulating Judicial and Industry Practices

Another possible role for IBRs is to shape or influence decisions of courts at international, regional and national levels. As highlighted in section II, one characteristic feature of IBRs is that they are results of cross-fertilization of norms, including those drawn from decisions of regional and domestic courts. But, the reverse has also been the case, albeit seldomly. Many IBRs have been considered by courts in a few occasions. In a partial realization of Rodotà's vision of IBRs serving as 'reference' to the global community of judges,⁵³³ the Supreme Court of Argentina has recently made a reference to Brazil's IBRs in one of its decisions.⁵³⁴ At the regional level, AU's prime quasi-judicial human rights body has 'taken note' of the African Declaration in its Resolution on Freedom of Expression on the Internet.⁵³⁵ The ECtHR has also referred to IBRs themes in a number of recent cases.⁵³⁶

⁵³¹ See Mike Godwin, 'The Great Charter for Cambodian Internet Freedom' on *LinkedIn* (8 March 2015) <<https://bit.ly/2GEF2UR>>

⁵³² Chinkin, above n 327, 36.

⁵³³ Rodotà, above n 50.

⁵³⁴ See Souza et al, below n 505, 93.

⁵³⁵ *The Right to Freedom of Information and Expression on the Internet in Africa*, ACHPR Res. 362(LIX)2016 (2016) preamble.

⁵³⁶ In the recent case of *Szabo and Vissy v Hungary*, the ECtHR made reference to a 2013 Report of La Rue, considered above, where the Special Rapporteur emphasised States' obligation of not interfering

The legal significance of the above noted judicial references to IBRs is, however, limited. More so in development of the right to privacy in international law. In the case of Brazil's IBRs, for instance, the reference was to a provision of the legislation dealing with network neutrality. This adds up to the fact that the Brazilian legislation, as already noted, is not a typical IBRs instrument. The references by the two regional human rights bodies are also more of symbolic, rather than substantive, value. There is nothing to suggest, in the case of ECtHR for instance, that aspects of IBRs have shaped the respective decisions. This thus means that potential of IBRs in shaping judicial practice in a meaningful way is yet to arrive. While the willingness of regional bodies to engage IBRs is useful, its relevance in developing current international law of privacy is circumscribed.

Beyond the legal arena, IBRs may also influence the *modus operandi* of technology companies in adopting practices that protect (digital) rights of users. In the light of frequent scandals plaguing major market players, a handful of Internet firms have recently saw the competitive advantage of pledging IBRs. An example is the social networking site Ello which recently proclaimed 'Bill of Rights for social Network Users' for its users.⁵³⁷ Ello's IBRs appears to be influenced by the 'Bill of Privacy Rights for Social Network Users' introduced by the Electronic Frontier Foundation (EFF), a digital rights advocacy organization, in 2010.⁵³⁸ The other way in which Internet corporations resort to privacy protective practices is through enabling encryption by default or issuing transparency policy detailing, albeit in broad-strokes, government requests for user data.

Besides the fact that the traction to these industry practices is restricted to a section of the industry, specifically small Internet businesses and the voluntary nature of these pledges reduce their significance. But more importantly, part of the reason for the recent corporate support towards digital rights may simply be a business strategy, perhaps one meant to overcome the backlash since the Snowden debacle.⁵³⁹ As Rodotà rightly cautions, (digital) rights activism championed by Internet corporations may be clouded by business priorities.⁵⁴⁰ The future of international privacy law must be one that encourages such voluntary industry best practices but

with the use of encryption technologies. See *Szabo and Vissy v Hungary* (ECtHR, Application No. 37138/14, 12 January 2016) [24]. The Concurring Opinion of Judge De Albuquerque in *Szabo and Vissy* makes extensive reference to the post-Snowden developments at the UN, including the passing of Resolutions which, as noted above, touch on IBRs. Id, [3-7], [51].

⁵³⁷ See details at <<https://bill-of-rights.ello.co/>> other social networking sites have also similar policies, an example being 'MeWe'. See <<https://t.co/7DetwK2FSr>>

⁵³⁸ See Kurt Opsahl, 'A Bill of Rights for Social Network Users' (EFF, 19 May 2010) <<http://bit.ly/2s2PMFp>>

⁵³⁹ See Ernesto Falcon and Jeremy Gillula, 'The Hypocrisy of AT&T's "Internet Bill of Rights"' (EFF, 1 February 2018) <<https://bit.ly/2qgTGY9>> Cf Randall Stephenson, 'Consumers Need an Internet Bill of Rights' (AT&T Media Release, 24 January 2018) <<https://soc.att.com/2DHA7ki>>

⁵⁴⁰ Stefano Rodotà, 'Data Protection as a Fundamental Right' in Serge Gutwirth et al (eds), *Reinventing Data Protection?* (Springer, 2009) 82.

seeks to broaden the role of Internet corporations in the protection of human rights, including in multi-level dialogues. The thesis returns to this point in chapters 5 and 6.

C Catalytic Role:⁵⁴¹ Prospects of Charting Normative Directions

As the above discussion demonstrated, the possibility of IBRs developing into a global treaty law is deeply doubtful. Nor would its role of gradually shaping further development of privacy principles go far enough to address international law's privacy problem. This section suggests that a more pertinent role for IBRs is should its progressive vision were geared towards a more focused and innovative approach to reform. If it were to be integrated with such an approach, IBRs would assist in lessening, to some degree, the weak normative contours of international privacy law. Chapters 5 and 6 explore what a pragmatic reform approach to international law of privacy would look like in greater details, but what follows points to two aspects of IBRs that would be drawn upon in those chapters.

The IBRs Project envisions, as shown in section II, the right to privacy in manner that unpacks the scope of the right in international human rights law. This offers an alternate way of addressing the problems of scope, considered in chapter 1, of the human right to privacy framework. The UN data privacy framework, as shown in chapter 2, is generally fragmented and outdated at many levels. The IBRs Project offers useful lessons in addressing the deep normative dispersion and normative paucity of the UN data privacy framework. As IBRs instruments generally treat the 'human right to privacy' and 'data privacy' in a holistic manner, future reform efforts could rely on this approach. Normative inferiority of the UN framework could similarly be addressed as IBRs generally embody widely accepted rights and principles of data privacy that now are grounded in domestic laws of many countries. The other major rectification, as noted above, concerns the provision of pertinent limitation clauses to privacy rights. Most IBRs initiatives now clearly envisage the grounds under which the right to privacy can lawfully be restricted. This would remedy the gap in international human rights law.

Thus, the legal significance of IBRs lies in pointing towards an alternate 'normative direction' for further development of current international law of privacy in the digital age. In that sense, its role resembles what Alston called the 'catalyst' role of older charters of rights such as the English Bill of Rights and other subsequent

⁵⁴¹ The terms 'catalytic role' is borrowed from Brownlie by which he refers to the potential of legal instruments like Resolutions (and judicial decisions) in provoking further development of law. See, e.g., Ian Brownlie, 'Legal Status of Natural Resources in International Law' (1979) 162 *Recueil des Cours* 1, 261 (noting the decisive 'catalytic effect' of soft law in provoking development in State practice).

national declarations of rights.⁵⁴² Like the international law of human rights that followed the Second World War was partly inspired by these monumental national documents, IBRs may also catalyse an international privacy law reform. In that way, pragmatic reform ideas, particularly the soft law supplement to present international law of privacy argued for in chapter 5, draws from the catalytic effects of IBRs.

IV CONCLUSION

The history of the IBRs Project in the past two decades or so has been replete with uncertainties as to scope and goals. Most IBRs initiatives emerged in momentary, disjointed and uncoordinated fashion. Often, each initiative for IBRs including those advanced by civil societies varied in scope, purpose and existed in isolation from one another. This approach appears to have limited, thus far, their impact in the international protection of (digital) privacy. This chapter examined the role of IBRs in reimagining the right to privacy in international law. It demonstrated that a more concrete role of the IBRs Project is in charting a normative direction for other more focused and practical reform. The chapter argued that IBRs will neither develop into a freestanding international instrument nor will it sufficiently shape privacy law and practice worldwide to address international law's privacy problem.

Progressive normative elements of IBRs would, instead, offer a novel way in which the scope of the right to privacy must be drawn. More particularly, IBRs move past the present, to use Michael Ignatieff's words,⁵⁴³ 'minimalist' approach of international privacy law. The relatively elaborate manner in which privacy rights are envisioned in IBRs would assist in unpacking the high-level abstract principles of international law. But, as this chapter has illustrated, the IBRs Project risks slightly overstressing the human rights framework. Chapters 5 and 6 explore an approach to privacy law reform that strikes a fair balance between minimalist and maximalist visions of the right to privacy. The soft law supplement argued for in chapter 5 seeks to critically embrace quasi-new rights without eroding the integrity and credibility of the international human rights system.

⁵⁴² Philip Alston, 'Conjuring Up New Human Rights: A Proposal for Quality Control' (1984) 78 *American Journal of International Law* 607, 614.

⁵⁴³ See Ignatieff, above n 485, 321-322.

CHAPTER 4 — INCHOATE CONVERSATION: DIGITAL PRIVACY AND PROMISES OF THE UNITED NATIONS' DISCOURSE ON THE "RIGHT TO PRIVACY IN THE DIGITAL AGE"

I INTRODUCTION

This chapter examines the second of international privacy initiatives: the ongoing UN discourse on the 'right to privacy in the digital age'. It interrogates the role of Privacy Resolutions adopted as part of the discourse in making the international law of privacy better-equipped in the digital age. In so doing, it seeks to demonstrate the extent to which normative and institutional gaps examined in chapters 1 and 2 are, or will be, addressed by the pending discourse. The chapter argues that the prime merit of the discourse lies, like the IBRs Project examined in chapter 3, in its role of catalysing the progressive development privacy law. The argument develops in three steps.

First, the chapter considers the 'freestanding' role of the Privacy Resolutions in reimagining the right to privacy in international law. The freestanding potential of the Resolutions primarily relates to their role in elaborating the rather dense rules of current international law of privacy. Further considered is whether the Resolutions constitute 'authoritative interpretations' of existing privacy provisions of international law. The chapter shows that the rather patchy and incoherent content of the Resolutions, *inter alia*, discounts the significance of the elaborative and interpretive functions.

Second, the chapter considers the 'contributory' role of the discourse in shaping further development of privacy law at national, regional or/and international levels. It first discusses the extent to which the Privacy Resolutions may substantively inform the making of laws and judicial decisions. Further considered is whether the Resolutions may ground the right to privacy in general international law. The chapter demonstrates that this contributory role of the discourse is inconsequential. The substantive reach of the Resolutions thus far is narrow means that their possible function of grounding the right to privacy in general international law is negligible.

Third, the chapter contends that a tangible role of the discourse is 'catalytic' by which it may shape the normative and methodological directions of a practical privacy reform. Because the freestanding and contributory roles of the discourse are nominal, the best outcome would be innovative utilization of the political will exhibited in the ongoing discussions. The stimulation of a privacy agenda at the UN evoked by the discourse carries a political capital that can catalyse a more focused and practical reform effort. Chapters 5 and 6 explore such a reform alternative that

critically embraces but goes beyond aspects the privacy discourse in general and the Privacy Resolutions in particular.

II DISCUSSING THE NATURE AND SCOPE OF THE PRIVACY DISCOURSE

As shall become clear, the UN privacy discourse is in a state of flux and its true colours are yet to fully emerge. Not only is the conversation sparked by this discourse still inchoate but also that its role in the international privacy framework has not been considered. To fill this void, this section positions the discourse in context. First, it offers a background as to the origins and the overall composition of the discourse. Second, it considers the novelties introduced by the series of Privacy Resolutions adopted from 2013 to 2018 as part of the discourse. The examination offers the background against which its roles in reimagining the international law of privacy are considered in section III.

A Background to the Discourse

The ongoing privacy discourse represents a revival of the privacy agenda at the UN after many years of hiatus. Since the introduction of a general right to privacy in the ICCPR in 1966, the subject has received little attention at the UN. The two major exceptions are the adoption of the UN Data Privacy Guidelines in 1990 and GC 16 two years earlier. Privacy returned to the UN agenda decades later through various reports of UN Special Rapporteurs. But even in those instances, the right to privacy was treated merely as an enabler of other human rights mainly freedom of expression.⁵⁴⁴ The Snowden revelations have played a key role in putting the right to privacy back in the UN agenda. It is this essentially 'new' privacy discourse sparked by the revelations that is the prime focus of the chapter.

In terms of scope, the discourse consists of a series of Resolutions adopted by the UNGA and the HR Council. As the time of writing, four Resolutions have been adopted by the UNGA⁵⁴⁵ and three Resolutions (and a Decision) by the HR Council.⁵⁴⁶ There are two common threads in these Resolutions. One is that they are all adopted by consensus without formal casting of votes. The practice of adopting Resolutions by consensus is a relic of the Cold War era meant to offer compromise over controversial draft Resolutions.⁵⁴⁷ It is often seen as a way of papering over

⁵⁴⁴ See, e.g., Report of La Rue, above n 448.

⁵⁴⁵ Resolutions of the UNGA chronologically are: Resolution 68/167 (18 December 2013); Resolution 69/166 (18 December 2014); Resolution 71/199 (19 December 2016); Resolution 73/179 (17 December 2018).

⁵⁴⁶ Resolutions (and a Decision) of the HR Council chronologically are: Decision 25/117 (27 March 2014) [Panel on the Right to Privacy in the Digital Age]; Resolution 28/16 (26 March 2015); Resolution 34/7 (23 March 2017); Resolution 37/2 (22 March 2018). Afterword: after submission of the thesis in late June 2019, the HR Council has adopted its fourth Privacy Resolution — i.e. Resolution 42/15 (7 October 2019). Beside reinforcing the UNGA's latest Resolution, this Resolution mandates another expert workshop to be held before the next session. See Id, [10].

⁵⁴⁷ See Cassese, above n 125, 197.

differences on the text of Resolutions.⁵⁴⁸ And this may ultimately leave its marks in vague textual formulations.⁵⁴⁹

Fidler notes, in the context of the Privacy Resolutions, that the adoption without a vote – i.e. by consensus – is a reflection of controversy among member States on the content of the Resolutions.⁵⁵⁰ And of course, there were reports of lobbying by the Five Eye States at the early stages of the discussions at the UNGA's Third Committee, but the resultant change was said to be more of style and toning-down wordings.⁵⁵¹ With that said, the initiation, and still sustained, discussion on the privacy agenda paves the way for further engagement on privacy issues. The affirmative gesture of States, expressed when agreeing to adoption by consensus, would create an expectation of the international community that the terms of the Resolution will be taken seriously.⁵⁵² The adoption of the Resolutions per se is, thus, of some value when one considers the need for urgent reform in international privacy law.

A second thread is that those Resolutions adopted by the HR Council are essentially iterations of the UNGA Resolutions and adopted as a follow-up. Generally, Resolutions of both UN bodies carry no legally binding force. But it appears that UNGA Resolutions are more authoritative, not least because the Council is a subsidiary organ of the Assembly. The UNGA is generally considered as the 'chief deliberative, policy-making and representative organ of the united nations'.⁵⁵³ That the Council operates through periodic membership (added to its exposure to politicization) further makes its Resolutions less authoritative.

In addition to the handful of Resolutions, the privacy discourse is accompanied by a number of reports prepared by the OHCHR and UN Special Rapporteurs, including the SRP.⁵⁵⁴ This means that the content of the Privacy Resolutions is shaped and informed by these various Reports. The first report of OHCHR, for instance, has been key in shaping the direction and substance of subsequent Resolutions of the UNGA. But again, that report was developed based on inputs from various sources,

⁵⁴⁸ See, e.g., Oscar Garibaldi, 'The Legal Status of General Assembly Resolutions: Some Conceptual Observations' (1979) 73 *Proceedings of the Annual Meeting of the ASIL* 324, 326.

⁵⁴⁹ See Conforti Benedetto, *The Law and Practice of the United Nations* (Martinus Nijhoff Publishers, 3rd ed, 2004) 82.

⁵⁵⁰ David Fidler, 'United Nations Resolution on the Right to Privacy in the Digital Age', in Fidler, above n 4, 313.

⁵⁵¹ See, e.g., Anupam Chander and Molly Land, 'Introductory Note to United Nations General Assembly Resolution on the Right to Privacy in the Digital Age' (2014) 53 *International Legal Materials* 727, 727.

⁵⁵² See Samuel Bleicher, 'The Legal Significance of Re-Citation of General Assembly Resolutions' (1969) 63 *American Journal of International Law* 444, 446-447.

⁵⁵³ See, e.g., *United Nations Millennium Declaration*, GA Res 55/2, 55th sess, Agenda item 60(b) (8 September 2000) [30].

⁵⁵⁴ See, e.g., Report of the High Commissioner, above n 193.

including submissions of civil society groups which, in turn, draw from the jurisprudence of regional courts, national legislation and even IBRs. In that sense, the UN privacy discourse has been a site for cross-fertilization of global privacy norms. The chapter makes incidental references to these reports, and the accompanying discussion driven by other actors mainly civil society groups.

For ease of reference, appendix 2 provides full text of UNGA's fourth Privacy Resolution, and reference in this chapter is also mainly to that Resolution.

B Novelties of the Discourse

A closer look at the way in which the UN privacy discussions have proceeded in the past five years reveal at least two novelties. One relates to the overall approach of the discourse. There is an apparent unifying approach to the right to privacy by which the series of Privacy Resolutions embody hitherto disparate normative sources as well as actors involved in the protection and/or violation of the right. Not only does this import norms to a rather 'human rights' discourse from other related regulatory fields but also reflect modern understandings of and challenges to the right to privacy in the digital age. As shall be shown below, privacy norms, standards and principles flagged in the Resolutions are drawn from different sources, including domestic or regional data privacy law, international human rights law and even aspects of IBRs. Moreover, there is a tendency to bring in non-State actors, particularly Internet corporations, as important actors in the protection of the right to privacy. Secondly, the Resolutions tend to unpack normative contours of the right to privacy in the digital context, particularly in specifying the respective role/obligations of States and technology companies vis-à-vis the right to privacy. What is novel about this is that its tendency to change course in the UN 'business and human rights' debate by addressing corporation more directly in human rights language. The discussion below elaborates these novelties of approach and substance.

1 Novelty of Approach

The privacy discourse, the outcome of which has primarily been in the form of Resolutions, displays a level of novelty in approach. At a higher level of abstraction, the discourse is gradually producing Resolutions that barely resemble other UN Resolutions, be it previous or current ones. The UN Charter does not explicitly mention 'Resolution' as one means of international standard setting. But traditionally it is understood to be a substitute for 'recommendation' and 'decisions' which are mentioned explicitly in the Charter.⁵⁵⁵ In the international law literature, the term 'Resolution' is often used to refer to both Declarations such as the UDHR which embody substantive principles and rights as well as hortatory Resolutions

⁵⁵⁵ See, e.g., Marko Oberg, 'The Legal Effects of Resolutions of the UN Security Council and General Assembly in the Jurisprudence of the ICJ' (2006) 16 *European Journal of International Law* 879, 800.

which contain no such substantive legal principles or rights.⁵⁵⁶ But the Privacy Resolutions defy these niceties in UN practice and the literature. They do so mainly by flagging some substantive privacy principles and norms, as shall be discussed further below.

While the Privacy Resolutions clearly are not Declarations like the UDHR, they are not also mere hortatory Resolutions either. Except for the initial Resolution, the subsequent Resolutions appear to reflect some substantive principles that are not common in hortatory Resolutions. A good comparison is the ongoing discourse at the HR Council on the right to freedom of expression online which has similarly resulted in the adoption of a series of Resolutions. Under the title of ‘promotion, protection and enjoyment of human rights on the Internet’, the free speech Resolutions are typically hortatory, lacking substantive norms.⁵⁵⁷ But there is also a variation in terms of legal authority. The free speech Resolutions are adopted by the Council, unlike the Privacy Resolutions which are adopted by both by the UNGA and the HR Council. This has a bearing on the legal value of the Resolutions. In the light of this apparent distinction, it is safe to state that the Privacy Resolutions are unique in their approach and perhaps can be called ‘hybrid Resolutions’.

The other novelty of approach also reflects, or reinforces, this propensity to hybridity. The discourse is informed by and cross-fertilizes different normative sources on the right to privacy. While the discourse clearly is anchored within the ‘human right to privacy framework’, it embraces other slightly autonomous regimes for privacy protection. One such regime is data privacy law which, as examined in chapter 2, is a disparate regulatory field, albeit to a lesser degree at the UN level. Not only do the Resolutions contain data privacy themes, as shall be considered below, but also the latest Resolutions unusually ‘recall’ the UN Data Privacy Guidelines.⁵⁵⁸ The Guidelines are the prime UN data privacy instruments, but they are rarely refereed to or are considered by relevant UN bodies. Data privacy themes covered in the Resolutions are sourced mainly from European data protection law.

Elements of IBRs are also visible in the Privacy Resolutions, a good case in point being the increasing emphasis on the importance of PETs for privacy protection. The migration of such norms to the UN process is a result of the consultations held by the OHCHR that preceded the adoption of the second and third Resolutions of the

⁵⁵⁶ See, e.g., Boyle and Chinkin, below n 509, ch 5.

⁵⁵⁷ See, e.g., Resolution 32/13 (1 July 2016). But intriguingly, the latest free speech Resolution reiterates a few of the seemingly substantive themes of the Privacy Resolutions particularly those on the importance of encryption and anonymity, and even embodies a paragraph that urge States to adopt, implement and/or reform law on the protection of ‘personal data and privacy’. See HRC Res 38/7 (5 July 2018) [17]. This is, of course, part of the overall cross-fertilization tendency between these two discourses. One also sees elements of the free speech discourse making their way into the Privacy Resolutions, a case in point being threats of disinformation. See, e.g., Res 73/179, above n 545, preamble, [23].

⁵⁵⁸ See, e.g., Res 73/179, above n 545, preamble, [2].

UNGA.⁵⁵⁹ The consultations paved a way for submissions by civil society groups that are, as discussed in chapter 3, the main drivers of the IBRs Project. In that regard, the 2014 post-consultation report of the OHCHR makes reference to a post-Snowden revelations IBRs initiative of ‘13 International Principles on the Application of Human Rights to Communication Surveillance’.⁵⁶⁰ Beyond these sources, one may also trace in the Resolutions the influence of UN Special Rapporteurs particularly reports of successive UN Special Rapporteurs on Freedom of Expression, discussed in chapter 3. Thus, the discourse has a unifying approach to the right to privacy which reinforces the hybrid tendencies of the Resolutions.

A third novelty of approach concerns the way in which the Resolutions address the role of technology companies under the right to privacy. As examined in chapter 1, the role of (Internet) corporations is mostly overlooked in international law human rights law. But, the UN privacy discourse gradually brings them to the fore by specifying their roles in upholding digital privacy. The Privacy Resolutions, for instance, routinely ‘call upon’ Internet businesses to, inter alia, strengthen technical privacy safeguards and adopt transparency policies.⁵⁶¹ Yet, while the discourse usefully addresses the role of corporations vis-à-vis the right to privacy, it pays not heed to another parallel treaty process of the HR Council on business and human rights that moves towards addressing corporation more directly. The lack of synergy between the privacy discourse and the treaty process risks resulting in duplicity of efforts, and perhaps divergence of approach. We return to this point later in the thesis.

2 Novelty of Substance

The Privacy Resolutions also exhibit some novelty of substance. This novelty has two dimensions. One lies in the reflection of a few privacy principles that tend to elaborate the rather vague international rules on the right to privacy. This is occurring progressively. With the initial mostly hortatory Resolution that ‘reaffirms’ exiting rules to the digital space, the subsequent three Resolutions moved to flag substantive principles. One sees gradually emerging marks of the jurisprudence of judicial and quasi-judicial bodies such as the HR Committee and the ECtHR, IBRs initiatives as well as a number of thematic Reports of the UN Special Rapporteurs. As such, the novelty of the privacy principles flagged in the Resolutions is mostly to the UN privacy system. The other dimension of novelty is that the Resolutions specify – in a soft legal language of course – the roles/obligations of States and businesses vis-à-vis the right to privacy. This section examines these novelties of the

⁵⁵⁹ See Carly Nyst and Thomaso Falchatta, ‘The Right to Privacy in the Digital Age’ (2017) 9 *Journal of Human Rights Practice* 104, 105 (noting that ‘soft laws’ launched by civil society groups have informed the discourse).

⁵⁶⁰ Report of the High Commissioner, above n 193, [22], footnote 14.

⁵⁶¹ See, e.g., Res 73/179, above n 545, [7]. See more below.

privacy discourse. As shall be demonstrated, while the privacy discourse goes to some length in introducing modern privacy themes to the UN system and specifying the role of technology companies, it does so in a selective and hence less holistic manner. What follows, first, provides an overview of (data) privacy themes, and then, the role of (Internet) businesses flagged in the Privacy Resolutions.

(a) (Data) Privacy Iterations

Metadata and Biometric Information: an important privacy theme raised in the Resolutions concerns collection of metadata and biometric information.⁵⁶² In keeping with recent revelations about metadata collection, the Resolutions recognize the privacy implications of gathering and aggregating communication data, including when it is done so on a mass scale. The Resolutions provide that metadata may reveal insights into the private tests, preferences and other private aspects of a person's life when combined with other information.⁵⁶³ This proviso is imported from the Report of the OHCHR, which of course was informed by the case law of the ECtHR and the CJEU.⁵⁶⁴ In the case of *Malone v UK*, the ECtHR held that generation of metadata records through metering solely for billing purposes does not constitute interference with the right to private life under Article 8 of the ECHR, but when such record is shared with law enforcement, it will be and hence has to be justified.⁵⁶⁵ The Resolutions do not go as far as to stipulate when (and whether) generation of metadata on its own constitute interference with the right to privacy but they usefully flag an important issue to be addressed as the discourse further evolves.

With respect to biometric data, the Resolutions address both States and businesses but in a less clear manner. They stipulate that States and businesses 'must' respect their human rights obligations when collecting, storing, processing and sharing sensitive biometric information.⁵⁶⁶ But it is not entirely clear what exactly such obligations are. As will be noted further in section III, neither current law nor jurisprudence offer guidance on this point.

Mere collection of personal data interferes with privacy: a related substantive issue engaged by the Resolutions is the widely accepted dictum that the sole act of collecting and storing personal information constitutes interference with the right to privacy.⁵⁶⁷ This principle has been recognized by the ECtHR in the case of *Leander v Sweden* where the Court held that storing of personal information alone interferes with the right to privacy.⁵⁶⁸ This principle has later been codified in the EU data

⁵⁶² Ibid, preamble, [17], [25].

⁵⁶³ Id, preamble, [17].

⁵⁶⁴ See Report of the High Commissioner, above n 193, [19-20].

⁵⁶⁵ *Malone v UK* (ECtHR, Application No. 8691/79, 26 April 1985) [63-89].

⁵⁶⁶ See Res 73/179, above n 545, preamble, [25].

⁵⁶⁷ Ibid, preamble, [28].

⁵⁶⁸ *Leander v Sweden* (ECtHR, Application No 9248/81, 26 March 1987) [48].

protection laws, and as a result, amassing personal information constitutes processing of personal information thereby engaging the right to data protection.⁵⁶⁹

Data Protection Regulation: the latest Privacy Resolutions emphasis the need to regulate processing of personal data by law. Primarily, they call upon States to ‘adopt and implement data protection legislation, regulation and policies’ and establish independent and competent data protection authorities.⁵⁷⁰In a preambular proviso, the Resolutions further urge businesses to consider adopting ‘data protection policies and safeguards’.⁵⁷¹ The former reinforces GC 16 which reads into Article 17 of the ICCPR, as highlighted in chapter 1, States’ obligation to enact data protection legislation applicable to both the public and private sectors. But what exactly is implied in the latter proviso is unclear: are those policies internal documents that domesticate national data protection rules in corporate parlance? Does the reference to ‘data protection safeguards’ relate to the technical, administrative and organizational measures that data controllers are commonly required to institute?

Regulation of Digital Surveillance: the Resolutions address regulation of digital surveillance in two respects. First, they require States to align their domestic surveillance legislation with international law standards. What those standards exactly are is not clearly stated, but they emphasise the need for surveillance legislation to be clear, accessible, precise and comprehensive and non-discriminatory.⁵⁷²The emphasis here on the principle of non-discrimination, in the context of foreign surveillance, seems to be a direct response to discriminatory surveillance law and practice in Five Eye States brought to the spotlight by Snowden. Second, the Resolutions address the issue of intelligence sharing, calling respect for international human rights obligations.⁵⁷³But again, the nature, scope and source of these obligations are far from clear.

Artificial Intelligence and (Data) Privacy by Design: the privacy implication of rapid automation first found reference in the second Privacy Resolution of the HR Council where the need to further discuss and analyse practices of automated processing of personal data and profiling is stated.⁵⁷⁴ But that reference was mainly in the context of non-discrimination and economic, social and cultural rights. The latest UNGA Resolution makes a more direct reference. Not only does it recognize novel threats posed by rapid growth of automated technologies like artificial intelligence and machine learning but also emphasises the need to align their ‘design, evaluation and

⁵⁶⁹ See, e.g., GDPR, above n 350, art 4(2).

⁵⁷⁰ See, e.g., Res 73/179, above n 545, [6(g)].

⁵⁷¹ Ibid, preamble, [25].

⁵⁷² Ibid, preamble, [22] cum [6(h)] (calling for privacy safeguards and remedies to ‘all’ individuals).

⁵⁷³ Ibid, preamble, [24].

⁵⁷⁴ See HRC Res 34/7, above n 388, preamble, [16].

regulation’ with international human rights law.⁵⁷⁵ It appears that the addition of this new theme is a result of civil society work in the area.⁵⁷⁶ Through civil society advocacy, elements of European data protection law are thus slowly migrating to the international plane.

Overall, these privacy themes are merely highlighted in the Resolutions. Important details of the themes are slightly vague, but it is possible that they may find proper articulation in a future UN instrument as the discourse evolves. It is also worth emphasising that not all aspects of the Resolutions are novel. Less novel about the Resolutions, for instance, is that they reiterate the jurisprudence of the HR Committee. One example is that they reinforce the requirement that interference by States with the right to privacy to be consistent with the principles of legality, necessity and proportionality.⁵⁷⁷

(b) Obligations/Roles of States and Corporations

The second novelty concerns the clarification offered on the nature and scope of corporations’ obligations as well as State under the right to privacy. This, of course, is without losing sight of the obviously soft law nature of the Resolutions. No obligation flows from them in the strict sense of the term. But these clarifications are possible foreshadows of what ‘obligations’ might be specified to the human right to privacy should the discourse evolve into a more focused and concrete legal instrument. The terms of the Resolutions appear to follow the conventional types of State human rights obligations in international law: to ‘respect’, ‘protect’, and to some extent, ‘fulfil’.

(i) Obligations of States

The articulation of obligations begun with the initial Resolution which states that the obligations of States is not just to ‘respect’ – i.e. negative obligation – but also to ‘protect’ – i.e. positive obligation.⁵⁷⁸ GC 16 of the HR Committee has already stipulated this point, but the reinforcing role of the Resolutions is a welcome development particularly in dispelling the (wrong) view that Article 17 of the ICCPR guarantees merely a negative freedom. But as shown below, the Privacy Resolutions go farther in specifying both the negative and positive obligations of States compared to GC 16 whose truncated nature limited its scope as well as relevance.

An important elaboration of States’ negative obligation is that the Resolutions call upon States to refrain from measures that oblige businesses to take steps that

⁵⁷⁵ See Res 73/179, above n 545, preamble, [19] cum [7(d)].

⁵⁷⁶ See, e.g., ‘Privacy and Freedom of Expression in the Age of Artificial Intelligence’ (Privacy International, April 2018) <<https://bit.ly/2Hvso7I>>

⁵⁷⁷ See, e.g., Res 73/179, above 545, [4].

⁵⁷⁸ Ibid, [6(a)].

interfere with the right to privacy in an unlawful and arbitrary manner.⁵⁷⁹ This point is further reinforced by a proviso which requires States to respect their obligations under international law when they seek disclosure of personal data from third parties, including technology companies.⁵⁸⁰ What appear to be envisioned here are circumstances where States require companies to disclose user personal data, install backdoors in their products, provide encryption key escrows or even disclose specific encryption keys. This particular point may also be a result of the cross-fertilization of UN efforts on the right to privacy.

Positive obligations of States are provided in a relatively elaborate fashion under the latter Resolutions. In addition to the recurrent requirement to bring national law and practice in line with international law, the Resolutions provide specific obligations. These include enacting legislation that regulates ‘collection, processing, retention or use of personal data’ both in the public and private sectors.⁵⁸¹ This proviso requires for such a national legislation to envisage sanctions and remedies that apply when violation occurs, and the law shall cover ‘individuals, governments, business enterprises and private organizations’. Moreover, it calls upon States to provide effective remedy for people whose right to privacy has been violated by digital surveillance.⁵⁸²

Four specific positive measures that are more pertinent to digital privacy are also provided in the Resolutions. First, they call upon States to promote digital literacy that would equip users with technical skills needed to protect privacy.⁵⁸³ This proviso, which appears to reflect an ‘obligation to fulfil’, mandates digital literacy training on PETs such encryption technologies, which is often envisioned in IBRs in a human rights parlance. Second, they call upon States to consider measures that would enable businesses to adopt voluntary transparency measures regarding government requests for user personal data.⁵⁸⁴ The underlying aim seems nudging States to abolish or modify rules that impose what are commonly called ‘gag orders’ which prohibit businesses from informing users about government request for personal data. Third, the Resolutions call upon States to regulate by law the manner in which user personal data may be sold, resold or otherwise shared by businesses without the free, explicit and informed consent of the data subject.⁵⁸⁵ This adds up to the above noted call upon States to introduce a comprehensive data protection legislation.

⁵⁷⁹ Ibid, [6(l)].

⁵⁸⁰ Ibid, preamble, [24].

⁵⁸¹ See Res 73/179, above n 545, [6(f)].

⁵⁸² Ibid, [6(e)].

⁵⁸³ Ibid, [6(k)].

⁵⁸⁴ Ibid, [6(m)].

⁵⁸⁵ Ibid, [6(n)].

(ii) Role of Corporations

To a degree, the role of Internet corporations under the right to privacy are specified in the Resolutions. The exercise began in the first Resolution with a hint in a preambular paragraph that ‘surveillance, interception and data collection’ could well be undertaken by non-State actors such as ‘companies and individuals’ and later grew into elaborate principles.⁵⁸⁶ The later Resolutions directly address the role of businesses both as agents of protection and of violation of digital privacy. What makes this important is that the responsibility of Internet corporations in the protection of the right to privacy is, as discussed in chapter 1, often overlooked in international human rights law and discourse.

In addressing the role of Internet corporations, the Privacy Resolutions follow a layered and, at points, incremental, approach. First, they acknowledge the risks posed to the right to privacy by the growing capability of Internet businesses in collecting, processing and using personal data.⁵⁸⁷ Second, they provide for general points. One is that unlike earlier Resolutions which merely ‘recall’ the human rights responsibility of businesses under the Ruggie Principles, the latest Resolutions definitively state that the Ruggie Principles *apply* to the human right to privacy in the digital context. They do so by calling upon businesses to ‘meet their responsibilities’ under the Guiding principles.⁵⁸⁸ This clarifies an ambiguity in an earlier Resolution which vaguely stated that businesses may owe responsibilities under ‘applicable laws and other international principles’.⁵⁸⁹ It has not been clear what these laws and international principles are, but now is clear that those are the Ruggie Principles, regardless of whether they are adequate to address responsibilities of technology vis-à-vis the right to privacy.

Third, the Resolutions stipulate a set of specific responsibilities of corporations vis-à-vis the right to privacy, as highlighted below:

a. Internet businesses are called upon to inform users about the collection, use, sharing and retention of their personal data when there are risks to the right to privacy.⁵⁹⁰ This provision mirrors many data protection instruments worldwide, but is couched in a vague language. It is not clear, for instance, whether the requirement includes data breach notification to users. The provision also leaves wide latitude to corporations in determining when to inform users.

⁵⁸⁶ See Res 68/167, above n 545, preamble, [4].

⁵⁸⁷ See Res 71/199, above n 526, preamble, [26].

⁵⁸⁸ See Res 73/179, above 545, [7(a)].

⁵⁸⁹ See Res 71/199, above n 526, preamble, [28].

⁵⁹⁰ See Res 73/179, above 545, [7(b)].

b. Internet businesses are ‘encouraged’ to adopt transparency policies on government requests for user data.⁵⁹¹ Part of this undertaking is to reveal the extent and nature of routine requests of personal data made by law enforcement and intelligence agencies. In that sense, it does not seem to involve disclosure at an individual level. Corollary to this proviso is the ‘call’ on States to ensure that ‘gag orders’ — i.e. statutory or judicial orders preventing disclosure — are not unduly imposed on corporations.⁵⁹² The scope of the transparency policy does not, however, appear to specifically cover a ‘right to be notified’ when one has been subject to surveillance, despite the fact that this has been one of the comparative lessons drawn by the report of the OHCHR.⁵⁹³ In practice, transparency reports issued by technology companies are described in a generic sense that individual users are not necessarily notified. If that is the aim of the Resolutions, it would be a significant development but practically cumbersome.

c. Internet businesses are called upon to implement ‘administrative, technical and physical safeguards’ to ensure that processing of personal data is undertaken in line with classic data protection principles of ‘fair and lawful processing’, ‘use limitation’, ‘data quality’ and ‘data security’.⁵⁹⁴ In addition, the Resolutions call upon corporations to ensure that the design, operation and evaluation of automated decision-making technologies such as AI and machine learning respect international privacy standards.⁵⁹⁵ Latent in this proviso is what is called in EU law the principle of ‘data protection by design’ by which data privacy safeguards are imbedded in data processing systems.

d. Internet corporations are encouraged to secure their communications and adopt technical solutions towards safeguarding the right to privacy of their customers.⁵⁹⁶ This could include end-to-end encryption which is increasingly being implemented by some technology companies. This provision is reinforced by a proviso, highlighted above, that calls upon States to (i) offer digital literacy training on privacy enhancing technologies and (ii) to ‘refrain’ from measures that oblige businesses to take steps that interfere with the right to privacy in an unlawful and arbitrary manner.

In summary, the revival of the privacy agenda at the UN through the series of Privacy Resolutions flickers the hope that normative blind spots in the international law of privacy will be lessened. The discourse has brought along a set of novelties, both of substance and approach, that may assist in that effort. But, what has been

⁵⁹¹ *Id.*

⁵⁹² *Id.*, [6(m)]

⁵⁹³ See Report of the High Commissioner, above n 193, [40].

⁵⁹⁴ See Res 73/179, above 545, [7(c)].

⁵⁹⁵ *Ibid.*, [7(d)].

⁵⁹⁶ *Ibid.*, [8]

introduced so far does not go far enough in sufficiently attending to international law's privacy problem. As shall be demonstrated in the following section, the normative values of the discourse, particularly the Privacy Resolutions, is limited in reimagining the right to privacy in international law.

III THE ROLE OF THE PRIVACY DISCOURSE IN REIMAGINING INTERNATIONAL LAW OF PRIVACY

To what extent do the above highlighted novelties of the privacy discourse contribute towards reimagining the right to privacy in international law? To address this question, three potential roles of the discourse are examined. First, it considers two possible 'freestanding roles' of the discourse. One concerns the possibility that the Privacy Resolutions' substantive principles may offer normative guidance on the scope of the right to privacy in the digital context. The other is whether the Privacy Resolutions constitute 'authoritative interpretation' of Article 17 of the ICCPR. As will be shown, these unilateral roles of the privacy discourse are insignificant. This is mainly due to the limited normative reach of the Resolutions, and attendant questions of competence. Second, it considers the 'contributory role' of the Resolutions in offering the possibility by which a general right to privacy may be grounded in general international law, thereby broadening its scope of application. This contributory role not only carries limited legal significance but also will prove controversial. Third, it considers the 'catalytic' role of the discourse in charting new directions towards a pragmatic privacy law reform.

A Freestanding Role: Elaborative and Interpretive Functions

1 The Privacy Resolutions as Elaborative Soft Law

Soft law historically played a key role in illuminating otherwise crude provisions of international (hard) laws. As Shelton notes, soft law often formulates and reformulates hard law particularly in applying the latter to new circumstances.⁵⁹⁷ Soft law enunciates broad principles in new areas of lawmaking where details of obligations remain to be elaborated.⁵⁹⁸ Resolutions of the UNGA are good cases in point in clarifying rules of international law to specific and unique set of circumstances.⁵⁹⁹ To a degree, the Privacy Resolutions appear to assume a similar elaborative role. As discussed above, they tend to provide some content to existing international rules on the right to privacy. The rather vague and high-level abstract

⁵⁹⁷ Dinah Shelton, 'Commentary and Conclusions' in Shelton (ed), above n 327, 461.

⁵⁹⁸ Ibid.

⁵⁹⁹ See, e.g., Jutaro Higashi, 'The Role of Resolutions of the United Nations General Assembly in the Formative Process of International Customary Law' (1982) 25 *Japanese Annual of International Law* 11, 16.

principles of Article 17 of the ICCPR and UN Data Privacy Guidelines find some specificity in the Privacy Resolutions.

Peters comments that the initial Privacy Resolution does not create new law but ‘merely clarifies’ existing rules such as the ICCPR’s privacy provision to the Internet context.⁶⁰⁰ But what the initial Resolution does, as noted above, was perhaps a little less than clarifying, which rather is done so, to some extent, in the subsequent Resolutions. The more recent Resolutions embody some substantive privacy principles and specify the respective roles of States and corporations vis-à-vis the right to privacy. In that sense, they appear to be what Chinkin refers to as ‘elaborative soft law’, one that offers some content to and interacts with treaty law.⁶⁰¹ The repeated reaffirmation of and reference to privacy provisions of the UDHR and the ICCPR attest to the slightly ‘elaborative soft law’ nature of the Privacy Resolutions.

A primary advantage of an elaborative soft law is that it offers some normative guidance to judicial bodies in charge of monitoring implementation. In that sense, the addition of some flesh to the skeletal provisions of the international law of privacy would offer some guidance to, for example the HR Committee. The elaborative function would be useful to the Committee in examining individual communications, periodic State reports and even in revising GC 16. Resort by the Committee to an elaborative soft law adopted by the UNGA will be much less controversial than a comparative lesson drawn by the Committee from, say, the ECtHR.⁶⁰² States would be more heedful to principles invoked from UN instruments like the Privacy Resolutions than the jurisprudence of the ECtHR when the Committee makes legal determinations.

Another advantage of an elaborative soft law is that in interacting with and referring to hard law, a soft law imports some legal authority. Resolutions like the Privacy Resolutions that are tied to a hard law instrument like the ICCPR derive authority from the latter.⁶⁰³ Boyle and Chinkin suggest that the application of Resolutions – which inherently are soft laws, and hence interaction with hard laws – by judicial and quasi-judicial bodies alters their legal nature to some degree.⁶⁰⁴ This may be called ‘judicial hardening of soft law’ in that the soft nature of some instruments is, in practice, hardened by judicial and quasi-judicial interpretation of the

⁶⁰⁰ Anne Peters, ‘Surveillance Without Borders: The Unlawfulness of the NSA Panopticon — Part II’ *on EJIL: Talk!* (4 November 2013) <<http://bit.ly/2vElrhK>>

⁶⁰¹ Chinkin, above n 327, 30.

⁶⁰² Other UN institutional arrangements relevant to privacy may also draw upon the Resolutions. In a recent report, the SRP noted that his work is being ‘guided by’ a Privacy Resolution adopted by the HR Council. See *Report of the Special Rapporteur on the Right to Privacy, Joseph Cannataci*, UN Doc A/HRC/37/62 (28 February 2018) [5].

⁶⁰³ See Chinkin, above n 327, 30.

⁶⁰⁴ Boyle and Chinkin, above n 509, 213, 220.

rules.⁶⁰⁵ According to this viewpoint, possible reference to or application of the Privacy Resolutions by the HR Committee in its practice would elevate their legal status.

Indeed, the Committee has a tradition of relying on relevant soft law instruments in interpreting the ICCPR. In the case of *Herbert Potter v New Zealand*, the HR Committee, for instance, relied upon – as submitted by the author of the individual communications but objected by the respondent State – a soft law on prisoners' rights in finding violation of Covenant Rights.⁶⁰⁶ The Committee not only asserted its competence to such extraneous soft law instrument but also noted that the Rules provided 'valuable guidelines' for the interpretation of the ICCPR.⁶⁰⁷ However, in view of the fact that HR Committee's views in individual cases or concluding observations under the reporting procedure are clearly non-binding on States, the supposition that a soft law may be hardened when applied by the Committee seems to be logically fallacious.

Practical influences of the Privacy Resolutions in the jurisprudence of the HR Committee is yet to fully emerge. But it is already clear that the spirit of the Resolutions has started to show in the Committee's jurisprudence, particularly through recent concluding observations. As discussed in chapter 1, concluding observations adopted in the wake of the Snowden revelations – and hence the Privacy Resolutions – appear to be informed by themes of the Resolutions. The Privacy Resolutions are also considered by judicial bodies outside the UN, but it is yet to go beyond mere reference. An example is that the initial Resolution has been listed by the ECtHR among 'applicable international laws' in recent cases on digital surveillances.⁶⁰⁸

In sum, the elaborative role of the Privacy Resolutions is yet to be fully seen in action. This state of affairs is probably because the substance of the Resolutions is not significant enough to warrant much reference. In the case of ECtHR, which has a far more advanced privacy jurisprudence, the lack of reference is unsurprising. New Zealand's objection, alluded to above, also reflects the attendant question of competence when an extraneous instrument is referred to by the Committee. But more importantly, the evolving nature of the discourse means also that the elaborative function of the Resolutions may elapse without exerting much effect.

⁶⁰⁵ See Dinah Shelton, 'Introduction: Law, Non-Law and the Problem of Soft Law' in Shelton (ed), above n 317, 14.

⁶⁰⁶ HR Committee, *Herbert Potter v New Zealand* (Communication No. 632/1995, 6 April 1995) [4.5], [6.3].

⁶⁰⁷ Ibid cum *UN Standard Minimum Rules for the Treatment of Prisoners (Nelson Mandela Rules)*, GA Res 70/175, 70th sess, Agenda Item 106, UN Doc A/RES/70/175 (17 December 2015).

⁶⁰⁸ See, e.g., *Roman Zakharov v Russia* (ECtHR, Application No. 47143/06, 4 December 2015) [139].

2 The Privacy Resolutions as Authoritative Interpretation of Art 17 ICCPR

The other possibility by which the Privacy Resolutions may find a meaningful place in international privacy law, or obtain some legal force, is based on what may be called the 'authoritative interpretation' analogy. The analogy flows from the more general view that soft law may be a mechanism of authoritative interpretation or 'amplification' of treaty law.⁶⁰⁹ Claims of treaty law interpretation through soft law take various forms. In the context of the UN Charter for instance, Schachter suggested that if States agree that the 'Charter means what the Resolution says it states', the Resolution may be regarded as an authoritative interpretation of the Charter.⁶¹⁰ The UDHR, a soft law adopted by a Resolution of the UNGA, is often presented to support such claims.

UDHR's non-binding nature and the failure of universal ratification of binding treaties like the ICCPR, inter alia, brought the claim that the Declaration acquires legally binding force because it represents an authoritative interpretation of the UN Charter's human rights provisions, which is binding.⁶¹¹ The Charter's provisions on human rights are general and basically affirm the importance of respect for and promotion of human rights than specific catalogue of human rights and concomitant obligations.⁶¹² The UDHR specifies, the argument goes, these provisions into a specific list of rights and obligations of Member States, which in turn represent authoritative interpretation of the Charter's human rights provisos. The 'authoritative' nature of the interpretation derives from the fact that the UDHR was adopted by the UNGA which is considered to be a forum for the consideration and expression of the collective will of the international community.

If that claim were to be analogised to the Privacy Resolutions, it would mean that they constitute an authoritative interpretations of relevant privacy provisions in international (hard) law. The general inclination to use the term 'Resolution' in referring to Declarations such as the UDHR, added with the affirmation by the UN that no difference exists, as a matter of strict legal principle, between a Declaration and a Recommendation (i.e. Resolution)⁶¹³ tends to make the analogy an appealing line of argument towards adding normative force to the Privacy Resolutions. The question, then, is if the UDHR is an 'authoritative interpretation' the UN Charter, could the Privacy Resolutions – as hybrid as they are in their legal form and substance – be considered 'authoritative interpretations' of the ICCPR's privacy

⁶⁰⁹ See Boyle and Chinkin, above n 509, 216.

⁶¹⁰ Oscar Schachter, *International Law in Theory and Practice* (Martinus Nijhoff Publishers, 1991) 85.

⁶¹¹ See Ronald Burke and James Kirby, 'The Universal Declaration of Human Rights: Politics and Provisions (1945-1948)' in Gerd Oberleitner (ed), *International Human Rights Institutions, Tribunals and Courts* (Springer, 2018) 43-44; see also Humphrey, above n 141, 357.

⁶¹² UN Charter, above n 118, arts 1(3), 13, 55, 62, 68, 76.

⁶¹³ See *Use of the Terms "Declaration" and "Recommendation"*, Memorandum by the Office of Legal Affairs, UN Doc E/CN.4/L.610 (2 April 1962).

provision, other subsequent specialized human rights treaties and/or even the human rights provisions of the UN Charter? The repeated references in the Privacy Resolutions to the UDHR and ICCPR as well as their privacy provisions appear to lend weight to the claim. Moreover, the reference made by each Resolution to the UN Charter in the preamble may also add to a view that the Resolutions are not just authoritative interpretations of the privacy provisions of the UDHR and the ICCPR but also the generic human rights provisions of the UN Charter.

The analogy, however, gives rise to a question of legitimacy. Can a soft law instrument interpret provisions of a treaty and to what extent parties to that treaty will be bound by the interpretation? Can they refuse to accept interpretation that goes beyond the original intentions of State Parties to the treaty? Would States that objected the adoption of the soft law or simply abstained during voting be bound by it? The Privacy Resolutions are, as highlighted above, adopted through consensus and hence without any express disclosure of agreement equivalent to affirmative votes. Should that be taken as implied agreement, and hence be bound by the Resolutions' 'interpretations'? Moreover, in engaging in an interpretive exercise, would not UNGA be doing both lawmaking and judicial interpretations?

Lauterpacht was at the forefront of the objection to the analogy. He argued that the analogy not only is illogical but also that aligning UDHR's legal force with the Charter would diminish the latter's inherent legal standing.⁶¹⁴ In considering the fact that a proposal to give the UNGA a legislative power was rejected, the suggestion that UNGA would somehow gain a legislative power through the adoption of a Resolution appears to be extraordinary. In short, the attempt to attach some normative value to the Privacy Resolutions via the analogy of 'authoritative interpretation' would prove controversial. If the analogy has not entirely succeeded in altering the legal nature of an instrument as widely accepted as the UDHR, it would be more farfetched for mere Resolutions (not even a Declaration!) like the Privacy Resolutions riddled with ambiguities.

B Contributory Role: Towards Universalizing Privacy Standards

The Contributory role relates to the way in which the Privacy Resolutions may shape or inform the progressive development of privacy law. It can be considered from two perspectives. One is the possibility of the Resolutions leading to the formation of privacy norms in general international law, either as a customary norm or general principles of law. The other is the extent to which the discourse in general and the Resolutions in particular may influence the making of law and judicial decisions at domestic and regional levels. This section will show that legal significance of the contributory role is limited and shrouded in uncertainty.

⁶¹⁴ Lauterpacht, above n 126, 394 et seq.

1 Accretion of General International Law (of Privacy)

The question of whether the Privacy Resolutions contribute towards grounding the right to privacy in general international law is worthy of consideration for the following reasons. First, grounding rights or principles in international law would broaden the scope and impact of human rights especially when human rights treaties have not achieved universal ratification.⁶¹⁵ A general rule of international privacy law would apply to all States regardless to whether they are parties to treaty law. This would mean that States like China that have not ratified the ICCPR would be obliged, for instance, under a customary privacy norm. It is also important even in cases where treaties are ratified but may be derogated by legislation due to the same hierarchy that treaties and any other legislation enjoy in a State party's constitutional law.⁶¹⁶

Second – and relatedly, solidifying a given human right in general international law would be a way of emphasising the importance of the respective right.⁶¹⁷ Because a rule of customary international law norm, for instance, emerges after extensive State practices over a period of time, its ultimate formation reflects the prominence of the rule and the right that it guarantees. Third, the crystallization of human rights norms into customary law would allow recourse to remedies available in general international law by those whose rights have been violated.⁶¹⁸ Fourth, variations in the interpretation of treaty provisions would be mitigated once a customary norm crystallizes as it would add a level of certainty to the scope of that particular rule of law.⁶¹⁹ This is in addition to the benefits of a general international law rule to serve as a 'fall back' when interpretation of treaties proves difficult.⁶²⁰ Finally, a customary rule of international law moulds the content of treaty law which might not otherwise be amended to keep up to speed with new developments.⁶²¹ The latter especially is appealing to the right to privacy in the digital space where there is incessant dynamics.

The attempt at linking UNGA Resolutions with formal sources of international law emanates from their uncertain place in international law. Resolutions find no

⁶¹⁵ See Bruno Simma and Philip Alston, 'The Sources of Human Rights Law: Custom, Jus Cogens and General Principles' (1992) 12 *Australian Yearbook of International Law* 82, 82.

⁶¹⁶ Ibid, 86.

⁶¹⁷ See Michael O'Boyle and Michelle Lafferty, 'General Principles and Constitutions as Sources of Human Rights Law' in Dinah Shelton (ed), *The Oxford Handbook of International Human Rights Law* (Oxford University Press, 2013) 209.

⁶¹⁸ See Schachter, above n 610, 85.

⁶¹⁹ See Pierre-Marie Dupuy, 'Formation of Customary International Law and General Principles' in Daniel Dobansky et al (eds) *Oxford Handbook of International Environmental Law* (Oxford University Press, 2007) 463.

⁶²⁰ Ibid, 450.

⁶²¹ See James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 2012) 33-34.

mention under Art 38(1) of the Statute of the International Court of Justice (ICJ) which is widely accepted to provide an authoritative list of international law sources. But this provision is sometimes taken to have a limited role of guiding the Court than controlling sources of international law, so that Resolutions may be drawn upon by the Court when necessary.⁶²² The list is also argued to be merely an illustrative one, as opposed to exhaustive, which as a result does not preclude Resolutions from sources of international law.⁶²³ Some commentators even situate Resolutions within the ranks of Art 38 as falling just below ‘judicial decisions’ but certainly above ‘teachings of most highly qualified publicists’, which are identified as subsidiary sources of international law under Art 38(1(d)).⁶²⁴ What follows considers how and whether the Privacy Resolutions may find a place in general international law. It does so by looking at how Resolutions may facilitate the formation of an international custom and general principles of law.

(a) Customary International Law (of Privacy)

Whether the right to privacy has attained the status of customary international law has recently become a recurring question in the privacy literature. Answers in the affirmative are predominant but take various forms. A more general and older version of the argument departs from the UDHR which, over the years, have had significant impact worldwide. The impact of the Declaration is said to have made all of its provisions, including one on the right to privacy, rules of customary international law.⁶²⁵ This view holds that given the wider incorporation of the UDHR into national constitutions, statutory and case law as well as the very nature of the rights embodied therein, the UDHR is part of customary international law. This would mean that the right to privacy guaranteed under the Declaration and later reproduced, *nigh verbatim*, in the ICCPR is grounded in customary international law. Another but a more recent version of the argument holds that wider recognition of the right to privacy in several international instruments, national laws and the prominence of privacy in legal commentary has paved the way for creation of a ‘general right to privacy’ in customary international law.⁶²⁶

⁶²² See, e.g., Merlin Magallona, ‘Some Remarks on the Legal Character of UN General Assembly Resolutions’ (1976) 5 *Philippine Yearbook of International Law* 84, 96.

⁶²³ See generally Christopher Joyner, ‘UN General Assembly Resolutions and International Law: Rethinking Contemporary Dynamics of Norm-Creation’ (1981) 11 *California Western International Law Journal* 445.

⁶²⁴ See Leo Gross, ‘The United Nations and the Role of Law’ (1965) 19 *International Organization* 537, 557.

⁶²⁵ See John Humphrey, ‘The Universal Declaration of Human Rights: Its History, Impact and Juridical Character’ in Bertrand Ramcharan (ed), *Human Rights Thirty Years After the Universal Declaration* (Brill, 1979) 21, 37; see also Louis Sohn, ‘The Human Rights Law of the Charter’ (1977) 12 *Texas International Law Journal* 129, 129, 133.

⁶²⁶ See Rengel, above n 57, 108. Recent expert reports also claim that the right to privacy has become a rule of customary international law. The Tallinn Manual 2.0, for instance, concluded that despite

This viewpoint is problematic on many levels. At the most basic level, it overestimates the value of a customary norm based on existing international privacy norms. As demonstrated in chapter 1, the right to privacy in international law is formulated in an exceedingly vague and abstract manner. Boundaries of the international right to privacy is then too vague to make its elevation to customary norm appealing. The viewpoint, moreover, tends to settle for less in international privacy law reform.⁶²⁷ Added to inherent the uncertainty and fluidity of customary law, a customary international law of privacy based on the UDHR may not probably be adequate to improve the existing systems of protection. As Lauterpacht argued in the context of the UDHR, the focus in situating Resolutions within the existing formal sources of international law risks retracting the interest in pursuing a rather effective international legislative response.⁶²⁸

Beside the above general contemplation of privacy as a rule of customary international law, the Privacy Resolutions may lend weight to the argument that, indeed, such rules have emerged. Resolutions of UNGA are often seen as incipient steps towards the creation of customary international law.⁶²⁹ Higgins notes that Resolutions provide a rich source of evidence when taken as indications of a general customary law.⁶³⁰ The constitution of the UNGA as a global political organ with universal membership adds weight to its Resolutions. As Higashi notes, Resolutions of the UNGA are expressions of the ‘collective will of the international community’, reflective of ‘collective practices of States’.⁶³¹ As such, they would facilitate formation of customary international law.

It has recently been suggested, this regard, that the adoption of Privacy Resolutions and preparation of reports by UN bodies such as OHCHR are adequate to show *opinio juris* under modern theories of custom. The Resolutions, the argument goes, demonstrate consensus on the importance of data privacy and could be interpreted under modern custom theories as (1) crystalizing a customary rule of (data) privacy which is needed to keep abreast of new technological developments and (2) demonstrate emergence of consensus on the right to privacy.⁶³² Similar limitations of

some variance on its scope, the right to privacy is of an international customary law character. See Tallinn Manual 2.0, above n 159, 180, 189. But see ‘Annex D: Protection of Personal Data in Transborder Flow of Information’ (Report on the Work of the International Law Commission, 58th sess, May-August 2006) (holding that State practice in the area (of data protection) is not extensive or fully developed, and therefore warrants no further work of codification).

⁶²⁷ See more in the introductory part of the thesis on the limitations of a ‘hard legalization approach’ to privacy reform.

⁶²⁸ Hersch Lauterpacht, ‘The Universal Declaration of Human Rights’ (1948) 25 *British Yearbook of International Law* 354, 376.

⁶²⁹ See, e.g., Joyner, above n 623, 459.

⁶³⁰ Rosalyn Higgins, *The Development of International Law Through the Political Organs of the United Nations* (Oxford University Press, 1963) 5.

⁶³¹ Higashi, above n 599, 13-15.

⁶³² See Zalnieriute, above n 57, 121 et seqq.

the first set of views extends to this line of argument, however. What added value, if at all, would flow from the creation of a customary (data) privacy norm based on existing international human rights instruments is not entirely clear.

Overall, the contention that the right to privacy has developed into a norm of customary international law appears to be misplaced in the context of the Privacy Resolutions. The fact that existing international privacy rules, particularly Article 17 of the Covenant, are binding on the vast majority of States reduces the promises of customary international law of privacy. The argument would have held more water if the supposed customary rule would introduce more robust and progressive rules rather than sheer reinforcement of treaty law. Perhaps, the modest content introduced by the Privacy Resolutions might, if they were to facilitate the formation of customary privacy norms, come handy to support the argument.

But again, this would be to overlook the evolving nature of the Resolutions. In other words, an argument for a customary international law of privacy induced by the Resolutions would have made more sense had the discourse already culminated. But it has not. Another possibility would have been if, for instance, the HR Committee relies upon the Resolutions in its jurisprudence but faces objection from States claiming that they are not bound by the provisions of the Resolutions. In the latter case, the Committee may rely on the above arguments, or one of them, to insist that the Resolutions apply to State parties to the ICCPR. This has not yet occurred and perhaps objections of those types may not arise, probably ever.

(b) General Principles of (Privacy) Law

General principles of law recognized by civilized nations are the other sources of international law next to consent-based sources of treaty and customary law.⁶³³ When it comes to the right to privacy in the digital context, two threshold questions arise regarding the role of general principles. One is whether the substantive principles flagged in the Privacy Resolutions constitute general principles of privacy law and secondly, whether general principles of law could ever be sources of international privacy law at all. This source of international law is often considered to have fell into disuse due to proliferation of treaties and development of customary norms that address most areas of international regulation.⁶³⁴ Perhaps, the absence of a comprehensive and binding international data privacy instrument may lend weight to an argument on the need to revitalizing general principles in the privacy field. What follows weighs the tenability of the argument.

There are generally two perspectives on the nature of general principles which we might call 'traditionalist' and 'modernist' perspectives. The traditionalist perspective

⁶³³ See *Statute of the International Court of Justice* (1948) art 38(1(c)).

⁶³⁴ See, e.g., Gennady Danileko, *Law-Making in the International Community* (Martinus Nijhoff Publishers, 1993) 181.

defines the scope and nature of general principles in light of the original intent behind them. During the drafting of the Statute of the Permanent Court of International Justice, which later become a Statute to the present Court – i.e. ICJ, the Advisory Committee of Jurists that drafted the Statute was divided as to what these ‘principles’ meant.⁶³⁵ But it was finally agreed that these principles were meant to cover principles of procedure, good faith and other ‘maxims’ of law derived from national legal orders.⁶³⁶ The traditionalist perspective, therefore, restricts the scope of general principles to rules of procedure such as ‘principle of estoppel’ or ‘*res judicata*’, ‘good faith’, ‘*pacta sunt servanda*’, and other rules of fair procedure that are common to most legal systems.⁶³⁷ This nature of general principles appears to readily exclude substantive principles. As such, they aim to offer interpretative aid when (substantive) provisions of treaty law or structure of customary norms are found to be complex.⁶³⁸ The traditionalist perspective further restricts the purpose of general principles to be a ‘fall back’ when there are gaps in treaty or customary law.⁶³⁹ This will most likely be in new areas of law where State practice is yet to extensively emerge or treaty law is adopted.⁶⁴⁰ The heterogeneous nature of the international community would also mean that commonly shared principles are few and far between.⁶⁴¹

Privacy would not fare well under the traditional perspective. One obstacle relates to the very nature of this source of general international law. These principles of law, as noted above, concern age-old principles of law. Privacy principles especially those that apply in the digital space are relatively recent, and the extent of their wider acceptance is contestable. The other concerns the conventionally ‘procedural’, as opposed to substantive, nature of general principles of law. Even if they are widely accepted, that digital privacy principles are mostly substantive reduces their candidacy to general principles of law. Scenarios where general principles might come into play in privacy cases, per the traditional formulae, are thus likely to be few, if not none.

The modernist perspective pursues a liberal path as to the nature and scope of general principles in moving beyond the procedural nature of such principles. O’Boyle and Lafferty, for instance, write that ‘respect for fundamental rights’

⁶³⁵ Ibid, 173-174.

⁶³⁶ Ibid, 174-175.

⁶³⁷ See, e.g., Gregory Kerwin, ‘The Role of United Nations General Assembly Resolutions in Determining Principles of International Law in US Courts’ (1983) 32 *Duke Law Journal* 876, 878.

⁶³⁸ See Bleicher, above n 552, 451.

⁶³⁹ See Kerwin, above n 637, 878.

⁶⁴⁰ See Beatrice Bonafe and Paolo Palchetti, ‘Relying on General Principles in International Law’ in Catherine Brölmann and Yannick Radi (eds), *Research Handbook on the Theory and Practice of International Law Making* (Edward Elgar, 2016) 172.

⁶⁴¹ See Danileko, above n 634, 180-181.

constitutes a general principle of international law.⁶⁴² And UNGA Resolutions, particularly Declarative Resolutions, constitute important sources of general principles.⁶⁴³ The UDHR particularly is said to enunciate general principles of law.⁶⁴⁴ For Ramcharan, general principles of law can be deduced from various sources, including national law and jurisprudence as well as from numerous declarations, bodies of principles and guidelines adopted by the UN.⁶⁴⁵ In his dissenting opinion in *South West Africa Case*, Justice Tanka of Japan argued that the universal nature of human rights *ipso facto* makes their protection general principles of law.⁶⁴⁶ A more recent version of the modernist perspective holds that principles of privacy law recognized in the private law of major legal traditions constitute general principles of law.⁶⁴⁷

However, the possibility of relating the right to privacy and the Privacy Resolutions to general principles, despite the promises of the modernist approach, faces a fundamental obstacle. This transpires from the very nature of general principles in that they come into play in the context of inter-State relations, as opposed to State-individual relations. The right to privacy falls in the latter. Overall, any attempt to extend the applicability of the general principles to privacy would be an extraordinary over-stretch. To argue that the proliferation of (data) privacy laws and constitutional privacy provisions in several national legal systems creates general principles of law will be to near rewriting sources of general international law. This barrier, added to the normative limits of the Privacy Resolutions, downplays the place of general (privacy) principles in international privacy law.

2 Cross-fertilizing Global Privacy Norms

The other possible contributory role for the privacy discourse is inspiring the making of law and judicial decisions at domestic and regional levels. As discussed in section II above, the content of the Privacy Resolutions is, to some degree, a result of cross-fertilization of norms drawn from multiple sources. From domestic privacy law and decisions of regional human rights courts to IBRs, the Privacy Resolutions synthesis modern privacy norms. This potential role of the Resolutions is important, at least theoretically, because the level of privacy protection in the world over is hardly approximate. While Europe has the most advanced privacy regime espoused through progressive legislation and regional courts, less is the case in other parts of the world. As discussed in chapter 2, even the recent proliferation of data privacy

⁶⁴² See O'Boyle and Lafferty, above n 617, 196.

⁶⁴³ Ibid, 207.

⁶⁴⁴ See Humphrey, above n 141, 357.

⁶⁴⁵ Bertrand Ramcharan, 'The Law-Making Process: From Declaration to Treaty and Custom' in Shelton (ed), above n 617, 514.

⁶⁴⁶ Dissenting Opinion of Judge Tanka in *South West Africa (Ethiopia v. South Africa)* [1962] ICJ Reports 319, 292-299.

⁶⁴⁷ See Sourgens, above n 58, 367-392.

legislation in some parts of the world is yet to be complemented by independent and well-resourced monitoring agencies.

In the light of this landscape of global privacy legislation, the role of a universal soft law like the Privacy Resolution in lessening the gap seems appealing. But importantly, the Resolutions' tendency of flagging the roles/obligations of Internet corporations as well as States brings forward some novelties worth transposing to domestic legal regimes. Partly because the discourse is still ongoing – and the short time since it began, the extent to which the Resolutions have shaped lawmaking or judicial decisions at national or regional level is limited. An additional reason for this lack of influence may be the limited substantive scope of the Resolutions. That the Resolutions are by-products of an inchoate and hence evolving discourse means that the reference to its narrow set of privacy principles would be lesser.

Little is known as to the actual and direct, if ever, impact of the Resolutions in domestic law. Perhaps, the signing of Presidential Policy Directive (PPD)28 by the former US President Barack Obama is remotely one example of the influence. The Directive partly addresses discriminatory nature of the US digital surveillance legal regime, albeit half-heartedly.⁶⁴⁸ Half-heartedly because the Directive simply recognizes the 'privacy interests' of non-US persons, thereby avoiding a human rights language, and its attendant implications. Its preambular paragraph partly reads:

In addition, our signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information.⁶⁴⁹

The adoption later of the FREEDOM Act may also be seen as a reflection of UN Resolutions' effect, although adopted as a way of re-enacting the PATRIOT Act which was then expiring. The Act introduced some privacy safeguards such as the prohibition of bulk collection of phone record or metadata of 'Americans', restriction of the collection of data, permission to Internet companies to disclose the number of orders to hand over user data under the Foreign Intelligence Surveillance Act and creation of a public advocate before the Foreign Intelligence Surveillance Court for certain novel cases to represent public interest.⁶⁵⁰ Some of these principles particularly those relating to gag orders have found expression in the later Privacy Resolutions, as discussed in Section II above. But again, the Directive was more a result of the political fallout and public outrage against US intelligence practices exposed by Snowden than a product of the discourse. Moreover, apart from the

⁶⁴⁸ See David Fidler, 'Cyberspace and Human Rights' in Tsagourias and Buchan (eds), above n 101, 114.

⁶⁴⁹ *Presidential Policy Directive 28: Signals Intelligence Activities* (17 January 2018) <<https://bit.ly/2P08kOI>>

⁶⁵⁰ *FREEDOM Act* of 2015, Pub L No 114-23, 129 Stat 268, §§ 103, 201, 401, 501, 603.

general recognition of aliens' privacy interests in the Directive, the above noted privacy-protective provisions of the Freedom Act apply to American citizens and residents.

Another remote example is the 2017 draft EU e-Privacy Regulation which codified recurring themes in the Privacy Resolutions. Amendment 116 to Article 17 of the proposed Regulation provided that States must refrain from requiring corporations to take measures weakening encryption.⁶⁵¹ Moreover, it required corporations to notify end users when there is risk to security of their networks and services and, where applicable, provide remedies.⁶⁵² The former proviso corresponds to a paragraph in the Privacy Resolutions which calls upon States to 'refrain from requiring business enterprises to take steps that interfere with the right to privacy in an arbitrary or unlawful way'.⁶⁵³ Another paragraph in the Resolutions also resembles the latter proviso which calls up on businesses to 'inform users about the collection, use, sharing and retention of their data that may affect their right to privacy and to establish transparency policies, as appropriate'.⁶⁵⁴ But, the latest version of the draft Regulation, released in May 2018, removed those provisions for unknown reasons.

Judicial references to the Resolutions have also been limited. In a number of its decisions pronounced after the Snowden debacle, the ECtHR has been incorporating the initial Resolution in a section of judgment where it lists 'relevant international law'.⁶⁵⁵ It reproduces two paragraphs from the first Privacy Resolution that urge States to align their domestic laws with international human rights standards and introduce independent oversight mechanisms. Nothing of substance is thus contained in those referenced paragraphs. While listing the Resolution is a positive gesture particularly in recognizing its status as a pertinent international (soft) law, it was essentially inconsequential in the decision making. Inconsequential because not only did the Court not engage with the Resolution but also reference is still to the merely hortatory initial Resolution. As noted above, subsequent Resolutions have become more substantive than the original one which, though, importantly charted the discussions. The reference to a now older, and less significant, Resolution manifests the basically symbolic nature of its mention in the Court's judgments.

At the international level, the impact of the UN privacy discourse was simply stimulative. Since the discourse was set in motion, the Committee's reporting procedure has seen a spike in the number of comments on States digital surveillance

⁶⁵¹ *Draft Report on the Proposed e-Privacy Regulation* (Committee on Civil Liberties, Justice and Home Affairs, 2017/0003(COD), 9 June 2017) amendment 116 to art 17.

⁶⁵² *Ibid*, amendment 117 to art 17.

⁶⁵³ See, e.g., Res 73/179, above n 545, [6(l)]

⁶⁵⁴ *Ibid*, [7(b)].

⁶⁵⁵ See, e.g., *Big Brother Watch and Others v UK* (ECtHR, Application Nos. 58170/13, 62322/14 and 24960/15, 13 September 2018) [201-202].

practices. As discussed in chapter 1, a recent independent survey by a member of the HR Committee reveals that concluding observations relating to digital surveillance have increased by 25% since the Snowden debacle.⁶⁵⁶ But the brief nature of concluding observations means that detailed substantive principles cannot be considered in them. The most that could come out of concluding observations is that a new GC may later be developed by the Committee. And whether such a GC will be developed, and how fast is uncertain, as already submitted.

To summarize the above discussion, partly due to the nature and the narrow normative scope of the Resolutions, their level of influence in shaping the development of law at regional or domestic level, or even in informing judicial decisions, has been limited. This makes the contributory role of the privacy discourse in cross-fertilizing global privacy norms insignificant. This leaves us with the third, and probably the most meaningful role: catalytic role, considered immediately below.

C Catalytic Role: Prospects of Charting Normative and Methodological Directions

A more tangible role for the ongoing UN privacy discourse is its potential of spurring a more pragmatic approach to international law of privacy. The catalytic role of the discourse has two mutually reinforcing strands. One is that the discourse charts a process which, its problems notwithstanding, may be instrumental in the progressive development of international privacy law. The political capital witnessed since the start of the discussions at the UN can be geared towards pragmatic rethinking of the right to privacy in international law. The second relates to the innovative approaches to privacy pursued, albeit with some limitations, in the Resolutions. This relates to the unifying way in which the right to privacy is envisioned and the fiat given to a multi-stakeholder approach to privacy. What follows discusses these two aspects of the discourse.

1 Political Capital for Meaningful Reform

The political capital shown over the past few years in the UN privacy discussions cannot simply be dismissed as reactive, temporal, and hence negligible. But what is a 'political capital' and what is its role in reimagining current international law of privacy in the digital age? The term 'political capital' is a term of art, niche to the field of political science; but its technical definition essentially captures what is intended here.⁶⁵⁷ For purposes of the discussion here, the term is meant to represent the symbolic value of the ongoing UN privacy discourse, particularly the Privacy

⁶⁵⁶ See Shany, above n 244.

⁶⁵⁷ Political scientist Bourdieu, for instance, defines it as 'a form of symbolic capital, credit founded on credence or belief and recognition'. See Pierre Bourdieu, 'Political Representation: Elements for a Theory of the Political Field' in Pierre Bourdieu (ed), *Language and Symbolic Power* (Polity Press, 1991) 192.

Resolutions, in setting the agenda of reimagining the scope and meaning of right to privacy in international law in the light of the new realities of the digital age.

In that light, a prime significance of the discourse is that it has initiated a conversation on the way how best to secure digital privacy.⁶⁵⁸ With the initiation of a conversation particularly at the UN level, and remarkably in a sustained way for over five years, the discourse presents the opportunity for gradual but meaningful international legislative response. The significant level of support that the adoption of the Resolutions has received among many States, added to the strong civil society engagement with the discourse, reflects the existence of some political capital and hence political will for reform. Long-term and practical legislative measures may gradually grow out of the discourse should the political will lingers long enough, and exploited judiciously.

In international lawmaking, there are several precedents where a discourse charted in a UNGA Resolution ultimately grew into tangible legislative outcomes. In new areas of international legalization, the work often begins with a Resolution than a treaty.⁶⁵⁹ More particularly, resort is made to soft law when the subject matter in question is new and a proper response is yet to be determined.⁶⁶⁰ Soft legalization, in such instances, is opted to initiate a conversation on the subject until a long-term normative response is developed.⁶⁶¹ The passing of a Resolution on a given subject matter, on its own right, gives rise to the need for some form of new regulation, and hence opens the door for further engagement.⁶⁶² As a stepping stone towards broader normative measures, the adoption of a soft law has also the advantage of avoiding possible 'anxieties of dealing with something new' in international regulation.⁶⁶³ In that sense, a soft law prepares the stage for a long-term process of reform.

The progressive development of international space law probably offers an instructive example. UN work in the field of the Outer Space begun with a UNGA Resolution on the Outer Space adopted in 1961,⁶⁶⁴ which later was followed by a Declaration in 1963.⁶⁶⁵ The Declaration, then, found translation into a number of

⁶⁵⁸ Of a related view, see Milanovic, above n 203, 85.

⁶⁵⁹ See Higashi, above n 599, 16

⁶⁶⁰ See Shelton, above n 605, 13.

⁶⁶¹ See Kenneth Abbott and Duncan Snidal, 'Hard and Soft Law in International Governance' (2000) 54 *International Organization* 421, 423.

⁶⁶² See Joyner, above n 623, 463-464.

⁶⁶³ See Boyle and Chinkin, above n 509, 227.

⁶⁶⁴ See *International Co-operation in the Peaceful Uses of Outer Space*, GA Res 1721 (XVI)A-E, 1085th plenary mtg, UN Doc RES/1721(XVI) (20 December 1961).

⁶⁶⁵ See *Declaration of Legal Principles Governing the Activities of States in the Exploration and Uses of the Outer Space*, GA Res 1962 (XVIII), 18th sess, Agenda item 28a, UN Doc A/Res/18/1962 (13 December 1963).

multilateral treaties.⁶⁶⁶ Following this track, the conversation that involved the adoption of a series of Privacy Resolutions may culminate in one or more treaty law, or may just conclude with a soft law. Whether the conversation started by the Privacy Resolutions will, like the Outer Space discourse, will progressively develop privacy law is uncertain. The underlying argument advanced in this thesis is that progressive development of international privacy law is needed in light of the new realities of the digital age. But, the approach towards achieving such progress must be pragmatic in that it must go beyond the rather common hard legalization paradigm in the privacy literature.⁶⁶⁷ Chapters 5 and 6 lay out the structures of the pragmatic approach to international privacy law, but it suffices to state here that the path taken by the UN regime on the Outer Space is not the best way forward for the right to privacy in digital age. With that said, there are still three aspects of the privacy discourse that diminish their catalytic role: lack of thematic focus, ambiguous formulation of provisions and uncertainty of scope.

Lack of thematic focus is patent in the Resolutions' increasing tendency to address themes that go beyond the right to privacy. Such loss of direction is reflected in the way in which the Resolutions import topics from other parallel discourses at the UN. One example is the emphasis on the role of ICTs for the attainment of the SDGs.⁶⁶⁸ The issue of SDGs is a broad and cross-cutting theme at the UN in contrast with the rather specific subject of digital privacy. Cybersecurity is another theme, currently in vogue, at the UN which the privacy discourse picks up. Para 5 of Resolution 73/179 of the UNGA, for instance, urges States to 'promote an open, secure, stable, accessible and peaceful' ICTs environment based on respect for international law'.⁶⁶⁹ Themes from the ongoing discussions at the HR Council on the right to free speech online, highlighted earlier, are also slowly creeping into the privacy discourse. For example, a preambular paragraph raises the 'fake news' phenomenon, a theme covered in the free speech Resolutions of the HR Council.⁶⁷⁰

The concern is that the central goal of the Privacy Resolutions might be side-tracked by the above issues. When one considers the long-running controversy about those themes in the Internet governance discourse, the evolution of the Privacy Resolutions may be frustrated by the lack of thematic focus and ambivalence of path. The more the privacy discourse cherry picks themes from other, albeit remotely related themes, the less core privacy themes find proper stipulation in the Privacy Resolutions and perhaps ultimately in the instrument where/if the discourse

⁶⁶⁶ See, e.g., *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, opened for signature 27 January 1967 (entered into force 10 October).

⁶⁶⁷ See the introductory part of the thesis.

⁶⁶⁸ See, e.g., Res 73/179, above n 545, [2].

⁶⁶⁹ *Ibid*, [5].

⁶⁷⁰ *Ibid*, preamble, [23].

culminates. In practical terms, such a future instrument might end up failing to adequately reimagine current international law of privacy in the digital age.

Ambiguous formulations are also visible when one compares the elaborative tendency of the Resolutions, on the one hand, and vague cross-referencing of ‘obligations under international human rights law’ on the other. UNGA’s Resolution 73/179 in para 6(b), for instance, calls upon States:

‘to take measures to put an end to violations of the right to privacy (...) including by ensuring that relevant national legislation complies with their obligations under international human rights law’.

Such phraseology is commonplace in the Privacy Resolutions. But the question of what these obligations are, in specific terms, remains. In considering the vaguely worded provision of the right to privacy in the ICCPR and the dearth in treaty body jurisprudence, the cross-reference to obligation in international human rights law makes little sense. But at a higher level, the Resolutions’ consistent call for States to align their domestic laws, procedures and practices with international law – the content of which is either uncertain or absent – is that they may, if implemented by States, lead to an incoherent mosaic of domestic laws and practices. The risk is not of just being ignored by States but also that they may be translated into real measures in a divergent manner. In the digital context where privacy threats are transnational in nature, the need for comparable and harmonized privacy safeguards worldwide cannot be overemphasised.

A common premise that underpins all the Privacy Resolutions is that international human rights law provides a sound basis for the protection of the right to privacy in the digital age.⁶⁷¹ But again, they note the need to further discuss specific principles. They, for instance, provide that there is a need to ‘further discuss and analyse based on international human rights law’, specific issues and principles surrounding digital privacy rights such as the ‘principles of non-arbitrariness and lawfulness’.⁶⁷² This is often reinforced by a concluding paragraph that ‘encourages’ further discussion to identify best practices, in addition to ‘clarifying existing principles and standards’, on the right to privacy.⁶⁷³ These phrases reveal a sense of ambivalence in upholding the adequacy of existing international privacy norms while simultaneously acknowledging the need to examine those norms if they still are fit for purpose to the digital context as well as to look out for best practices. This suggests the ambivalence of the discourse that may reduce its catalytic role.

The thematic approach of the Resolutions – i.e. ‘communication surveillance, interception and collection of personal data’ – is also misleading. It sends the signal

⁶⁷¹ See also ch 1.

⁶⁷² See, e.g., Res 73/179, above n 545, preamble, [11].

⁶⁷³ Ibid, [10].

that the three are essentially and necessarily distinct processes. But they might well be part of a single measure of surveillance which involves interception and collection of personal data. Of course, surveillance of digital communication on its own either without interception of the whole or part of the relevant communication or collection of personal data (which might often be part of the interception) is of little use to intelligence or law enforcement agencies. A 2013 report of La Rue, former UN Special Rapporteur on the Freedom of Expression, offers an instructive description of ‘communication surveillance’:

The monitoring, interception, collection, preservation and retention of information that has been communicated, relayed or generated over communications networks.⁶⁷⁴

This description appropriately captures what is probably intended in the Privacy Resolutions. But one finds the lack of clarity in the Resolutions striking because the same report has been referred to in the opening paragraphs of the first and second Resolutions, with approval.⁶⁷⁵ The third and fourth Resolutions refer, instead, to reports of La Rue’s successor, which do not carry the same definition of communication surveillance.⁶⁷⁶

In conclusion, the ongoing UN privacy discourse carries a level of political capital that could be tapped in reforming the international law of privacy. While the Privacy Resolutions are replete with inconsistencies, uncertainties and ambiguities, the political capital would assist in realizing a more focused and practicable reform initiative.

2 Innovative Approaches to Privacy

As considered in section II above, the ongoing UN privacy discourse carries not only novelty of substance but also of approach. The second catalytic role of the UN privacy discourse draws from the latter. One is the unifying approach of the Resolutions in pulling together the various normative sources of privacy. Such an approach would be instrumental in distilling and cross-fertilizing diffuse privacy norms that reflect modern understandings on the legal protection of the right to privacy in the digital age. The idea of a soft law supplement argued in chapter 5 builds on, but goes beyond, this unifying and holistic approach to privacy.

A multi-stakeholder approach to privacy is the other innovative notion espoused in the Resolutions. In addition to the acknowledgment of ‘informal dialogues’ among relevant stakeholders for having greatly facilitated the discussion on the right to privacy, the Resolutions set a process in motion to further discuss the issue of digital

⁶⁷⁴ See Report of La Rue, above n 448, [6(a)].

⁶⁷⁵ See, e.g., Res 68/167, above n 545, preamble, [7].

⁶⁷⁶ See, e.g., Res 73/179, above n 545, preamble, [4].

privacy through a multi-stakeholder process.⁶⁷⁷ They provide that challenges to the right to privacy in the digital environment must be considered in a multi-stakeholder process.⁶⁷⁸ As considered in the context of IBRs in chapter 3, multi-stakeholderism offers – its inherent limitations notwithstanding – new ways of norm-creation. References to and supports for multi-stakeholderism in the Privacy Resolutions lack clarity, however. This is particularly the case in relation to the nature and scope of the dialogue.

Yet the support for a dialogical approach to privacy is, on its own right, a pragmatic way forward. Considering virtues of a multi-level dialogue as a way of building consensus and then gradually improving human rights protection, the support for a multi-stakeholder approach is a step forward. As shall be argued in chapter 6, a dialogical approach to digital privacy is the most practical step towards lessening institutional gaps in present international law. Introducing a privacy forum where emerging and current privacy issues are debated would be pragmatic and logical ways of realizing the support for dialogue expressed in the Privacy Resolutions.

In summary, the Privacy Resolutions' important value lies in their role of beginning a process that may culminate in long-term international legislative measures on digital privacy. The conversation commenced by the discourse and its innovative approaches to privacy yield a catalytic role in reimagining the right to privacy in the digital age. Together with progressive aspects of the IBRs Project explored in the preceding chapter, the UN privacy discourse offers the normative and methodological direction in that front.

IV CONCLUSION

This chapter examined normative significances of the evolving UN privacy discourse, with a particular focus on the series of Resolutions adopted between 2013 and 2018, in reimagining the international law of privacy in the digital age. It demonstrated that the elaborative and contributory roles of Resolutions are valuable on their own but less so in the context of international privacy law given the limited normative reach of the Privacy Resolutions. Partly dictated by the very nature of Resolutions in that they are not formally suited to capture as much regulatory details, the Privacy Resolutions address privacy themes in a selective manner. Worse, institutional aspects of international privacy law are not considered. Inchoate state of the discussions further reduces the freestanding role of the privacy discourse. As this chapter has shown, inevitable uncertainties (and controversy) surrounding the possibility of a customary international law of privacy or even general principles of law also makes them ill-suited to reimagine the right to privacy in international law.

⁶⁷⁷ Ibid, [9] cum preamble, [13].

⁶⁷⁸ Ibid, preamble, [11-12].

The chapter argued that a more promising value of the discourse is its potential of catalysing a pragmatic privacy law reform. Resolutions have long served as incipient steps towards a hard law especially in the area of human rights, including in the form of a treaty. But that is not necessarily be a pragmatic way forward for international privacy law. A future international legal response to the privacy problem in digital space must not necessarily follow, for example the path of the UN Resolutions on the Outer Space, at least in the short and long-term. As shown at the outset, treaty law is neither desirable nor viable in effectively responding to contemporary privacy challenges in the digital environment. What is needed is a focused and practical approach that builds on but moves beyond the Privacy Resolutions. Such an approach would build on the political will exhibited in the discourse and some substantive aspects of the Privacy Resolutions. Chapters 5 and 6 explore the nature, scope and content of that pragmatic approach to the international law of privacy.

**PART III: REIMAGINING INTERNATIONAL LAW OF
PRIVACY PRAGMATICALLY**

CHAPTER 5 — JUST A SUPPLEMENT: TOWARDS AN (INTERNATIONAL) SOFT LAW ON THE RIGHT TO PRIVACY

I INTRODUCTION

This chapter explores the first strand of the pragmatic approach towards reimagining current international law of privacy in the digital age: a soft law supplement. The second strand, which seeks to address institutional-structural gaps, is explored in the next chapter. This chapter considers the virtues of a soft law on the right to privacy in making international privacy law better equipped in the digital age, particularly in lessening its normative gaps. It argues that a soft law is virtuous in three respects: first, it would translate the rather vague provisions of the right to privacy in international law; second, it would globalize emergent privacy norms; and third, it would enable the progressive development of (privacy) law.

Over the years, soft law has been proposed as a pertinent instrument of translating human rights, including the right to privacy, based on new realities of the digital age. A former UN Special Rapporteur on Human Rights and Counter-terrorism, Scheinin, for instance, had recommended the HR Council to initiate a process for the creation of a ‘global declaration on data protection and data privacy’ as a ‘soft law complement to the hard law in the area’.⁶⁷⁹ Perhaps because his proposal was part of a broader theme, the recommendation did not go far enough to outline what exactly that proposed Declaration would incorporate, and why a ‘Declaration’ is the appropriate instrument. In addition, whether the Council has a mandate to issue a Declaration, which is often adopted by the UNGA, is not entirely clear. The periodic membership of the Council, added to its vulnerability to politicization, probably makes it a less optimum body to adopt the proposed Declaration.

Proposals for soft law of other forms, particularly a GC of the HR Committee, have also been made before and after the Snowden debacle. Most notably, the American Civil Liberties Union (ACLU) not only advocated for a GC but also tabled a draft.⁶⁸⁰ But as shall be argued in this chapter, a GC may not be a pertinent instrument to address the ‘normative gap’ in the international law of privacy. Another soft law proposal has been for a broader Internet governance declaration, akin to the UDHR, negotiated through a multi-stakeholder process.⁶⁸¹ But this proposal not only is too

⁶⁷⁹ Report of Scheinin, above n 198, [73]. See also Martin Scheinin, ‘Privacy and Security can be Reconciled’, *The Guardian* (online), (21 January 2010) <<https://bit.ly/2OmKY4C>>

⁶⁸⁰ ACLU, above n 178.

⁶⁸¹ Wolfgang Kleinwächter, ‘Internet Governance Outlook 2014: Good News, Bad News, No News?’ on *Circle ID* (31 December 2013) <<https://bit.ly/1k8uufl>>; see also Andrea Pettrachin, ‘Towards a Universal Declaration of Internet Rights and Freedoms’ (2018) 80 *International Communication Gazette* 337, 349-350.

broad to pay as much focus to digital privacy but also does not offer any details of its possible content.

This chapter goes beyond proposing a soft law supplement and explores the justifications, content and legal form of an international soft law on the right to privacy. In that sense, it seeks to provide a clear conceptual basis and justification for earlier proposals, particularly the one made by Scheinin a decade ago, based on developments that have occurred since. The proposed soft law would also fulfil (cumulatively) functions of Reed's imaginary 'successful law', alluded to above in the epigraph, in entrenching existing norms – while at the same time clarifying embedded uncertainties and ambiguities – and reinforcing emerging norms.

The thesis follows Boyle and Chinkin's explication of the notion 'soft law'. They describe soft law as a catchphrase for 'a variety of non-legally binding instruments used in contemporary international relations'.⁶⁸² And as such, what essentially distinguishes it from 'hard law' like treaties is its lack of binding force. Yet, despite the lack of binding force, soft law may enjoy in practice 'legal effect' to a varying degree. As Boyle and Chinkin further note, the use of soft law is not restricted among States, but also among States and non-State actors as well as among non-State actors alone.⁶⁸³ The discussion in this chapter is, therefore, within this analytical parameter.

Soft law takes different forms in international lawmaking. From Declarations and Resolutions to GCs and policy briefs of civil society groups, they all fall under the rubric of 'soft law'. Having examined pertinence of these forms of soft legalization in filling the normative gaps in current international law of privacy, the chapter concludes that a UNGA is the most appropriate instrument for two reasons.⁶⁸⁴ First, compared to other types of soft laws such as the UN Privacy Resolutions explored in chapter 4, a UNGA Declaration sits at a higher normative hierarchy and hence is normatively more authoritative, while at same time enjoying all the merits of 'softness'. Second, unlike other soft laws like Resolutions and GCs, a UNGA Declaration is structurally-suited to provide relatively detailed substantive and institutional norms.

For ease of reference, core aspects of the proposed soft law are provided in appendix 3.

⁶⁸² Boyle and Chinkin, above n 509, 212-213.

⁶⁸³ Ibid, 213.

⁶⁸⁴ See more in section D below.

II VIRTUES OF A SOFT LAW SUPPLEMENT IN THE INTERNATIONAL PROTECTION OF DIGITAL PRIVACY

What makes a soft law an apposite instrument in attending to normative limitations of the current framework flows from two underlying factors. The first relates to the place and nature of soft law in the mosaic of international lawmaking. Unlike a hard law, soft law is far more feasible and flexible in developing international legal norms. That is a widely recognized virtue of soft legalization in heeding to expediency in international lawmaking. The other, equally important, factor relates to the present state of the international law of privacy. As examined in chapters 1 and 2, the right to privacy already finds a high-level recognition and articulation in international (hard) law. Albeit to a lesser degree and mainly provided in dispersed soft law instruments, the UN data privacy framework also embodies key data privacy norms and principles. Thus, foundational norms of international privacy law are codified in hard law, making a new hard law instrument less desirable, at least at this stage. What is acutely needed, instead, is simply a ‘supplement’ to those norms, in a soft law form, to revitalize current international law of privacy in the digital age.

A soft law supplement would play a key role in unpacking the rather vague high-level abstract privacy principles based on new developments, including international privacy initiatives considered in chapters 4 and 5. In translating these principles in the light of new developments in the digital age, a soft law – while avoiding the long-road to hard legalization – retains the relevance of existing international privacy law. The privacy field is also uniquely a highly fragmented area of international regulation, further aggravated by a myriad of reform initiatives pursued at various levels. A soft law would be vital in being a site for norm cross-fertilization by which it unifies and universalizes these initiatives. This section discusses these virtues of a soft law supplement on the right to privacy in more detail.

A Reimagining the Right to Privacy in the Digital Age

A prime significance of the soft law would be to reimagine the scope and meaning of the right to privacy in the digital age. The argument in this chapter is that a soft law is an appropriate instrument to revitalize norms that already found a general level of recognition in a hard law in the light of the new realities of the digital age. This is especially so with respect to the right to privacy in international human rights law. As explored in chapter 1, the right to privacy is guaranteed in several human rights instruments, including the ICCPR, but in an exceedingly vague manner. High-level abstract principles articulated in these instruments can be elaborated through a soft law.

Soft law historically played a key role in backing-up hard law by ‘concretizing’ some of its abstract notions, including in the context of human rights instruments.⁶⁸⁵ As Saul notes in the context of the UN Declaration on Rights of Indigenous Peoples (DRIP), the Declaration particularises general human rights for indigenous peoples.⁶⁸⁶ It ‘variously consolidates existing norms, clarifies certain rules and progressively develops others’.⁶⁸⁷ The proposed soft law, then, would clarify and consolidate the existing international law of privacy while at the same time progressively embracing emergent norms anchored in IBRs and the series of UN Privacy Resolutions. In that sense, it might be argued that the proposed soft law on the right to privacy would function as a ‘legislative interpretive instrument’ in offering an authoritative interpretation of the privacy provisions of the UDHR and the ICCPR. Similar arguments, indeed, have been made in relation to other soft laws. The DRIP, for instance, is considered as an authoritative elaboration of the relevant provisions of several UN human rights instruments and sector-specific instruments with respect to the rights of indigenous peoples.⁶⁸⁸

The elaborative potential of a soft law is useful in at least three respects. One is that it would offer normative guidance in the implementation process. Judicial and quasi-judicial bodies could draw upon the instrument in entertaining cases or conducting periodic reviews of States. In practice, this has been the case in many areas of human rights. The jurisprudence of UN treaties bodies has, for instance, been directly informed by the relevant provisions of the DRIP.⁶⁸⁹ In a similar way, a soft law on privacy may assist in offering normative guidance on the content of the right to privacy, for instance, to the HR Committee. In view of the ICCPR’s crude privacy provisions, a soft law that specifies the scope and meaning of the right would offer some guidance to the Committee in its practice. Beyond the adjudicative fora, soft law would also be useful in providing a roadmap for deliberations in less formal platforms, where the right to privacy is considered. Chapter 6 explores how the soft law would provide a blueprint by which emerging and current challenges relating to privacy can be considered in the proposed multi-stakeholder privacy forum.

A second advantage is that it would constitute an important normative progression in keeping with new developments. Instead of pursuing the rather cumbersome procedure of introducing treaty amendments, the adoption of a soft law would allow embracing new normative initiatives. Good cases in point, in this regard, are IBRs and the evolving UN privacy discourse, examined in chapters 3 and 4

⁶⁸⁵ See Handl et al, above n 346, 380.

⁶⁸⁶ Ben Saul, *Indigenous Peoples and Human Rights: International and Regional Jurisprudence* (Hart Publishing, 2016) 8.

⁶⁸⁷ Ibid.

⁶⁸⁸ See Mauro Barelli, *Seeking Justice in International Law: The Significance and Implications of the UN Declaration on the Rights of Indigenous Peoples* (Routledge, 2016) 52-54.

⁶⁸⁹ See Benedict Kingsbury, ‘Indigenous Peoples’ in *Max Planck Encyclopedia of Public International Law* (2015) [5].

respectively, that – to a degree – introduce privacy norms mostly new to international law of privacy. An effective way to embrace such emergent norms within the rubric of international law is through a soft law that cross-fertilizes and then reinforce them. Not only is this effective but also innovative in the sense that these international privacy initiatives, as they currently stand, are unlikely to result in any reform of international privacy law on their own right. But this merit of facilitating normative progression would not be restricted to these initiatives. The soft law would additionally open the doors for future similar initiatives meant to respond to emergent privacy challenges to be incorporated.

Related to this is that the soft law would also be a key instrument in reviving the (largely) invisible UN data privacy framework. Despite being an important regulatory tool for the protection of privacy, the UN data privacy framework has received little attention. Apart from recent progressive internal documents of UN agencies, as examined in chapter 2, the UN data privacy framework not only is deeply fragmented but also normatively outmoded. The soft law would be a pertinent UN instrument to update and revive the UN data privacy framework based on significant developments in field in the past decade or so. In that sense, in expanding existing high-level abstract privacy norms, the soft law would contribute towards lessening the normative gaps of international law of privacy identified in chapters 1 and 2.⁶⁹⁰

A common weakness associated with soft law is its lack of binding force.⁶⁹¹ In the context of the discussion here, a question might arise: what is the point of having a soft law that does not carry enforceable obligations? This takes us to the third advantage to an elaborative soft law. A soft law that interacts with and reformulates a widely accepted hard law like the ICCPR may draw from the normative force of the latter. To the extent that the soft law is an elaboration of the ICCPR's otherwise dense privacy provision, States may arguably be bound by it. If the soft law were to be, as they should, adopted by the UNGA, it would lend weight to the authority of the instrument. An argument on the authoritative value of soft law may be useful in countering resistance to the soft law due to its inherently non-binding nature. A soft law's authority hinges, of course, on a number of factors, including the extent to

⁶⁹⁰ See section III below on the possible normative content of the proposed soft law.

⁶⁹¹ But soft law has also its detractors at a conceptual level. See, for instance, Jan Klabbers, 'The Undesirability of Soft Law' (1998) 67 *Nordic Journal of International Law* 381, 381-391 (suggesting that an argument for soft law is (a) detrimental because it tends to rob the formal authority of law and circumvents formal processes to the benefit of the powerful elite and (b) undesirable because it vouches for what is often either a non-law or hard law); see also Jean d'Aspermont, 'Softness in International Law: A Self-Serving Quest for New Legal Materials' (2008) 19 *European Journal of International Law* 1075, 1075-1093 (claiming that international lawyer's resort to soft law as a new area of study is partly a result of professional insecurity caused by perceived saturation of the field). As this chapter will show, these criticisms of soft legalization do not necessarily apply to the proposed soft law on the right to privacy, and indeed virtues of soft law explored here are recognized, at times, by its critics.

which its adoption drew consensus and support from States. The level of support and consensus will also later have a bearing on its implementation in practice, but as Shelton argues, a soft instrument that builds on already well-entrenched hard law instruments is likely to draw better reception and hence compliance.⁶⁹² This is partly because the adoption of a soft law instrument that furthers, or somehow relates to, a widely accepted instrument is an indication of ‘greater commitment’ on the part of States for the implementation of the law.⁶⁹³

Translation of hard law through soft law is also consistent with precedents in international lawmaking. One finds several instances where specific rights provided in a given human rights treaty are elaborated in soft law instruments. One is the ‘right to freedom of religion’. Although freedom of religion, conscience and thought has been introduced as a separate right under the UDHR and the ICCPR, a Declaration on the Elimination of All Forms of Intolerance and of Discrimination Based on Religion or Belief was adopted several years later.⁶⁹⁴ While the Declaration appears to have a specific scope – i.e. religious intolerance and discrimination – the example reveals a unique instance of normative progression from hard to soft law. Art 1 of the Declaration, for instance, replicates the three sub-articles of Art 18 of the ICCPR, and the fourth one is dealt with under Art 5. The scope and content of the right are further specified under Art 6 of the Declaration.

Similar examples of normative progression are available in other areas of human rights. The UN Declaration on the Rights of Minorities is one such example, which is meant to elaborate Art 27 of the ICCPR, which provides protection to the rights of persons belonging to minority groups.⁶⁹⁵ The Declaration was meant to ‘throw light on the various implications of Art 27 and to specify measures needed for the observance of the rights recognized in the Article’.⁶⁹⁶ Not only is it inspired by Art 27 but also builds on, and adds to, the rights contained in the international bill of rights.⁶⁹⁷ Another precedent shows that the progression from Declaration to treaty could, at times, again go the other way. This has been the case for the Women Rights Convention, which began with a Declaration on the Elimination of Discrimination against Women, then a Convention. The relevant provisions of the Convention later are specified by a Declaration on Violence against Women. The Preamble of the

⁶⁹² Shelton, above n 605, 14.

⁶⁹³ Ibid.

⁶⁹⁴ See *Declaration on the Elimination of All Forms of Intolerance and of Discrimination Based on Religion or Belief*, GA Res 36/55, 93rd plenary mtg, UN Doc A/RES/42/97 (25 November 1981).

⁶⁹⁵ See *Declaration on the Rights of Persons Belonging to National or Ethnic, Religious and Linguistic Minorities*, GA Res 47/135, 92nd plenary mtg, UN Doc A/RES/47/135 (18 December 1992).

⁶⁹⁶ See Patrick Thornberry, *International Law and the Rights of Minorities* (Clarendon Press, 1991) 152; see also *Report of Special Rapporteur of the UN Sub-Commission on Prevention of Discrimination and Protection of Minorities, Francesco Capotorti*, UN Doc E/CN.4/Sub.2/384/Add.5 (28 June 1977).

⁶⁹⁷ See *Commentary of the Working Group on Minorities to the United Nations Declaration on the Rights of Persons Belonging to National or Ethnic, Religious and Linguistic Minorities*, UN Doc E/CN.4/Sub.2/AC.5/2005/2 (4 April 2005) [3-4].

Declaration provides that it is meant to ‘strengthen and complement’ the Convention – and to provide clear prohibition of violence against women.⁶⁹⁸ In the area of child rights, there are a number of instances where treaty law has been expanded through soft law. Examples include the UN Riyadh Guidelines and the Alternative Child Care Guidelines which elaborate and expand aspects of the CRC.⁶⁹⁹ Thus, children’s rights law is the other area of international human rights law that exhibits normative progression, and elaboration, from a treaty law to a variety of soft laws.

To summarize, the primary merit of a soft law supplement is redefining the scope and meaning of the right to privacy based on developments that have emerged since its codification in international law, particularly the new realities of the digital age. A soft law would assist in revitalizing the classic privacy principles of international law in the digital age. Beyond the law better equipped in the digital age, the soft law would also be suitable instrument to remedy its normative gaps. Moreover, it would offer much needed normative guidance to the HR Committee (and other non-judicial forums) where digital privacy themes are routinely debated. Not only would a soft law avoid the uncertain and time-taking process of treaty lawmaking, but also provides normatively strong roadmap to advance the privacy agenda in the digital age.

B Globalizing Emergent Privacy Standards

As the analysis in earlier chapters have shown, sources of global privacy standards are diverse. From human rights law and data privacy law to IBRs and the UN Privacy Resolutions, privacy standards find no single underlying international instrument. This, added to the already excessive normative dispersion that characterizes the UN data privacy framework, is problematic. Progressive tendencies of international privacy initiatives like IBRs will remain buried unless they are integrated with the present international law of privacy. As already highlighted above – and explored further in chapters 4 and 5, no viable reform of international privacy law is likely through and solely by IBRs and the ongoing UN privacy discourse.

In the absence of an institutional process that draws upon the merits of these initiatives, they would just remain invisible, or stall without resulting in any tangible outcome. The proposed soft law would be key in unifying, and giving some effect to, these extant and emerging global privacy standards. It would distil globally accepted privacy standards and best practices advanced under different banners. From the present framework on the human right to privacy and data privacy to

⁶⁹⁸ *Declaration on the Elimination of Violence against Women*, GA Res 48/104, 85th plenary mtg, UN Doc A/RES/48/104 (20 December 1993) preamble.

⁶⁹⁹ *Guidelines for the Prevention of Juvenile Delinquency (Riyadh Guidelines)*, GA Res 45/112, 68th plenary mtg, UN Doc A/RES/45/112 (14 December 1990); *Guidelines for the Alternative Care of Children*, GA Res 64/142, 6th sess, UN Doc A/Res/64/142 (24 February 2010).

IBRs, the soft law would synthesis the emerging consensus on the right to privacy. An international soft law on the right to privacy would then effectively globalize emergent privacy standards and map them onto the present international law of privacy.⁷⁰⁰

As discussed in chapter 4, one novelty of the UN privacy discourse is its ‘unifying’ approach to the right to privacy. Although proceeding under a ‘human right to privacy framework’, Privacy Resolutions adopted as part of the discourse embrace diverse sources of privacy standards: human rights law, data privacy law and IBRs. To a certain extent, the IBRs Project also pursues a unifying approach when it addresses privacy rights in tandem with the rather regulatory field of data privacy, while it essentially is a human rights project. This is not, of course, entirely out of place given that data privacy increasingly is moving towards a human rights language with recognition of enforceable ‘data subject rights’. But what makes this holistic approach particularly novel and beneficial is that it attends to the problem of normative dispersion and projects privacy standards globally. Normative unification increases the accessibility and visibility of global privacy standards. More accessibility and visibility would further the goal of facilitating the protection of the right to privacy on the ground.

With more visibility and accessibility also comes the possibility that global privacy standards shape the development of national privacy jurisprudence. Often, soft law offers ‘reference points’ by which domestic law and judicial decision making are guided. As Dupuy notes, soft law norms normally bear impact on national legislatures as ‘reference models’ and are often taken into account by municipal judges.⁷⁰¹ In this sense, the soft law on the right to privacy can inspire local action, be it in triggering domestic legislation or guiding judicial adjudication, or even informal dialogue on the subject in question. It may also serve as a ‘model law’ for the enactment of an equivalent domestic legislation. Even in the absence of a formal legislative incorporation of the soft law or aspects of it, domestic and regional courts could draw from it in entertaining matters relating to the right to privacy. As highlighted in earlier chapters, soft law instruments such as the UN Privacy Resolutions are, actual impact regardless, already being considered by local and regional courts such as the ECtHR.

The globalizing mission of a soft law is in accord with the underlying assumption of international human rights law: complementarity. The notion of complementarity holds that a properly functional national human rights system is key to the realization of international human rights. The globalizing potential is significant

⁷⁰⁰ Soft law sceptics also recognize the ‘globalizing’ role of a soft law. See, e.g., d’Aspermont, above n 691, 1082 (acknowledging the potential of soft law in ‘internationalizing’ a subject matter as well as in providing normative guidance and facilitating formation of custom).

⁷⁰¹ Pierre-Marie Dupuy, ‘Soft Law and the International Law of Environment’ (1990/91) 12 *Michigan Journal of International Law* 420, 434-435.

because the recent prominence of new privacy standards is, to a greater degree, restricted to some parts of the world. The IBRs, for instance, has been adopted only in a handful of countries – and the majority is a product of civil society advocacy. The proposed soft law – by embracing aspects of the IBRs Project, among other components – would be the first global articulation of emerging privacy standards now widely championed by various stakeholders. It would transform these standards into global standards which, in turn, may enhance the global protection of privacy over time.

‘Globalizing’ emergent privacy standards may also indirectly alter behaviour of technology companies. As discussed in chapter 3, there is a growing corporate appeal to IBRs by a growing number of small companies that offer competitive privacy-protecting services and pledge IBRs. By embracing Internet rights in an international instrument, the soft law would globalize and perhaps nudge bigger corporations towards such industry practices. Coupled with local regulatory interventions such as through competition law tools of breaking up bigger companies or forcing them to share data with smaller firms, the soft law would gradually mainstream current marginal industry practices.

In summary, the soft law would offer a potential of globalizing emergent privacy standards and promoting the applicability of privacy standards at the global level. That the proposed soft law is to be adopted by the UN, a representative body of the international community, furthers the globalizing aim.

C Facilitating Progressive Development of (Privacy) Law

The inherent flexibility of soft legalization is another factor for its plausibility. The flexibility can be explained in at least three ways. One is that a soft law, compared to hard law, entails a lower ‘contracting cost’ – and hence is comparatively feasible.⁷⁰² A soft law can be negotiated and adopted – as often is the case, more easily than hard law. It short-circuits what is called ‘treaty fatigue’ and domestic constitutional hurdles that often stand in the way of new binding international rules of cooperation.⁷⁰³ Thus, unlike hard law, a soft law would not require signature and ratification by States – and could enter the statute book more quickly.

Some soft laws, of course, had taken many years before they were finally adopted. One recalls, in this regard, the DRIP and Declaration on Freedom of Religion.⁷⁰⁴ Work on the Religious Freedom Declaration, for instance, began in 1962 – while the ICCPR was being drafted and debated – but, the work on the Convention was

⁷⁰² See Abbott and Snidal, above n 661, 422-423, 435.

⁷⁰³ See Joost Pauwelyn et al, ‘When Structures Become Shackles: Stagnation and Dynamics in International Law Making’ (2014) 25 *European Journal of International Law* 733, 738-743.

⁷⁰⁴ See *The United Nations Declaration on the Rights of Indigenous Peoples*, GA Res 61/295, 61stss Agenda item 68, UN Doc A/61/295 (2 October 2007); GA Res 36/55, above n 694.

abandoned and it was finally adopted in 1981.⁷⁰⁵ Similar delay had occurred in the process of negotiating and adopting the DRIP. This raises the question of whether a soft law on the right to privacy would wait the same fate of delay. Despite some inevitable resistance, or even opposition, from some States and non-State actors mainly technology companies, there are reasons to believe that the proposed soft law would be adopted relatively quickly.

To start with, the discussion set in motion at various levels by the Snowden revelations offers some hope. As considered in chapter 4, the revelations have already started a discourse at the UN on the right to privacy in the digital age. This discourse has so far been translated into successive Resolutions that exhibited notable consensus in addressing privacy issues at the international level. More importantly, these Resolutions appear to evolve from sheer reaffirmation of the right to privacy to embracing modern privacy standards. The various sources of global privacy protection, including data privacy and IBRs have found some form of expression in the Resolutions. These signs of distilling and synthesizing global privacy standards would prove useful in facilitating consensus. The broader acceptance of the DRIP, despite many years of negotiation, was made possible because the drafters were careful in benchmarking the Declaration on State practices and established jurisprudence in the area.⁷⁰⁶ A soft law on privacy that builds on well-established best practices and emerging State practices stands a good chance of being adopted sooner. It will also be a natural and logical evolution of the UN Privacy Resolutions.

A no less significant ‘political capital’ that can usher in more robust global privacy standards has been created by the adoption of these Resolutions. As shown in chapter 4, there was relatively wider support to these Resolutions from States on all sides of the global political axis. Except for the lobbying by Five Eyes States, particularly the US to water-down the Resolutions, there was support from the overwhelming majority of States. That the discussion still continues at the UN also suggest that the momentum is far from being an ephemeral political phenomenon. Civil society advocacy which found significant place in these discussions, particularly in terms of paving ways of developing the UN privacy regime based on regional and local developments, is likely to assist in sustaining the discourse. Thus, these set of circumstances surrounding the privacy discourse at the UN makes a soft law more feasible than not. In light of the ongoing effort to introduce a binding treaty on business and human rights at the UN, it is plausible that Internet businesses would settle for the rather modest proposal of a soft law. After all, when one considers that Cold War politics was the principal factor in delaying the

⁷⁰⁵ See Bahiyyih Tahzib, *Freedom of Religion Or Belief: Ensuring Effective International Legal Protection* (Martinus Nijhoff Publishers, 1996) 122-165.

⁷⁰⁶ See Saul, above n 686, 7.

adoption of a soft law on freedom of religion, as reported by Cassese⁷⁰⁷ – which now appears to be largely absent, a soft law on privacy would be feasible.

The second way to consider the flexibility of a soft law is its potential to gradually develop into hard law. While a hard law instrument on the right to privacy in the digital age might not be desirable and feasible at this stage, a soft law would still serve as a way station towards hard law, be it treaty or customary law. This would be useful in the sense that the hardening of the soft law over time enhances its normativity particularly in creating legally binding obligations. Hard law is more likely to evolve from a soft law which promotes a trend of ‘hardening’ international relations.⁷⁰⁸ Soft law is generally considered as a ‘precursor’ to hard law, a ‘probationary’ candidate for eventual recognition as a fully-fledged law.⁷⁰⁹ It is possible, and perhaps desirable, that domain-specific regulatory treaty(ies) on themes relating to privacy might be negotiated and adopted. An example, in this regard, is the ongoing effort of the SRP to start a negotiation on a treaty on government surveillance.⁷¹⁰ The proposed soft law could be a springboard towards such long-term multilateral treaty processes. It is also in accord with the tradition in international law making, for a treaty to evolve from a soft law, rather than a work from scratch. One recalls here that several UN human rights treaties were preceded by Declarations, including on disability rights, child rights and women’s rights.⁷¹¹

Another pathway for the hardening of soft law is development of customary law. Soft law carries the potential to facilitate the rapid codification of emerging State practices into customary law.⁷¹² While a long-term and uncertain process, this could also be used to counter possible resistance from States to heed the proposed the soft law owing to the lack of legally binding force. A related point is that a soft law is also a convenient mechanism of holding to account States that have not ratified the ICCPR at all. Non-ratification means that States like China would not be reviewed under the periodic reporting mechanism of the treaty bodies, not to mention the complaints procedure. That the UPR, another venue of periodic review of human rights performance, applies regardless of ratification of human rights treaties – and hence addresses the gap in treaty body periodic review is also questionable. This is because, as discussed in chapter 1, the UPR is conducted by high-level government

⁷⁰⁷ Cassese, above n 125, 303-304.

⁷⁰⁸ See Tadeusz Gruchalla-Wesierski, ‘A Framework for Understanding “Soft Law”’ (1984) 30 *McGill Law Journal* 37, 37.

⁷⁰⁹ See Gross, above n 362, 176; see also Hilary Charlesworth, ‘Law Making and Sources’ in James Crawford and Martti Koskeniemi (eds), *The Cambridge Companion to International Law* (Cambridge University Press, 2012) 198.

⁷¹⁰ See ‘Special Rapporteur on the Right to Privacy presents Draft Legal Instrument on Government-led Surveillance and Privacy’ (February 2018), available at <<https://bit.ly/2ZcNe4Y>>

⁷¹¹ See a comprehensive list of UN human rights instruments at <<http://bit.ly/LAdFKU>>

⁷¹² See Joyner, above n 623, 459.

officials, as opposed to experts, and hence is unlikely to be a commensurate replacement to periodic review by the HR Committee.

To summarize, the proposed soft law is flexible at many levels. On top of its inherent feasibility to be adopted relatively quickly, it is also a more pertinent instrument to develop into hard law in areas of privacy where such hardening is desirable. It could be taken as part of the natural evolution of the ongoing privacy discussions.

III WHAT SUPPLEMENT? SKETCHING NORMATIVE STRUCTURES OF THE SOFT LAW

A follow-up question then would be what substantive content should the proposed soft law have? What makes this a key normative question is the apparent multiplicity of sources of privacy standards. The proposed soft law is an international human rights instrument, but how should it treat emergent privacy standards drawn from the rather regulatory field of data privacy law? To what degree should it embrace progressive elements of IBRs? More importantly, to what extent can a soft law embody such diversity of norms? Questions of both scale and normative reach arise in considering the normative structures of the soft law.

As considered in earlier chapters, there is a considerable convergence among jurisdictions and several stakeholders on the minimum standards that a right to privacy must embody in the digital age. The IBRs Project increasingly converges towards a set of digital privacy rights and principles. So are data privacy instruments, which largely are moving towards European data privacy standards. And, these two tiers of privacy protection are, to a degree, finding holistic expression in the ongoing UN discourse on the 'right to privacy in the digital age'. The proposed soft law would, then, be the next logical legislative step in concretizing this unifying approach.

Based primarily on post-Snowden reform initiatives, what follows provides a modest sketch of what the content of the right to (digital) privacy in international law should look like. The substance of the soft law explored below seeks mainly to respond to core normative gaps of present international law of privacy explored in chapters 1 and 2. More particularly, the aim is to clarify and translate the meaning and scope of the right to privacy ambiguously formulated in current international (human rights) law. This involves specifying the respective obligations of States and non-State actors in the respect for and protection of the right to privacy. A unifying approach also means that the soft law must attend to, to an extent, weaknesses of the UN data privacy framework, particularly its archetypal normative fragmentation. Moreover, in reimagining the right to privacy in the digital age, the proposed soft law supplement would assist in specifying the scope of the right while at the same time holistically synthesising modern privacy standards.

In what follows, normative contours of the soft law are described in three steps. First, it discusses how the scope of the right to privacy must be framed in the digital context. Second, it highlights core privacy principles that must be incorporated in the law. Third, it outlines the respective obligations/roles of States, corporations and other non-State actors under the right to privacy. Further details are provided in appendix 3.

A Clarifying Scope of the Right to Privacy in the Digital Age

Clarifying boundaries of the right to privacy in the digital context should be the prime focus of the soft law. In view of the vague manner in which the right to privacy is stipulated in international law – as explored in chapter 1, the soft law is best-positioned to clarify, elaborate and entrench the right based on developments that have occurred in the past few decades. More particularly, the IBRs and the UN privacy discourse, among other sources, offer fertile ground to redefine the scope of the right to privacy in at least the following three respects. One is untangling interests protected under the underlying right to privacy; second, reframing the right to privacy into a set of sub-rights consistently with emerging conceptions of the right; and thirdly, introducing explicit limitation clause for the right to privacy.

1 Decoupling Protected Interests

Among protected interests under Article 17 of the ICCPR as well as Article 12 of the UDHR are ‘reputation and honour’. As examined in chapter 1, current international human rights law bundles the right to privacy with these related but distinct interests of reputation/honour leading to confusion. Ideally, then, the soft law should disentangle the right to privacy from the distinct rights to reputation and honour. While reputation and honour are valid interests worthy of protection, they should not be conflated with the rather broad and unique right to privacy. This is not to mention the question of whether ‘honour’ – an entirely subjective view of a person about oneself, and hence not generally protected even under defamation law,⁷¹³ as opposed to ‘reputation’ – is worthy of protection as a distinct human right. In line with the recent approach of the UN Privacy Resolutions, the content of proposed soft law should be restricted to privacy interests. The other way forward is to envisage the circumstances where interference with reputational interests of an individual merit protection under the right to privacy. While the ECtHR, as highlighted in chapter 1, has clearly ruled that privacy and reputation are distinctive interests, certain attacks on reputation may engage the right to privacy. The most common of such instances is when attacks to one’s reputation results in harm to private life. This is the other way in which the proposed soft law can reconcile these bundled interests.

⁷¹³ See, e.g., Mark Armstrong et al, *Media Law in Australia* (Oxford University Press, 3rd ed., 1995) 9-13; see also Nowak, above n 179, 552.

Moreover, the soft law must reframe the right to privacy in a manner that clarifies the nexus between the ‘zones’ of privacy protection and the underlying right itself. The common zones of privacy protection – i.e. ‘family’, ‘home’ and ‘correspondence’ – as shown in chapter 1, are framed in international law in a manner that suggests they are not covered under the umbrella term ‘privacy’. This has created confusion and hence led to erroneous interpretations, including by the HR Committee, that those zones of protection are distinct from ‘privacy’. This should be rectified in a manner that clarifies the fact that the right to privacy provides protection from unlawful interference with ‘privacy of the family, home and correspondence’ as opposed to ‘privacy’, and ‘family, home and correspondence’. This will also be in line with the increasing tendency in the literature to adopt this understanding.⁷¹⁴ Additionally, it should set out how these zones of protection apply in the digital context, for instance that ‘home’ in cyberspace includes one’s digital devices and accounts. See further on this point in appendix 3.

2 Subset of Privacy Rights

With the launching of several IBRs initiatives, the classic right to privacy has found, as explored in chapter 3, specific formulation into a number of subset of rights. Of these rights, the right to *use* encryption technologies and freedom from of surveillance are the commonest. A number of other rights that grew out of judicial interpretation of the broader right to personality, but that are essentially protective of privacy interests, have also emerged. An example in this regard is the right to the confidentiality and integrity of information systems. Both data privacy legislation and IBRs are increasingly embracing rights that fall under what might be referred to as ‘right to personal data protection’ such as the right to be forgotten. The proposed soft law instrument would be a pertinent global instrument to further develop the classic right to privacy in the digital age based on these emerging normative developments.

There are at least four benefits in incorporating these subsets of privacy rights. First, it clarifies the scope and meaning of the right to privacy based on the increasingly ‘overlapping consensus’ at various levels, including internationally in the ongoing UN privacy discourse. As explored in chapter 3, the normative content of these rights draws, *inter alia*, from IBRs, privacy legislation (national, regional and international) and case law. This suggests the growing recognition of these subset of privacy rights globally. Second, codifying these rights as well as the corresponding obligations in an international soft law adds a sense of legitimacy, particularly so when one considers that most of these rights are promoted and framed by civil society groups. Third, as highlighted in chapter 3, there is a tendency among some

⁷¹⁴ See, e.g., John Tobin and Sarah Field, ‘Article 16: The Right to Protection of Privacy, Family, Home, Correspondence, Honor and Reputation’ in John Tobin (ed), *The UN Convention on the Rights of the Child: A Commentary* (Oxford University Press, 2019) 559 (noting this tendency in the literature).

small technology companies to pledge IBRs as a competitive strategy. Stipulation of these rights in a (soft) law would then provide a legal basis in international law to already existing, albeit limited, industry practices supporting digital privacy rights. Fourth, enshrining some of the privacy rights would also bring harmonization in areas where there are diverging domestic rules. In the case of encryption policy, for instance, countries follow different and often conflicting approaches.⁷¹⁵ By enshrining in an international soft law a right to use PETs, it may contribute towards narrowing down such divergence in approach.

But of course, this must be done with caution. In particular, the conceptual-theoretical ambiguities imbedded in many of the IBRs must be weeded out. As considered in chapter 3, most IBRs documents embody a ‘right to *use* encryption’ whereas a few other provide for a ‘right *to* encryption’. But no clear conceptual demarcation is drawn between these seemingly different rights. As submitted in that chapter, in terms of conceptual coherence and practicality, the ‘right to *use* encryption’ is more sensible. But again, that right is not conceptually broad enough to embrace technologies that are increasingly applied to enhance privacy in the digital space. Beyond encryption, technologies such anonymizers, ToR, software that filter cookies, spyware and other tracking codes considerably enhance privacy. Because of this reality, the soft law should guarantee a broader ‘right to *use* privacy enhancing technologies’ to properly capture state of the art. As elaborated in appendix 3, the ‘right to PETs’, therefore, embraces not only the right to *use* encryption technologies but also the right to anonymity which feature disparately, as highlighted in chapter 3, in some IBRs instruments.

3 Permissible Restrictions

Except for a generic clause in Art 29 of the UDHR and the ‘arbitrary and unlawful’ clauses in the privacy provision of the ICCPR, no proper limitation clause is, as considered in chapter 1, provided in privacy provisions of international human rights law. The problem with the absence of a limitation clause is that it opens the door for a narrow interpretation the right to privacy. To address this gap, the soft law should provide a fully-fledged ‘limitation clause’. Such a clause can easily be adapted from other rights in the ICCPR such as the rights to freedom of expression, peaceful assembly and association or other regional instruments such as the ECtHR whose privacy provisions provides a limitation clause.⁷¹⁶ Many IBRs initiatives also offer useful samples of a limitation clause, one example being the African

⁷¹⁵ On the diverse mosaic of encryption policies, see Wolfgang Schulz and Joris van Hoboken, ‘Human Rights and Encryption’ (UNESCO Series on Internet Freedom, 2015) 29-49.

⁷¹⁶ The Siracusa Principles also offer a sample limitation clause comprising the requirements of ‘prescribed by law’ (legality) and ‘in a democratic society’ (necessity). Note, though, that it – in a complex set of principles – subsumes the requirements of proportionality and legitimate aim under necessity. See Siracusa Principles, above n 194, part I.

Declaration of Internet Rights and Freedoms.⁷¹⁷ An appropriate limitation clause would provide at least the following three grounds for restriction:

First, it should provide the requirement of ‘legality’ – i.e. restrictions must be sanctioned by law that is clear, accessible and specific. Second, it should enshrine the requirement of ‘legitimate aim’ – i.e. the restriction must be necessary in a democratic society to achieve certain legitimate aims like public security. Third, the restriction should be ‘proportional’ to the legitimate aims pursued. Indeed, the HR Committee has developed – albeit in less consistent fashion – aspects of these three tests in its jurisprudence, particularly in its concluding observations. But it often faces opposition from States like the US that constantly argue that the only grounds for restriction under the right to privacy are ‘unlawful’ and ‘arbitrary’.⁷¹⁸ A soft law that is equipped with a proper limitation clause would help counter such opposition, by firmly establishing in international law permissible grounds for restriction.⁷¹⁹

B Core Privacy Principles

In the area of digital privacy, as shown throughout the thesis, principles play an important role in reinforcing and furthering the underlying right to privacy. Good cases in point are principles provided in data protection instruments. Drawing on these, the soft law – in addition to embodying the subset of privacy rights considered above – should incorporate the following core minimum principles.

1 Extraterritoriality of the Right to Privacy

As highlighted at the introduction of the thesis, a defining feature of the ‘privacy problem’ in the digital age is the ubiquity of transnational privacy interference. The Snowden revelations have exposed far-reaching foreign surveillance practices of the Five Eyes States. But the question of whether the right to privacy applies extraterritorially has been controversial. The US, a member of the Five Eyes spy network, has consistently rejected the extraterritorial scope of the ICCPR, including the right to privacy. This has been the case, as shown in chapter 1, despite repeated determinations of the HR Committee, that Covenant rights apply extraterritorially in circumstances where States exercise jurisdiction outside their physical territory. To address this issue, the soft law must decisively stipulate that the right to privacy applies extraterritorially.

In light of the fact that interference with personal privacy occurs remotely in the digital age, the right to privacy makes little sense unless its scope of application

⁷¹⁷ African Declaration, above n 443, art 8.

⁷¹⁸ See, e.g., Keith Harper, ‘Establishment of an HRC Mandate on Privacy Rights Comes at a Critical Time: Explanation of Position by the Delegation of the United States of America’ (26 March 2015) <<http://bit.ly/2fHI53O>>

⁷¹⁹ See below on the question of whether a similar limitation clause should apply when the interference is made by (Internet) corporations.

extends beyond geographic borders. More so when one considers, as highlighted by the Snowden revelations, that US surveillance practices affected subjects outside the US territory. In the wake of the revelations, the US position has loosened to some degree. One instance has been the issuance of a 2015 PPD, as highlighted in chapter 4, that appears to recognize ‘privacy interests’ of non-Americans located overseas. This reflects the growing global consensus on the extraterritoriality of the right to privacy. In explicitly and authoritatively codifying this important principle, the soft law would place under firm legal basis the normative position of various determinations of the HR Committee and further draw universal acceptance.

2 (Data) Privacy Principles

Baseline principles on the right to privacy in the digital age should also be incorporated in the soft law. It should, for instance, enshrine major data privacy principles and other broader procedural safeguards that have found some expression in the UN Privacy Resolutions and widely recognized elsewhere. One such rule concerns ‘metadata’. As discussed in chapter 4, the Resolutions acknowledge the now widely accepted dictum that metadata can be as revealing of private life as the content of the data, more so with the rise of sophisticated technological capabilities such as big data. The soft law must, therefore, extend the protection of the right to privacy to ‘metadata’ in addition to content data.

The soft law should also adopt a broader definition of what constitutes ‘interference’ with the right to privacy in the light of new developments worldwide. Applied in the context of data collection, this would mean that mere collection of personal data constitutes interference and hence must be justified under the three-part tests outlined above. Moreover, the soft law must impose an absolute ban on all forms of mass surveillance, including bulk collection of personal data and bulk device hacking. The absolute prohibition is justified because mass surveillance measures are inherently disproportional.

Data privacy rights and principles should also be provided in the soft law. As considered in chapter 3, most IBR initiatives – in addition to the subset of privacy rights – embody what elsewhere are to be found in data protection instruments. Examples in this regard are the ‘right to be forgotten’ and the ‘right to information self-determination’. To some degree, the UN Privacy Resolutions have also flagged widely accepted data privacy principles, as discussed in chapter 4. The proposed soft law must go a long that way to address the problem of normative fragmentation in the UN data privacy framework. As examined in chapter 2, normative dispersion typifies the UN data privacy framework. By embracing widely recognized data privacy rights and principles, the soft law would lessen this problem.

However, the essentially regulatory, and hence casuistic nature of data privacy legislation would make it imperative to limit the scope of the soft law to a set of rights and principles. No soft law, be it a GC or a Declaration, on the right to privacy

could adequately accommodate these bureaucratic aspects of data privacy law. This, in turn, would mean relegating the task of covering all aspects of data protection law to a separate global instrument. Such a global instrument – regardless of whether it would ever be introduced – would not only embrace data privacy rights and principles. It would also bring under one roof fragmented UN data privacy standards now contained in multiple soft law instruments, informed further by new developments elsewhere particularly the EU. The best way forward would, therefore, be for the proposed instrument to formally recognize a fundamental right to personal data protection. The international law of privacy, of course, protects data privacy under the broader right to privacy. This is, for instance, overt in the jurisprudence of the HR Committee, particularly GC 16. But recognition of a ‘right to personal data protection’ would have a significant normative value. This value lies primarily in providing an enabling legal foreground to further international regulation in this area.

3 Independent Surveillance Oversight

One of the major challenges in safeguarding digital privacy has been the absence of a robust and independent oversight mechanism for government surveillance measures. Domestic surveillance legislation in many countries does not mandate independent oversight. When an oversight regime exists, the sanctioned oversight lacks independence as well as competence. To help address this gap, the soft law must provide for a mandatory requirement of judicial or at least administrative oversight for (a) conducting of domestic and foreign surveillance, (b) requesting user personal data from third parties and (c) intelligence sharing among States. In line with the UN Privacy Resolutions, IBRs initiatives and jurisprudence of the HR Committee, the soft law must stipulate a mandatory requirement of independent domestic oversight for all surveillance measures. This would allow for each instance of surveillance to pass through the scrutiny of an investigative judge to reduce risks of abuse. Prior judicial or administrative warrant must also be mandated when States seek user personal data for national security and law enforcement purposes from third parties, including Internet corporations. This would respond to the practices of warrantless access to user personal data from technology companies disclosed by the Snowden revelations.

Independent oversight is also equally desirable when States share among themselves intelligence containing user personal data. The need for oversight mechanism in the context of intelligence sharing has recently been recognized by the UN Privacy Resolutions and the post-Snowden concluding observations of the HR Committee as well as the case law of the ECtHR.⁷²⁰ Unlike current prevalent practices, the oversight requirements should be applicable both before the sharing of the intelligence at the

⁷²⁰ See, e.g., Res 71/199, above n 526, [5(d)]; see also ‘Secret Global Surveillance Networks: Intelligence Sharing Between Governments’ (Privacy International, 2018).

originator State, and after the sharing at the receiving State. This is justified because the intelligence is to be passed on to another State's authorities and hence potentially causing new privacy harm. Oversight upon sharing would be crucial in preventing privacy harms that might otherwise arise due to, for example repurposing of the intelligence uses – e.g. initially collected for terrorism and then used for organized crime investigation. This would be the best way to overcome circumvention of domestic restrictions/prohibitions – e.g. for mass surveillance, in the receiving State and the risk that there might not be an independent oversight body in the receiving State.

C Defining Obligations and/Roles of State and Non-State Actors

Defining the respective obligations/roles of State and non-State actors under the right to privacy should be the other substantive aspect of the soft law. In that regard, obligations of two actors must be specified in the soft law: States and (Internet) corporations. The existence of State obligations, both negative and positive, under the right to privacy is incontrovertible.⁷²¹ What the soft law would, then, do in that respect is to define those obligations based on the new realities of the digital age and emerging understandings of the right to privacy. Controversial is the horizontal obligations, or the absence thereof, of non-State actors, particularly corporations – and, to some extent, international organizations. As shall be explained below, defining or foreshadowing the possible obligations of technology companies, in a soft law is both desirable and plausible. The discussion below also briefly flags the role of international organizations focusing on relevant UN agencies and other non-State actors that play a key role in the promotion, respect for and protection of human rights in general and privacy in particular.

In discussing the obligations of States and technology companies, the widely accepted tripartite typology of human rights obligations are employed. These are obligations to 'respect', 'protect' and 'fulfil'. The notion of obligation to 'fulfil' is often associated with economic, social and cultural rights, as opposed to civil and political rights like the right to privacy. But, this chapter considers the obligation to 'fulfil' under the right to privacy in line with the emerging tendency in the literature as well as case law to apply them to civil and political rights.⁷²² Similarly, duties that are sometimes grouped under a distinct obligation to 'promote' are subsumed under the obligation to 'fulfil'. And of course, it worth noting that there is no a clear-cut distinction between the obligation to 'protect' and 'fulfil'.⁷²³ For the sake of clarity, obligations of States and (Internet) corporations considered below follow the three subsets of privacy rights highlighted above.

⁷²¹ See, e.g., generally GC 31, above n 33; see also GC 16, above n 155, [1, 9].

⁷²² See, e.g., Frédéric Mégret, 'Nature of Obligations' in Daniel Moeckli et al (eds), *International Human Rights Law* (Oxford University Press, 2nd ed, 2014) 101-103.

⁷²³ Ibid, 101

1 Obligations of States

(a) *Obligation to Respect*

States' primary obligation under the right to privacy is to 'respect' – i.e. to refrain from measures violating the right.⁷²⁴ Under the 'right to use PETs', the obligation to respect involves refraining from any measure that interferes with the *use* of such technologies by individuals and entities. This obligation should also involve restraint by States from obliging or forcing Internet businesses to install backdoors on their encrypted products/services, provide encryption key escrows or even to disclose encryption keys.

The obligation to 'respect' under 'freedom of surveillance' primarily concerns an absolute prohibition of mass surveillance and mass data collection of personal data generally. Where the surveillance is a targeted one, it should be justified under the three-part tests of the limitation clause and be subject to independent oversight. A more recent manifestation of State mass surveillance practices is resort to 'bulk hacking' of devices such as smartphones.⁷²⁵ Following treatment of hacking as a form of digital surveillance by the HR Committee,⁷²⁶ the latest Privacy Resolution of the UNGA has classified hacking as a surveillance measure.⁷²⁷ In line with this emerging consensus, the soft law must thus totally prohibit bulk hacking in all circumstances. But crucially, characterizing device hacking as a surveillance measure would fill a protection void that the 'right to use PETs' leaves. Unless one is guaranteed protection against arbitrary device hacking, mere right to use, for example encryption services, would not safeguard against access to the decrypted data already loaded on a device.

In defining State obligations under the 'right to the confidentiality and integrity of information systems', regard must be had to its semblance with the 'right to use PETs'. The former appears to guarantee individuals a right to secure digital products and services. End-to-end encryption is perhaps an example of measures that ensure security, integrity and confidentiality of digital communications. But this particular right, as noted in chapter 3, grew of the broader right to personality in German constitutional jurisprudence. It seeks to extend the protection to information systems whose integrity and confidentiality is important for the full development of personality. So, the obligation flowing from this right is distinct from those under the 'right to PETs'. Thus, the obligation to 'respect' would require States to refrain from any measures that weaken the security, integrity and confidentiality of digital services and products.

⁷²⁴ Id, 102.

⁷²⁵ See details on Privacy International's website: <<https://bit.ly/2OQ98ox>>

⁷²⁶ See, e.g., 'Concluding Observation of the HR Committee: Italy' (1 May 2017) [36-37]

⁷²⁷ See Res 73/199, above n 545, preamble.

(b) Obligation to Protect

A State's obligation to 'protect' under the right to privacy concerns a duty to ensure that the right to privacy is not interfered with by third parties.⁷²⁸ A primary duty in that regard, then, is to put in place the requisite legal and institutional framework to uphold the right to privacy. This would involve enacting appropriate regulations on processing of personal data and government surveillance practices. Under the 'right to use PETs', the obligation to 'protect' concerns ensuring that the use of PETs is not obstructed by third parties including by measures that restricts the interoperability of such technologies on digital platforms and services.

Under 'freedom of surveillance', the obligation to 'protect' primarily concerns putting in place legal and institutional arrangements that regulate online monitoring, tracking and profiling by third parties. Regulation of, for instance, private sector data processing falls in this category. Moreover, States must put in place export control in relation to surveillance technologies sold by businesses in their respective jurisdictions. This obligation would involve a requirement of a special license to those types of businesses and rules that regulate when, how and to whom that surveillance technologies could be exported or sold. With a view to prevent sale of these technologies to actors that might use it in a manner contrary to international human rights standards, it is also vital to include an obligation to conduct regular review of the licensing regime.

In line with the case law of the German Constitutional Court, the 'right to the confidentiality and integrity of information systems' involves a positive obligation of 'protect'. Thus, the obligation to 'protect' requires States to take steps to protect the integrity and trustworthiness of information systems they own, or otherwise control to prevent interference by third parties.⁷²⁹ Where applicable, the obligation would involve providing appropriate remedies when the right to privacy is undermined due to breach of security.

(c) Obligation to Fulfil

A State's obligation to 'fulfil' concerns positive measures that facilitate the realization of the right to privacy.⁷³⁰ Under the 'right to use PETs', the obligation to 'fulfil' has two components. First, it includes removing unnecessary barriers to access and use of PETs such as import/export restrictions or discriminatory tariffs. Second, it includes an obligation to raise awareness on the use of technical means of safeguarding (digital) privacy. If formulated with such a precise scope, this positive obligation would avoid possible overlap with the right to education in ICESCR or at least read as a *sui generis* right/duty. The corresponding obligation will be more or

⁷²⁸ See Mégret, above n 722, 103.

⁷²⁹ Quoted in Schulz and van Hoboken, above n 715, 38.

⁷³⁰ See Mégret, above n 722, 103.

less the same under the 'right to the confidentiality and integrity of information systems'. It would involve a duty to promote the importance of enhancing the integrity and confidentiality of information systems, especially those operated or owned by the private sector.

Under freedom of surveillance, the obligation to 'fulfil' involves two distinct obligations. One is that States must provide a notification to the targeted individual once the surveillance has ended. This would allow the individual to ascertain the extent to which the interference with one's privacy was lawful and to further seek remedy. Secondly, States must ensure accessibility of laws that sanction surveillance to any interested party. This would require States not to sanction surveillance under secret laws and procedures, as is the case in some jurisdictions.

2 Obligations/Roles of Internet Corporations

(a) Questions of Plausibility and Scale

Defining the role, responsibility, or obligations of technology companies is the other important aspect of the right to privacy in the digital age. But any attempt to stipulate, or envision, obligations of Internet businesses in the proposed soft law is likely to generate controversy. This, as already discussed, is because of the absence of direct corporate human rights obligations in international law. In making corporations in general and Internet corporations in particular duty-bearers in international human rights law raises fundamental questions. A primary question, in this regard, is whether it is legally, conceptually and practically plausible to impose direct human rights obligations on Internet corporations. Alwicker argues that the notion of extending the reach of human rights to apply horizontally is implausible because (i) it lacks any legal basis and (ii) there is no consistent and uniform State practice.⁷³¹ Specifying the role or obligation of Internet businesses in the soft law would not, however, attract as much controversy for the following reasons:⁷³²

First, that these 'obligations' would be envisaged in a soft law – i.e. with no legally binding force, means the possibility of objection, particularly from Internet corporations is remote. But beyond its lack of binding force, there are reasons to suggest that Internet corporation might not oppose it, if not support it. One is that major Internet corporations have over the years openly called for stronger privacy standards. One recalls occasional calls by tech giants for global privacy standards, more recent instances being Apple's call for GDPR-like US federal privacy law, Google's initiative for a framework for data privacy regulation and Facebook's call

⁷³¹ Alwicker, above n 95, 598.

⁷³² Note that the discussion here deliberately uses the terms 'role' and 'obligations' interchangeably because the soft law cannot strictly impose 'obligations' but the argument is made in a programmatic sense that international law must evolve towards imposing direct human rights obligation on at least some corporations, particularly those operating in cyberspace.

for a 'common global framework' on privacy.⁷³³ Add to that emerging privacy-protective industry practices of rolling out PETs. While such corporate pro-privacy views and practices must be taken with scepticism, codifying obligations in the soft law that essentially reflect what they publicly preach for would give the legal basis Alwicker mentions. What the soft law seeks to do is distil these practices and articulating them in manner that could draw widespread and consistent application by businesses. Arguably, the more legal norms resonate with already accepted practices and standards, the more they would have 'persuasive appeal' and hence of practical value.⁷³⁴

Moreover, in view of the ongoing UN effort to draft a global treaty on the subject, Internet businesses are more likely to settle for the soft law than a treaty. In considering the debates on the international regulation of corporations, regard must be had to the fact the opposition historically come from non-Internet corporations, typical examples being mining and oil companies. Internet corporations are new to the controversy, and the supposed opposition probably does not necessarily apply to them, more so when one considers the above noted positive gestures towards regulation. In part, the corporate push for regulation of their activities is driven by their own business interests. Operating in unregulated environments but often under scandals too damaging to their reputation is counterproductive. As Wouters and Chane note, regulation is good for transnational corporations because it provides legal certainty but importantly reduces the cost implications of reputational damages.⁷³⁵ This would resonate with technology companies that are often plagued with privacy scandals.

Second, these roles or obligations are drawn partly from the UN Privacy Resolutions, but with more specificity and clarification, which have not so far caused any known opposition. And of course, as discussed in chapter 4, some laws at national and regional levels, to some extent, enshrine these privacy rights or aspects of them – and their corresponding obligations. To a degree, privacy laws such as EU's GDPR apply extraterritorially, thereby covering Internet corporations that are not physically located or operate in the respective jurisdiction. There is, therefore, already some precedents by which Internet corporation are subject to enforceable obligations. The soft law would then be an international law equivalent to the

⁷³³ See Russell Brandsom, 'Tim Cook Wants a Federal Privacy Law — but so do Facebook and Google', *The Verge* (online), 24 October 2018 <<https://bit.ly/2qaAYSg>>; see also 'Google: Framework for Responsible Data Protection Regulation' (September 2018) <<https://bit.ly/2DoNt5m>>; Mark Zuckerberg, 'The Internet Needs New Rules: Let's Start in Four Areas', *The Washington Post* (online), 30 March 2019 <<https://wapo.st/2uEbrTT>>.

⁷³⁴ Of a related pointed, see Tobin, above n 26, 22 (citing Ryann Goodman, 'Sociological Insights into International Human Rights Law' (IILJ International Legal Theory Colloquium: Interpretation in International Law, NYU School of Law, 3 April 2008).

⁷³⁵ See Jan Wouters and Anna-Luise Chance, 'Multinational Corporations in International Law' in Math Noortmann et al (eds), *Non-State Actors in International Law* (Hart Publishing, 2015) 238, 250.

increasing transnational regulation of Internet corporations. Another reason why stipulation of corporate privacy obligations would be less controversial is that international human rights law already contemplates or implies an implicit negative obligation of non-State actors to ‘respect’.⁷³⁶

Third, the soft law as conceived in this chapter is essentially, to use Dupuy’s term, a ‘programmatory law’,⁷³⁷ that seeks to shape the progressive development of international privacy law. The aim here, then, is to envision a future of international law that embraces Internet corporations as duty-bearers alongside States. As the law develops progressively, the obligations considered below represent the types and forms that international law must, or would, impose. Soft law, indeed, often reinforces not just what the current law on a given topic is but also reflects ‘future law’ which becomes law proper once adequate consensus builds around it.⁷³⁸ Handl et al note that a ‘substantial part of soft law already describes, in an impressionistic way, part of the (hard) law of tomorrow’.⁷³⁹ Codifying obligations of corporations in soft law would also facilitate the discourse and doctrine on the obligations of corporations in international law. It would provide a ‘common language’ in the debate on corporate human rights obligations.⁷⁴⁰ This is what Abbott intimates as the role of a soft law in initiating an institutional process and ‘normative dialogue’ that might later ripen into hard legalization.⁷⁴¹ Thus, a programmatic vision with respect to corporate human rights obligations is methodologically useful in clarifying the nature of rights, although those rights are not enforceable.⁷⁴²

A corollary to the above question is the legal and practical implications of introducing direct human rights obligations on corporations. In particular, four core questions arise:

Does it mean corporations would directly be held to account before courts and quasi-judicial bodies like the HR Committee?

That is not what is being proposed here, for three reasons. First of all, corporations are not parties to human rights treaties like the ICCPR, and importantly its first

⁷³⁶ See Manfred Nowak and Karolina Januszewski, ‘Non-State Actors and Human Rights’ in Noortmann et al (eds), above n 735, 159; see also John Knox, ‘Horizontal Human Rights Law’ (2008) 102 *American Journal of International Law* 1, 20.

⁷³⁷ René Dupuy, ‘Declaratory Law and Programmatic Law: From Revolutionary Custom to “Soft Law”’ in R.J. Akkerman (ed), *Declaration on Principles: A Quest for Universal Peace* (Kluwer Law International, 1977) 248, 254.

⁷³⁸ See Higashi, above n 599, 23-24.

⁷³⁹ See Handl et al, above 346, 388.

⁷⁴⁰ See Steven Ratner, ‘Corporations and Human Rights: A Theory of Legal Responsibility’ (2001) 111 *Yale Law Journal* 443, 545.

⁷⁴¹ Kenneth Abbott, ‘The Many Faces of International Legalization’ (1998) 92 *Proceedings of the Annual Meeting of the ASIL* 57, 63.

⁷⁴² Of a related point, see Eric Boot, *Human Duties and the Limits of Human Rights Discourse* (Springer, 2017) 67.

Optional Protocol that mandates a complaints procedure, simply means corporations as respondents/defendants is inconceivable. But at a more general level, the lack of judicial recourse per se would not diminish the existence of a right or a correlative obligation. Even without judicial mechanisms of enforcing rights, the value of rights (and obligations) will exist when there is, as Higgins writes, an authoritative source and an accompanying expectation of the international community.⁷⁴³

The second reason concerns a basic point of practicality. The principal monitoring body relevant to privacy at the international level is the HR Committee. But as considered in chapter 1, the Committee is handicapped by a host of structural setbacks. It is not only a part-time body that meets just three times in a year but also has frequent reshuffling of members. On top of its lack of authority to give authoritative decisions, it is already inundated with backlogs. For the most part, similar observations apply to other relevant treaty bodies that monitor treaties where the right to privacy is provided.

A related point that makes litigation or judicial/quasi-judicial recourse less realistic is the sheer number of potential duty-bearer Internet corporations. No international judicial or quasi-judicial body would withstand the deluge of suits if corporations could be sued, certainly not the Committee. Therefore, it would be implausible to envisage a scenario where corporations could be held to account through a judicial means. The issue of practicality relates to the underlying argument made in chapter 6 that dialogue, as opposed to litigation, at the international level goes a long way in realizing human rights, including the right to privacy. But the provision of rights and obligations would be a tool to engage Internet corporations in discussions, for instance, at the proposed multi-stakeholder privacy forum.

Would all Internet corporations bound by these obligations irrespective of their market share, user base or any other criteria?

In international human rights discourse, the issue of which non-State actors should be envisaged as duty-bearers is fiercely debated.⁷⁴⁴ This is precisely because the ‘more diverse the range of duty-bearers, the higher the risk that human rights get diluted’.⁷⁴⁵ Pertinent to the case in question is the issue of ‘which’ Internet corporations should be duty-bearers vis-à-vis the right to privacy. The diversity of Internet corporations in terms of market share, user-base, loci of influence and the

⁷⁴³ Rosalyn Higgins, *Problems and Process: International Law and How We Use It* (Oxford University Press, 1995) 98, 102.

⁷⁴⁴ See generally, Wouters and Chance, above n 735.

⁷⁴⁵ See Wouter Vandenhoe and Willem van Genugten, ‘Introduction: An Emerging Multi-Duty-Bearer Human Rights Regime?’ in Wouter Vandenhoe (ed), *Challenging Territoriality in Human Rights Law: Building Blocks for a Plural and Diverse Duty-Bearer Regime* (Routledge, 2015) 4.

attendant dynamism dictates some form of criteria as to who is subject to the soft law, or more generally in a future treaty law.

Criteria considered in the human rights literature range from one that includes ‘all’ non-State actors, those that possess ‘institutional power’ to those that are ‘relevantly public’.⁷⁴⁶ In commenting on the ‘zero draft’ of the business and human rights treaty, Ruggie rightly notes that the issue of ‘scale’ is key in determining which of the transnational corporations fall under the treaty regime.⁷⁴⁷ The huge number of transnational corporations, and the complexities in the supply chain, raises a question of scale. This is because scale is crucial in the effective implementation of a treaty, particularly in attributing liability to the appropriate delinquent party. As noted above, inclusion of ‘all’ non-State actors, including corporations, would render the protective regime ineffective. In the digital rights context in general and privacy in particular, at least the following three criteria must be considered in identifying which Internet corporations are bound, or rather covered, by the soft law.

One is the truly transnational nature of the relevant corporation. This concerns particularly whether the relevant corporation operates in a single or a few jurisdictions, or the world over. The proposed soft law must be restricted to those corporations that have global operations but are subject only to the laws of one or more jurisdictions. Secondly, the nature of operation of the relevant corporations must also be taken into account in that the extent to which the corporation involves in collection, processing and sharing of personal data. This would exclude those whose primary operations do not pose threats to the privacy rights. Thirdly, the user-base of the Internet corporation should be considered. Technology companies that have users above a given threshold should be bound by the soft law. In applying these criteria regard must, however, be had to the characteristically dynamic nature of the digital corporate marketplace. The not too uncommon rise and fall of Internet firms as well as fluctuation or saturation of user-base, dictated by various factors, must be taken into account in defining the ‘scale’.

⁷⁴⁶ Ibid, 4-5 and the accompanying footnotes; see also Ratner, above n 740, 497-520 (discussing four criteria namely: the corporation’s relations with government, nexus to the affected population, the rights at issue and the internal corporate structure).

⁷⁴⁷ See John Ruggie, ‘Comments on the “Zero Draft” Treaty on Business and Human Rights’ (Business and Human Rights Resource Center, August 2018) <<https://bit.ly/2DcDv75>>; see also Knox, above n 736, 41 (warning against ‘overinclusion’ of corporations).

*What happens when corporations fail to comply with obligations stipulated in the soft law?*⁷⁴⁸

The use of the terms ‘rights’ and ‘obligations’ necessarily suggest consequent ability of individuals to seek remedies and imposition of sanctions against delinquent duty-bearers. Rights and obligations envisioned here are normatively soft means they are theoretically nominal. But on top of the soft law’s aim of foreshadowing ‘future law’, the underlying argument of the thesis for a dialogical approach reduces the role of sanctions. As shall be argued in chapter 6, an effective way of addressing enforcement problem of the international law of privacy is by entrenching the already existing ‘cooperative dialogue’ framework in the UN human rights system. The transnational nature of privacy threats increasingly makes litigation a less effective means of securing digital privacy. Envisaging rights and obligations at the international level would, however, shape the development of privacy law at regional and domestic levels where litigation is more likely to bear fruit.

Furthermore, present institutional arrangements at the international level, for instance the part-time HR Committee, are not structurally best positioned to meaningfully enhance protection of the right to privacy through litigation. Therefore, legal effects of the digital rights and obligations stipulated in the proposed soft law would play out in three ways. First, as part of the soft law’s role of providing a roadmap for the dialogical approaches to privacy explored in chapter 6, those rights and obligation would serve as a way of engaging Internet corporations in the multi-stakeholder privacy forum. Second, the rights and obligations would inform the making of laws and decisions at domestic and regional levels, thereby localising (but hardening) soft international norms. Third, soft law would also provide an authoritative digital privacy advocacy tool to civil society groups, including in their strategic litigations before domestic and regional courts. Over the course of time, this would embed international privacy norms at the local level and hence enhance global protection of privacy.

What balancing test, i.e. limitation clause, should apply when the impinged restrictions are made by corporations?

In his theory of corporate human rights obligation, Ratner posits only a single countervailing interest: the ‘rights and interests’ of the relevant corporation in the restriction of the right in question.⁷⁴⁹ No doubt, the three-step tests of ‘legality’,

⁷⁴⁸ Perhaps another question would be: *what would be equivalent to the notions of jurisdiction and/or territorial control when it comes to corporate human rights obligations?* As Karavias rightly suggests, the decisive point is the factual situation where corporations exert functional control based on their factual relations with individuals. See Markos Karavias, *Corporate Obligations Under International Law* (Oxford University Press, 2013) 173-174. As such, the proposed corporate obligations under the right to privacy would apply to all netizens/users to whom Internet corporations offer services/products based on, e.g., contractual arrangements.

⁷⁴⁹ Ratner, above n 740, 512-515.

‘necessity’ and ‘legitimate aim’ that ordinarily apply to States cannot simply be transposed to corporate rights restricting measures. But Ratner’s approach gives too broad a latitude to corporations in restricting human rights. What is more appropriate, then, is a limitation clause that slightly adapts the three-part tests to the corporate world. Accordingly, the requirement of ‘legality’ in the corporate context would be fulfilled if the relevant corporation has a legal duty, right or some other legal basis such as contract that allows interference with the privacy rights.⁷⁵⁰ The restriction must then be ‘necessary and proportionate’ to achieve the legitimate aim pursued. Legitimate aims would include legitimate business interests of the corporation.

(b) Obligations/Roles

If the case for introducing direct corporate obligations under the right to privacy is persuasive, technology companies must be required to discharge the same tripartite obligations to ‘respect’, ‘protect’ and ‘fulfil’. Just like State obligations outlined above, the corporate obligations follow primarily the three subset of privacy rights.

(i) Obligation to Respect

Corporate obligations to ‘respect’ under the ‘right to use PETs’ and the ‘right to the confidentiality and integrity of information systems’ overlap. Thus, under the obligation to ‘respect’, corporations owe three distinct duties under both rights. First, they should refrain from any measures – including in collusion with States – that may weaken the security of computer systems or obstruct the use of PETs. Second, they should refrain from heeding to unlawful requests from States to install backdoors to their services or provide encryption keys. Third, they should refrain from selling or otherwise making available tools that may be used by States to undermine the security of information systems or products/services.

Under ‘freedom of surveillance’, the obligation to ‘respect’ should have four elements. First, technology corporations should refrain from engaging in unlawful tracking and profiling of their users either for their own business interests or as a proxy for State law enforcement purposes. Part of this obligation must be to refrain from designing technologies in a manner that enables surveillance contrary to international privacy standards. Second, they should not arbitrarily block or deny access to users relying on anti-tracking technologies. Third, they should refrain from disclosing user personal data to States without appropriate judicial authorization. Fourth, they should refrain from selling or otherwise making available technologies

⁷⁵⁰ Cf Karavias, above n 748, 189-191 [suggesting (in the context of ‘balancing corporate and individual rights’) that when domestic law specifies circumstances of permissible restriction by corporations, the requirement of legality would be met]. Note that the thesis does not envisage, unlike Karavias, corporations as rightsholders.

to third-parties that undermine the enjoyment of privacy where there is an apparent risk of abuse.

(ii) Obligation to Protect

Corporate obligations to ‘protect’ under the ‘right to PETs’ and the ‘right to confidentiality and integrity of information systems’ are not identical. Under the ‘right to PETs’, the obligation to ‘protect’ falls on those offering PETs to ensure that available security features are not exploited by third parties, including State intelligence agencies. This would involve a requirement to put in place a mechanism by which such exploitation is addressed within a reasonable time frame, and where applicable, to provide appropriate remedy.

The obligation to ‘protect’ under the ‘right to the confidentiality and integrity of information systems’ is to ensure the security and confidentiality of computer systems operated or owned by Internet businesses. One can think of here a requirement of deploying TLS in default to ensure confidentiality of communication between users and service providing corporations. In addition, corporations should provide notification to users where the security of their information systems is breached and where applicable provide appropriate remedies. More generally, the obligation to ‘protect’ must also include a requirement to ensure that international privacy standards are taken into account during the design as well as the operation of new technologies such as big data analytics, AI and machine learning.

Under ‘freedom from surveillance, the obligation to ‘protect’ has two components. First, corporations should take all reasonable steps, including through legal action, to prevent unlawful access to the personal data of their users. Second, they should protect their users from unlawful surveillance measures of third parties including State actors.

(iii) Obligation to Fulfil

The boundary between the obligation to ‘protect’ and ‘fulfil’ is, as already noted, not clear-cut. But the following obligations may fall under the corporate obligation to ‘fulfil’. Under the ‘right to PETs’, the obligation to ‘fulfil’ requires Internet businesses to take all reasonable steps to enable the use of PETs on their products, services or platforms. This would include ensuring interoperability of PETs on their websites or products. Under the ‘right to the confidentiality and integrity of information systems’, the obligation to ‘fulfil’ involves primarily a duty to inform or notify users. One is that technology companies that offer e-2-e communication services must inform users as to the nature and type of security feature included in particular communication sessions. This later positive obligation would simply codify recent

industry practices of providing notification to users regarding whether a given communication session is encrypted and the type/level of encryption.⁷⁵¹

Unlike ‘freedom of surveillance’, the corporate obligation to ‘fulfil’ concerns primarily adoption of transparency policies/reports at various stages. At a more general level, corporations should be required to issue regular transparency reports that offer the nature and extent of requests for user personal data lodged by State organs. In individual cases, they should inform a user when his personal data has been handed over to law enforcement agencies. Such transparency reports and notices would allow individual users to be informed when they have been subjected to surveillance or when request for their personal data is made by State agencies. The requirement of transparency should also extend to cases where businesses are involved in supplying surveillance technologies to third parties, including State actors. Such reporting should indicate as to which States and other non-State actors that such technologies have been supplied. With such disclosures, relevant human rights monitoring bodies can make meaningful review or scrutiny of States to whom such technologies were supplied.

3 Roles of Other Non-State Actors

The role of at least three groups of non-State actors must ideally also addressed in the soft law. First, the important role of civil society groups in supporting the respect for and protection of the right to privacy must be recognized. Such recognition is important because the ICCPR, unlike other human rights treaties, does not envisage a role for civil society. The proposed soft law must, for instance, recognize the important role of civil society in upholding the right to privacy particularly in raising public awareness, assisting individuals seeking redress and in mobilizing public opinion towards ensuring compliance by States of their human rights commitments.

In flagging emerging practices, both of States and businesses, that threaten the right to privacy, civil societies would play a role in enhancing accountability and transparency. Participation of civil society in the privacy forum is also important on many levels. For one, their advocacy work has the capacity to put significant social and political pressure on the ‘unsteady political will of States’.⁷⁵² One way to do so would be by highlighting in the privacy forum not only emergent anti-privacy practices or measures but also civil society groups could also play a key role in offering expertise on technical and complex issues surrounding privacy.

A second category of non-State actors includes international inter-governmental organizations, particularly specialized and related agencies of the UN. As examined

⁷⁵¹ See, e.g., ‘How Private Are Your Messaging Apps?’ (Amnesty International, 3 November 2016) <<https://bit.ly/2HnI4y7>>

⁷⁵² See Dupuy, above n 619, 465.

in chapter 2, a handful of UN specialized agencies have adopted intra-agency data protection policies. The adoption of these internal policies is mainly inspired by the UN Data Privacy Guidelines which call upon international organizations to introduce corresponding data privacy documents based on their specific needs. Arguably, these policies — by requiring those organization to put in place a framework through the right to privacy, among other objectives, could be upheld — tend to come close to putting international organization within the radar of international human rights law. Like corporations, whether international organizations, including UN agencies, are bound by international human rights law alongside States is a long-running debate.⁷⁵³ But stipulation of their obligation/role in the proposed soft law may not be as much controversial for two reasons.

One is that there is already proscription in the UN Data Privacy Guidelines, albeit in soft law language, to introduce data privacy policies. Soft law would basically elevate this proscription to a higher normative status, given that a Declaration appears to sit above Guidelines in the hierarchy of soft legalization.⁷⁵⁴ Second, best practices of already adopting internal data privacy policies means that envisaging UN specialized agencies in the soft law would simply provide a firm legal basis to these trends. Therefore, the idea of international organizations being potential duty-bearers is plausible. Their primary duty, then, would be to introduce internal data protection policies with a view to safeguard privacy rights of their clients or persons of concern. The soft law would circumscribe the obligation only to international organizations that routinely process personal data as part of their operations. This further would mean that the privacy rights discussed above would not necessarily apply to them.

The technical community such as the Internet Engineering Task Force (IETF) and Internet Architecture Board (IAB) that set core Internet standards is the third category of non-State actors to be addressed in the soft law. Recent efforts of the IETF and IAB to set standards in manner that overcome technical attacks, including surveillance, should be backed up through the soft law. In specifying their role, it would both formalize and sustain their effort in strengthening the protection of privacy at a technical level. The role would involve ensuring that Internet and web technical standards are designed in such a way to counter unlawful surveillance. The soft law must also ideally recognize the role of these technical bodies in the proposed privacy forum. The technical community would particularly assist in providing expertise at the Forum.

D A Question of Form

If the normative boundaries of the soft law are drawn, the next question is one of form. Soft law takes various forms in the repertoire of international legislation.

⁷⁵³ See, e.g., Nowak and Januszewski, above n 736, 156-158.

⁷⁵⁴ See more in section D below.

International instruments that are often considered under the rubric of soft law range from Declarations and Resolutions, GCs to policy briefs of civil society organizations. Chinkin points out two broad categories of soft law: legal and non-legal soft laws.⁷⁵⁵ While Declarations of the UN fall under the ‘legal soft law’ category, Resolutions, Codes of Practice, GCs and civil society policy briefs are treated as ‘non-legal soft laws’. This section considers which form of soft law is more suitable in effectively carrying the normative contents of the proposed soft law discussed above. Having examined the propriety of various soft law alternatives, it leans towards a UNGA Declaration as a pertinent instrument to enshrine the proposed elements of the soft law.

A primary candidate in terms of soft legalization is a GC. This can be achieved with the adoption of a GC on the right to privacy by relevant UN treaty bodies, more appropriately the HR Committee. As considered in chapter 1, the Committee has adopted GC 16, in 1988. But given the time when it was adopted, it now has little to offer in terms of providing guidance on the broader and novel issues surrounding the right to privacy in the digital age. With the recent amplified calls upon the Committee to update the GC – including by the UNGA, the HR Council, UN Special Rapporteurs, civil society and academia, it is likely that a new GC may be adopted in the not too distant future. The question, however, remains as to the extent to which such a GC would assist in filling normative gaps of the international law of privacy.

The major concern relates to the normative value or status of a GC which, in turn, would determine its reception by States and other possible addressees. In contrast to, for example Resolutions or Declarations of the UNGA, GCs are less authoritative for being adopted by treaty bodies. There exists little reason to suggest that a GC would readily be accepted, and trigger implementation.⁷⁵⁶ One must also consider the fact that GCs, unlike other soft laws, have a rather limited reach. As an instrument borne out of a dedicated human rights treaty, States not party to the relevant treaty such as the ICCPR would not be required to pay heed to it. The legitimacy and acceptance of the GC further dwindles when one considers that one possible normative source for a future GC might be — as often is the case — the case law of the HR Committee developed under the first Optional Protocol. State Parties to the ICCPR, but not the Protocol, are likely to resist monitoring based on standards carved out of processes from which they purposefully opted out. One recalls, in this regard, the objection from some States when aspects of the Committee’s draft GC on reservations, and more recently on the right to life, were perceived to have went beyond the Committee’s prior case law.⁷⁵⁷ With this precedent in mind, opposition to a

⁷⁵⁵ Chinkin, above n 327, 25-30.

⁷⁵⁶ See Seibert-Fohr, below n 815, 129 (noting the controversy in academia over the legal nature of GC, including the question of whether they even qualify as soft law).

⁷⁵⁷ *Ibid*, 129.

progressive GC on the right to privacy based on, for example ACLU's draft mentioned above, will probably stir opposition.

The part-time nature of the Committee's role, added to the thin jurisprudence on the right to privacy and the work-overload, further cast doubt on the feasibility of a GC in the near future. While adopting a new GC on the 'right to life', the Committee recently stated that next in line is a GC on the 'right to peaceful assembly'.⁷⁵⁸ In considering the fact that the process of adopting a GC takes a few years, the prospect of a GC on the right to privacy is remote.⁷⁵⁹ That said, GC has some inherent advantages, one being that it is easier to undergo amendments since it is all in the hands of the Committee to update or replace GCs.

Other alternative forms of soft law are those adopted by higher UN organs such as UNGA such as Resolutions and Guidelines. Examples in this regard are the four UNGA Privacy Resolutions, examined in chapter 4, and the various UN guidelines on data privacy, examined in chapter 2. The legal nature of these instruments, however, makes them less suited to serve the role of providing normative content for the right to privacy in international law. Resolutions and Guidelines are not structurally pertinent instruments to enshrine substantive principles in sufficient details. As shown in chapter 4, the UN Privacy Resolutions exhibit a level of selectivity when it comes to substantive principles despite the overall attempt of pursuing a unifying approach. The normative force of these instruments also appears to be lower, compared to other soft laws such as Declarations. Perhaps, similar observations apply to other less common UN standard-setting instruments such as 'Rules', 'Standard Rules', 'Standard Minimum Rules', 'Principles', 'Body of Principles', 'Guiding Principles' and 'Basic Principles'.⁷⁶⁰ More desirable, then, is a soft law that is both structurally pertinent and normatively strong so as to draw wider acceptance.

This brings us to a UNGA Declaration. In contrast to the above highlighted soft laws, Declarations of the UNGA appear to sit in a higher normative hierarchy but with all the benefits of 'softness' in international lawmaking. While the place of Declarations in the hierarchy of international legalization is less clear, it has come to assume an important normative value in practice. Indeed, the term 'Declaration' appears nowhere in the UN Charter, except as a title to Chapter XI of the Charter. The term is often used synonymously with 'Resolution', which is also not named within the Charter. But generally, the term Resolution is taken to represent a 'Recommendation' which finds expression under the Charter. Instruments such as the UDHR are sometimes misleadingly referred to as Resolutions.⁷⁶¹ Resolutions, like 'Declarations'

⁷⁵⁸ See 'UN Human Rights Committee Publishes New General Comment on the 'Right to Life'' (OHCHR Press Release, 1 November 2018) <<https://bit.ly/2P41uvm>>

⁷⁵⁹ The work on GC 36 on the 'Right to Life' took three years (2015-2018).

⁷⁶⁰ For a list of UN instruments bearing these nomenclatures, see <<http://bit.ly/LAdFKU>>

⁷⁶¹ See, e.g., Shelton, above n 597 in Shelton (ed), above n 327, 450.

and ‘Decisions’, are legal instruments that are formal expressions of political will.⁷⁶² And customarily, treaties and Declarations adopted by the UNGA are prefaced by Resolutions. But there appears to exist a stark difference between Resolutions and Declarations when it comes to their normative value.

UN practice suggests that Declarations are instruments that contain important legal and political principles. An earlier memo of the UN Office of Legal Affairs issued in response to a request for clarification by the former Commission on Human Rights regarding the distinction between Declaration and Recommendation (i.e. Resolution) states as follows:

In United Nations practice, a ‘declaration’ is a formal and solemn instrument, suitable for rare occasions when principles of great and lasting importance are being enunciated, such as the Declaration of Human Rights. A recommendation is less formal. [...] However, in view of the greater solemnity of a ‘declaration’, it may be considered to impart, on behalf of the organ adopting it, a strong expectation that members of the international community will be abide by it. [...] a declaration may by custom become recognized as laying down rules binding upon States.⁷⁶³

This memo suggests that the underlying distinction between Declaration and Resolution is that of value in normative terms. Resolutions generally tend to be exhortations while Declarations ‘codify’ a subject matter.⁷⁶⁴ A great deal of UNGA Resolutions are mere ‘exhortations’ than articulation of legal norms.⁷⁶⁵ Perhaps, an exception could be made for certain types of Resolutions, such as those Bleicher calls ‘law-giving Resolutions’, which move slightly beyond mere exhortatory statements on a given event, action or inaction.⁷⁶⁶ As highlighted in chapter 4, the latest UN Privacy Resolutions appear to be Resolutions of the latter type. But while these Resolutions appear to flag some privacy principles, and paved the way for further discussion in the area, they still fall short in adequately addressing the matter in a comprehensive manner. In part, this is for the obvious reason that Resolutions are not structurally best-placed to be instruments that articulate legal rights and principles, not to mention institutional norms. A Declaration on the right to (digital) privacy, therefore, would be a pertinent instrument to carry forward the aim of the Privacy Resolutions but in a more holistic manner, and higher normativity.

⁷⁶² See Rainer Lagoni, ‘Resolution, Declaration, Decision’ in Rudiger Wolfrum (ed), *United Nations: Law, Policies and Practice* (Springer, 1995) 1081.

⁷⁶³ See Memorandum by the Office of Legal Affairs, above n 613.

⁷⁶⁴ See Jorge Castenada, ‘The Underdeveloped Nations and the Development of International Law’ (1961) 15 *International Organizations* 38, 38.

⁷⁶⁵ For a comprehensive list of UNGA Resolutions, see <<http://bit.ly/1InBBIV>>

⁷⁶⁶ See Bleicher, above n 552, 458.

A Declaration would also slightly move beyond the soft language of Resolutions especially in articulating obligations of States and perhaps Internet corporations. This is partly because UN Declarations are often framed in such a manner that they seek observance from their addressees. One recalls, in this regard, the Declaration on the Granting of Independence to Colonial Countries and Peoples which states that it shall be observed ‘faithfully and strictly’.⁷⁶⁷ And, a subsequent UNGA Resolution authorizes the UN Decolonization Committee to monitor the implementation of the Declaration by ‘all means’.⁷⁶⁸ Other Declarations likewise appear to seek observance unconditionally with the use of obligatory terms. The Declaration on Freedom of Religion, for instance, appears to impose obligations on States, with terms such as ‘all states shall take effective measures or shall make all efforts’.⁷⁶⁹ Moreover, a soft law instrument like a Declaration could carry more normative force when its implementation is supervised by a monitoring body.⁷⁷⁰ As will be examined in the next chapter, the proposed institutional reform ideas would be useful in overseeing the implementation of the soft law.

IV CONCLUSION

This chapter argued that a pertinent approach towards lessening the ‘normative gap’ in the international law of privacy is adoption of a soft law supplement. A ‘supplement’ because there are already high-level privacy principles codified both in international hard laws such as the ICCPR as well as a range of soft laws on data privacy. Mapped onto these extant rules of international privacy law, the proposed soft law would make these rules better equipped in the digital age. As this chapter demonstrated, a well-framed programmatic soft law is an apposite instrument to translate international privacy initiatives, particularly the IBRs Project and the ongoing UN Privacy discourse, into a meaningful reform.

Because these initiatives, as shown in chapters 4 and 5, are unlikely to develop into a reform that would sufficiently reimagine the international law of privacy, this thesis takes the position that the best way forward is a soft law that draws upon aspects of these global privacy initiatives. In embracing substantive aspects of the IBRs and the privacy discourse as well as the latter’s political capital, the soft law would reimagine the right to privacy. This would effectively respond to normative gaps of the international privacy law. The next chapter explores on the way in which the structural-institutional gaps may be addressed through a set of dialogical approach.

⁷⁶⁷ *Declaration on the Granting of Independence to Colonial Countries and Peoples*, GA Res 1514 (XV), 15th sess, UN Doc A/RES/1514(XV) (14 December 1960) [7].

⁷⁶⁸ *The Situation with regard to the Implementation of the Declaration on the Granting of Independence to Colonial Countries and Peoples*, GA Res 1654 (XVI), 1066th plenary mtg (27 November 1961) [6].

⁷⁶⁹ See GA Res 36/55, above n 694, art 4.

⁷⁷⁰ See Shelton, above n 594, 14.

CHAPTER 6 — MORE BUT FOCUSED DISCOURSE: TOWARDS A DIALOGICAL APPROACH TO DIGITAL PRIVACY

I INTRODUCTION

This chapter turns to explore the second strand of the pragmatic approach: a dialogical approach to digital privacy. As shown in chapters 1 and 2, institutional gaps are rife both in the international human right to privacy and data privacy regimes. The human right to privacy framework is overseen by the HR Committee not only with no strong monitoring authority but also beset by structural constraints. Worse, institutional arrangements in the data privacy framework are as deeply fragmented as its norms, and lack adequate monitoring capacity. The lack of an effective institutional machinery, added to the underlying normative weaknesses, makes international privacy law ill-equipped to respond to the ‘privacy problem’ in the digital age. Chapter 5 examined virtues of introducing a soft law supplement towards lessening the normative gaps. The present chapter explores how and why a dialogical approach is the practical way of reducing institutional, and hence implementation, challenges.

As this chapter will show, rebuilding the UN human rights system’s ‘cooperative’ dialogue framework is the most effective way of remedying institutional gaps. Rejecting radical proposals such as the often-made plea for a world human rights court or hardening decisions of treaty bodies, the chapter argues that a dialogical approach wields the potential of realistically lessening the institutional lacuna, particularly in the international law of privacy. The term ‘dialogical’, in this context, is used in its ordinary dictionary meaning. Oxford English Dictionary defines the word ‘dialogic’ as ‘relating to or in the form of dialogue’.⁷⁷¹ By ‘dialogical approach’ the aim here is, then, to capture a mechanism that rely on fostering and reinforcing conversations on current and emerging privacy challenges among key players in the digital privacy domain.

A key feature of the proposed dialogical approach is that it favours sustained conversation, in formal settings, among actors involved in the promotion, respect and protection of the right to privacy. The main argument is that the nature of the ‘privacy problem’ requires mechanisms of enhancing compliance that relies primarily on engaging and persuading those actors that hold a unique position in the digital environment for the protection, and of course, violation of human rights. This notion of a dialogical approach coincides with its use in other areas of (international) law. One finds an example in international economic law where a ‘dialogical approach’ is meant to represent ways in which stakeholders in a given

⁷⁷¹ See <<https://en.oxforddictionaries.com/definition/dialogic>>

subject engage on cross-cutting issues.⁷⁷² In line with this conception, this chapter explores virtues of establishing a ‘multi-stakeholder privacy forum’. It argues that a privacy forum that brings together relevant stakeholders and facilitated by the SRP, would considerably complement and reinforce the work of existing institutional arrangements, particularly the HR Committee.

II VIRTUES OF A DIALOGICAL APPROACH IN THE INTERNATIONAL PROTECTION OF DIGITAL PRIVACY

A dialogical approach is uniquely suited to lessen implementation challenges of current international law of privacy for two reasons. First, it is a less radical and hence pragmatic way in which the objective of upholding digital privacy can be realized. Second, a dialogical approach embodies the dynamism that would allow international law to remain abreast of emerging and complex privacy issues. That makes a dialogical approach adaptive to the unique realities of upholding the right to privacy in the digital environment, where threats are complex and constantly shifting. This section explores these two merits of a dialogical approach.

A Dialogue as a Pragmatic Future

The primary virtue of the dialogical approach is that it is pragmatic. Unlike drastic reform ideas flaunted over the years, dialogical mechanisms are modest proposals that can be realized in the present political reality. But importantly, they would not require reinventing the wheel. Installing a privacy forum, for instance, would not substantially unseat existing institutional arrangements. Installing such a forum would, of course, involve creation of a new body but, as history of other similar UN forums suggests, it might not be a particularly cumbersome venture. As shall become clear, this is in stark contrast with earlier initiatives that would require fundamental restructuring of the entire human rights system.

As part of a broader reform of the UN system of human rights adjudication, various proposals have emerged over the years. One proposal has been to abolish the HR Committee altogether and establish a world human rights court because ‘views’ of the Committee are not legally binding and are, as a result, often ignored in practice.⁷⁷³ To this effect, a ‘Consolidated Statute for a World Court of Human Rights’ has been drafted.⁷⁷⁴ Notably unique and ambitious about this proposal is that it envisioned other ‘entities’, including corporations, as subjects to the court’s

⁷⁷² See, e.g., Elizabeth Trujillo, ‘A Dialogical Approach to Trade and Environment’ (2013) 16 *Journal of International Economic Law* 535, 537-544.

⁷⁷³ See, e.g., Manfred Nowak, ‘It’s Time for a World Court of Human Rights’ in Cherif Bassiouni and William Schabas (eds), *New Challenges for the UN Human Rights Machinery: What Future for the UN Treaty Body System and the Human Rights Council Procedures?* (Intersentia, 2011) 26-28.

⁷⁷⁴ *Ibid*, 28-32.

jurisdiction, albeit on a voluntary basis.⁷⁷⁵ Similar reasoning has also prompted suggestions for the establishment of a world human rights court in the context of the ICESCR.⁷⁷⁶

A related proposal has been for the establishment of two permanent enforcement bodies to replace the 'ineffective' HR Committee.⁷⁷⁷ Some scholars have also advocated for the 'reconstitution' of the entire human rights regime and creation of a system that only 'democratic States' would be invited to join.⁷⁷⁸ Along similar lines, the former High Commissioner Arbour had proposed the creation of a Unified Standing Treaty Body that would replace all treaty monitoring bodies established under UN human rights treaties, including the ICCPR.⁷⁷⁹ An earlier proposal, including by the HR Committee itself, has been to make views of the Committee binding by amending the First Optional Protocol to the ICCPR.⁷⁸⁰ A more domain-specific proposal has also been made, as discussed in the introductory part of the thesis, for a UN agency on data privacy to oversee the implementation of the UN Data Privacy Guidelines.⁷⁸¹

As can readily be gleaned, the nature of these initiatives would require radical restructuring of the human rights system, including the making of new treaties. In light of the international political reality and common challenges of treaty processes, there is little chance for such initiatives to materialize. Nothing best illustrates the feasibility challenge as much as the hibernation of the Swiss initiative for a world human rights court, which was launched a decade ago.⁷⁸² Except for occasional but modest reforms introduced by the OHCHR over the years and the treaty bodies themselves, none of the above reform ideas have also been taken seriously. But it is not also certain whether creation of, for example a human rights court, would result in significant improvement in the protection of human rights. This is precisely because several other factors, beyond lack of an authoritative global human rights body, are

⁷⁷⁵ See Martin Scheinin, 'Towards a World Court of Human Rights: Research Report within the Framework of the Swiss Initiative to Commemorate the 60th Anniversary of the Universal Declaration of Human Rights' (22 June 2009) 19.

⁷⁷⁶ See Manisuli Ssenyonjo, *Economic, Social and Cultural Rights in International Law* (Hart Publishing, 2nd ed, 2016) 651-660.

⁷⁷⁷ See Mutua, above n 127, 258-260.

⁷⁷⁸ See Anne Bayefsky, 'Making Human Rights Work' (1997) 26 *Studies in Transnational Legal Policy* 229, 262-265; see also John Barton and Barry Carter, 'International Law and Institutions for a New Age' (1992/93) 81 *Georgetown Law Journal* 535, 535, 557.

⁷⁷⁹ See *Concept Paper on the High Commissioner's Proposal for a Unified Standing Treaty Body*, UN Doc HRI/MC/2006/2 (22 March 2006).

⁷⁸⁰ See Thomas Buergenthal, 'The UN Human Rights Committee' (2001) 5 *Max Planck Yearbook of United Nations Law* 341, 376.

⁷⁸¹ See De Hert and Papakonstantinou, above n 89, 271 et seq.

⁷⁸² One of the project's progenitors recently acknowledged that the time is not yet ripe for 'such as a fundamental reform'. See Manfred Nowak, 'A World Court of Human Rights' in Oberleitner (ed), above n 611, 288.

liable for the sustained compliance deficit in international human rights law, including lack of political will and resources constraints both in developed and developing countries.⁷⁸³

Having a world human rights court, then, or a HR Committee with a power to issue binding decisions, would not necessarily guarantee effective protection of human rights. The issue, therefore, is not just of feasibility, but also of desirability. It would be unpragmatic to invest available limited resources on initiatives with little hope of turning around the status quo. The dialogical approach argued for in this chapter is premised on this reality in the international protection of human rights in general and the right to privacy in particular. Not only is the proposed dialogic approach feasible but also would considerably assist in mitigating the compliance deficit through engagement and building consensus among key players.

Advancing the human rights movement requires engaging not only States but also other relevant stakeholders. And engagement and the resultant change must involve a process one that requires, as aptly put by Alston, determined ‘incrementalism and organic evolution’.⁷⁸⁴ As this chapter will show, installing a privacy forum is essentially incremental, and constitute an organic progression in international privacy law. What makes this dialogical approach more realistic is that it simply builds upon practices not alien to the international law discourse. The proposed privacy forum, for instance, not only has many precedents in the UN human rights system but also would not require putting in place a new institutional machinery.

Pragmatic underpinnings of the dialogical approach also draw upon the ongoing UN discussions on the right to privacy. As examined in chapter 4, the UN Privacy Resolutions recognize that ‘effectively addressing the challenges relating to the right to privacy in the context of modern communications technology requires an ongoing, concerted multi-stakeholder engagement’.⁷⁸⁵ But the focus appears to be on ‘informal dialogues about the right to privacy’.⁷⁸⁶ The proposed multi-stakeholder forum, with a proper legal basis in international law, and hence formal, would be more effective in enhancing protection of digital privacy. That way, it builds on the consensus building around the UN privacy discourse, especially on virtues of dialogue in privacy protection.

B Dialogue as a Responsive Strategy

A dialogical approach, unlike non-dialogical mechanisms such as adjudication, responds relatively effectively to the unique challenges of securing digital privacy.

⁷⁸³ See Philip Alston, ‘Against a World Court for Human Rights’ (2014) 28 *Ethics and International Affairs* 197, 210-11.

⁷⁸⁴ *Ibid.*

⁷⁸⁵ See Res 71/199, above n 526, preamble, [13] cum [8].

⁷⁸⁶ *Ibid.*, preamble [14].

Dynamism is a characteristic feature of the digital environment where new technologies emerge more rapidly than what law could catch up with. New technological innovations come up with as much new threats to the right to privacy as new and obscure actors that wield significant influence over individuals. Law barely keeps pace with such incessant changes, thereby making legal protection of privacy through the traditional adjudicative means harder. Not only is international lawmaking follows a rigid process to keep up with such new developments but also that present institutional arrangements structurally are not adept to progressively apply the law through evolutive interpretation. As Weeramantry noted several decades ago, ‘aggressively burgeoning’ technological developments demand ‘constant surveillance’ to properly uphold human rights.⁷⁸⁷ A dialogical method provides the means to surveil burgeoning technological developments which, as highlighted in the introductory part of the thesis, are far more sophisticated now than were when Weeramantry made that observation.

The international law of privacy, as shown in chapters 1 and 2, is ill-equipped to match this novelty of the digital space. The present institutional machinery for the international protection of privacy is basically the treaty body system primarily involving the HR Committee, the UPR mechanism and the SRP. But, these bodies wield weaker institutional powers, operate on a part-time basis and suffer from compliance deficit. Worse, no dedicated institutional machinery exists at all at the UN data privacy framework, as considered in chapter 2, except for the part-time expert committees under relevant UNESCO instruments. This institutional lacuna is best illustrated by the dearth of privacy jurisprudence at the international level that would have developed existing norms in the new realities of the digital age.

As shall be explored in the next section, a privacy forum would equip current international law of privacy with a way that would considerably surveil continuous changes in the privacy landscape. Regular conversations among States, civil society groups and Internet corporations at the forum on current and emerging privacy issues would complement, and keep alive, the quasi-adjudicatory role of the HR Committee. In that way, a dialogical approach that is adaptive to changing circumstances would make international law flexible enough in the digital age. The argument in this chapter, then, is that a multi-stakeholder forum would offer a way in which international law can keep up with continuous developments in the global privacy landscape.

But the value of sustained conversation on digital privacy issues can also extend to regional and national courts. As much the regional courts like ECtHR have a progressive privacy jurisprudence, enforcement of their judgments is not all rosy. Structural problems such as case backlog further punctuates the relative successes of

⁷⁸⁷ See Weeramantry, above n 283, 42.

the Strasbourg court.⁷⁸⁸ When one considers the rapid pace in which technologies as well as attendant State and corporate practices change, the inherently time-consuming and bureaucratic nature of court process is a disadvantage. At times, judicial process is outpaced by the legislative process by which laws are being litigated in court are soon replaced with even more draconian rules.⁷⁸⁹

The degree to which courts are accessible to ordinary individuals is also questionable as most legal actions are brought by civil society groups. Issues of judicial independence as well as resource constraints reduce the capacity of national courts in many jurisdictions. This is in addition to the fundamental question of jurisdiction over transnational privacy matters. The extent to which adjudication is effective in practically enhancing privacy protection is also circumscribed. State and corporate practices that erode privacy rights do not always discontinue despite many several legal actions in domestic and regional courts.⁷⁹⁰

But at a more fundamental level, adjudication, in the strict sense of the terms, not only is ineffective but is inexistent in the international law of privacy. A dialogical approach then appears to be an indispensable additional tool in the repertoire of privacy right implementation.

III WAYS OF CONVERSATION: THE CASE FOR A MULTI-STAKEHOLDER PRIVACY FORUM

What follows considers the scope and nature of the proposed dialogical approach to digital privacy. It considers foundations of introducing a multi-stakeholder privacy forum. It then discusses two key functions of the forum as well as its interplay with existing institutional arrangements. Further highlighted are limits of ‘multi-stakeholderism’ that must be considered in installing a multi-stakeholder forum to ensure an inclusive and participatory process.

A Foundations of the Forum

The idea of introducing a multi-stakeholder privacy forum is based on three major premises. First, the notion of multi-stakeholderism enriches multilateral processes of the UN system. As the discussion shall show, the international legal order has recently recognized this virtue of multi-level approach to international regulation.

⁷⁸⁸ A latest privacy decision of the ECtHR in the case of *Big Brother Watch et al v UK* came almost after five years, which might even be considered quicker than other cases, perhaps, due to the fervour of the Snowden debacle. Id, above n 655.

⁷⁸⁹ A good example here is the replacement of a UK surveillance legislation litigated in the *Big Brother Watch* case before the case was decided. Id, above n 655.

⁷⁹⁰ See, e.g., ‘A Concerning State of Play for the Right to Privacy in Europe: National Data Retention Laws Since CJEU’s Tele-2/Watson Judgment’ (Privacy International, September 2017) [reporting that some European States non-compliance with decision of CJEU in relation to data retention].

Second, a multi-stakeholder approach is an effective way of rebuilding the model of ‘cooperative dialogue’ that forms a central part of the UN treaty body system. Third, because adjudicative means of upholding the right to privacy is moot, dialogue is the reasonable step to encourage compliance both by State and non-State actors. These three underlying rationales of the forum help explain why a privacy forum is a realistic approach towards lessening institutional gaps in international privacy law.

1 Enriching Multilateralism with Multi-stakeholderism

Installing a multi-stakeholder body would be in line with the increasing appeal for a multi-stakeholder approach at the UN and its various bodies, particularly in the human rights domain. This makes the proposal of a privacy multi-stakeholder body a rational exercise. The UN has beckoned multi-stakeholderism in international relations long before the post-Snowden UN Privacy Resolutions which, as noted earlier, endorse multi-stakeholder dialogues. One early instance has been at the WSIS in 2005 where the role of non-State actors in Internet governance, alongside States, was recognized.⁷⁹¹

But one of the earliest attempts to embrace non-State actors in the treaty body system was during the reform launched by former High Commissioner Pillay. In justifying the importance of multi-stakeholderism, Pillay argued that inter-governmental processes of the UN can embrace a multi-stakeholder participation in strengthening the treaty body system.⁷⁹² Unlike previous reform efforts, her reform initiative drew a great deal from the input of various stakeholders including States, civil society and national human rights organizations through a largely transparent, bottom-up, and participatory process.⁷⁹³ This pursuit of a multi-stakeholder approach was premised on the pragmatic assumption that the operation of treaty bodies mostly relied on the activities of these various actors, and hence that reform ideas must flow from them as well.⁷⁹⁴

Beyond reform efforts, multi-stakeholderism is increasingly becoming a new avenue of international lawmaking, perhaps an informal one. Recent studies have found that an ‘informal international law making’, that embraces new actors, follows new processes and produces new types of laws, has emerged.⁷⁹⁵ This alternative route of international lawmaking relies on transnational networks that have expert

⁷⁹¹ The Tunis Agenda, above n 314, [34]. The role of non-State actors in the promotion and protection of human rights has also been clearly recognized in the creation of the HR Council and its mechanisms mainly the UPR. See Res 60/251, above n 254, [5(h)] cum HRC Res 5/1, above 236, [3(m)].

⁷⁹² Navanethem Pillay, ‘Strengthening the United Nations Human Rights Treaty Body System: A Report by the United Nations High Commissioner for Human Rights’ (June 2012) 11.

⁷⁹³ See Suzanne Egan, ‘Strengthening the United Nations Human Rights Treaty Body System’ (2013) 13 *Human Rights Law Review* 209, 213-214.

⁷⁹⁴ *Ibid*, 214.

⁷⁹⁵ See generally Pauwelyn et al, above n 703; see also Joost Pauwelyn et al (eds), *Informal International Lawmaking* (Oxford University Press, 2012).

knowledge on specific issues, adopts an inclusive consensus-based multi-stakeholder process and the outcome of which are flexible instruments. The merit of this process lies primarily in addressing the legitimacy deficit of traditional international law by following inclusive and consensus-based approach – also referred to as ‘thick consensus’ – of lawmaking, as opposed to ‘thin consensus’ that is based solely on State consent.⁷⁹⁶

That the process embraces stakeholders with expertise in particular issues further means that outcomes of these process are normatively superior and hence likely to achieve desirable goals in practice. Examples of international law-making where multi-stakeholder participation played a key role include the drafting of the Disability Rights Convention and the Ruggie Principles.⁷⁹⁷ With such increasing appeal to multi-stakeholderism, the idea of installing the privacy forum is likely to materialize if taken seriously.

2 Rebuilding Cooperative Dialogue

The second premise is that constructive dialogue, as opposed to litigation, and persuasion, as opposed to confrontation, are practical ways of enhancing the protection of human rights. This is mainly because radical improvement in the state of human rights protection is unlikely to be achieved with the current weak structure of the institutional machinery. As much the prospects of a world human rights court are infeasible and undesirable, frequent treaty body reform efforts are also unlikely to bring the desirable level of effectiveness in the human rights system. Backlog of individual communications and overdue State reports, for instance, at the HR Committee, added to the prevalent compliance problem,⁷⁹⁸ attest to the fact that this route towards enhancing the protection of human rights is structurally inadequate. This calls for an additional mechanism that revitalizes and entrenches the cooperative dialogue practiced, to some degree, in the UN treaty body system and the UPR mechanism.

One such possible way is by investing more on fostering multi-stakeholder dialogue. Multi-stakeholder dialogue would be instrumental in raising the awareness of and persuading actors, particularly States towards the importance and strategies of strengthening human rights protection. As Alston notes, the best method in the international human rights enterprise is persuasion and building confidence in the system.⁷⁹⁹ The benefit of a multi-level dialogue is that it would bring stakeholders

⁷⁹⁶ Ibid, 740-42.

⁷⁹⁷ See, e.g., Grainne de Burca, ‘Human Rights Experimentalism’ (2017) 111 *American Journal of International Law* 277, 283.

⁷⁹⁸ See *Annual Report of the Human Rights Committee to the General Assembly*, GAOR, 72nd sess, UN Doc A/72/40 (March 2017) [39] (complaining that many States parties have failed to implement the views adopted under the Optional Protocol).

⁷⁹⁹ Philip Alston, ‘The Populist Challenge to Human Rights’ (2017) 9 *Journal of Human Rights Practice* 1, 3.

from all levels and create transnational networks of dialogue and cooperation. This, as Charlesworth writes, would contribute towards improving the protection of human rights by creating a 'regulatory web of influence' that combines the efforts of various actors, including those at the grass-root level.⁸⁰⁰ Such transnational network wield a considerable 'soft powers' which, by filling the void in hard power, may be marshalled towards incrementally solving specific cross-border challenges.⁸⁰¹

A network of governance that is built among human rights groups at the local level would lead to an improvement in the level of human rights protection. Repeated interactions of States with transnational networks and other actors at the local level has the capacity to gradually 'socialize' States to accept human rights standards.⁸⁰² This iterative process would create a pattern of State behaviour that would over time find translation and internationalization in domestic law and practice.⁸⁰³ The same observation applies to the private sector where interaction would facilitate understanding and consensus. In practice, such interaction between human rights communities and the technology sector will, for example, allow human rights considerations to be taken in designing new technologies.⁸⁰⁴ In that sense, the privacy forum would be a suitable platform to bring around the table relevant stakeholders and foster dialogue on privacy issues of mutual concern.

3 'Encouragement of Human Rights'

As a project, the protection of international human rights is a gradual and slow process – and in that sense, it involves ongoing debates and struggle.⁸⁰⁵ As much as there are adherents to principles of human rights protection, there has always been resistance to it. And what characterizes the project is that it is an ongoing struggle against such resistance. This dictates an approach that is aligned to the reality of the human rights project that espouses engaging in continued dialogue among various stakeholders. Such an approach would involve ways of fostering mutual understanding and sustained dialogue. This partly captures what Higgins terms the notion of 'encouragement of human rights' which involves 'invocation,

⁸⁰⁰ Hilary Charlesworth, 'A Regulatory Perspective on the International Human Rights System' in Peter Drhaos (ed), *Regulatory Theory: Foundations and Applications* (ANU Press, 2017) 360.

⁸⁰¹ See Goldin, above n, 112.

⁸⁰² See Margaret Keck and Kathryn Sikkink, *Activists Beyond Borders: Advocacy Networks in International Politics* (Cornell University Press, 1998) 16, 60, 214; see also Thomas Risse and Kathryn Sikkink, 'The Socialization of International Human Rights Norms in Domestic Practices: Introduction' in Thomas Risse et al(eds), *The Power of Human Rights: International Norms and Domestic Change* (Cambridge University Press, 1999) 1-39.

⁸⁰³ See Harold Koh, 'The 1994 Roscoe Pound Lecture: Transnational Legal Process' (1996) 75 *Nebraska Law Review* 181, 203-205.

⁸⁰⁴ See Mathias Risse, 'Human Rights and Artificial Intelligence: An Urgently Needed Agenda' (2019) *Human Rights Quarterly* 1, 11.

⁸⁰⁵ See Christian Tomuschat, *Human Rights: Between Idealism and Realism* (Oxford University Press, 3rd ed, 2014) 431.

interpretation and exhortation’ of human rights to cajole and nudge States and the private sector towards human rights compliance.⁸⁰⁶ Resort, then, can be made to political pressure on States (and possibly corporations) that fail to engage or resist dialogue. Indeed, even in regional human rights systems where binding judicial decisions are made, the level of effectiveness is relative, and has a political element.

Political pressure is the key tool of enforcing binding decisions of regional courts such as the ECtHR.⁸⁰⁷ Decisions of the Strasbourg Court are overseen by the Committee of Ministers, which is a political body, and hence its enforcement involves political considerations.⁸⁰⁸ And more often, political pressure falls short in yielding compliance. Russia, for instance, has declined to implement over 250 decisions of the ECtHR that found violations of human rights in Chechenia and the Northern Caucasus.⁸⁰⁹ Russia has also recently questioned the authority of the Court’s judgments rendered by judges in the selection of whom it did not participate at CoE’s Parliamentary Assembly.⁸¹⁰ This adds to the increasing signs of retreat from the Court by a number of other CoE member States. But importantly, this lends weight to the argument that, instead of traditional enforcement through sanctions, dialogical mechanisms are more likely to be relatively effective. The proposed forum would be instrumental in facilitating such dialogue on the right to (digital) privacy.

In summary, securing human rights, including the right to privacy, must rely more on dialogue than litigation to bear fruit. Sanction as a primary tool of ensuring human rights is not always successful. More so in the international legal order where no real authority of imposing sanctions exists in the first place. Instead of pushing for drastic reform to achieve such authority, entrenching dialogical approaches is needed. Creation of the privacy forum is, therefore, the way forward in that front.

B Roles of the Forum

If the underlying premises of the multi-stakeholder privacy forum are persuasive, the next step is considering the specific functions of the forum. The privacy Forum must assume the following two set of roles. The primary role of the forum is to facilitate consensus and cooperation among relevant actors that play key roles in the protection (and violation) of the right to privacy in the digital space. Exchanging best

⁸⁰⁶ See Rosalyn Higgins, *Themes and Theories: Selected Essays, Speeches and Writings in International Law* (Oxford University Press, Vol. I, 2009) 498-499.

⁸⁰⁷ See Eva Brems, ‘Introduction: Rewriting Decisions from a Perspective of Human Rights Integration’ in Eva Brems and Ellen Desmet (eds), *Integrating Human Rights in Practice: Rewriting Human Rights Decisions* (Edward Elgar, 2017)5.

⁸⁰⁸ See Alston, above n 783, 204.

⁸⁰⁹ See Philip Leach, ‘The Continuing Utility of International Human Rights Mechanisms?’ on *EJIL: Talk!* (1 November 2017) <<http://bit.ly/2z9IEeu>>

⁸¹⁰ See Andrew Drzemczewski and Kanstantsin Dzehtsiarou, ‘Painful Relations Between the Council of Europe and Russia’ on *EJIL: Talk!* (28 September 2018) <<https://bit.ly/2RTBfoD>>

practices among these stakeholders on the protection of digital privacy is the other possible role for the forum.

These roles of the forum are consistent with the role of existing multi-stakeholder forums in the UN human rights system. Among existing multi-stakeholder UN forums, the 'Forum on Minority Issues' assumes related roles. The forum was established in 2007 by the HR Council to serve as a platform for dialogue among relevant stakeholders including States, UN Specialized agencies and civil societies.⁸¹¹ Its stated aim is to be a platform for promoting dialogue and cooperation on issues pertaining to minority rights and to exchange best practices, challenges, opportunities and initiatives for the further implementation of the Minority Rights Declaration.⁸¹² Another example is the 'Forum on Business and Human Rights'. This forum is created to discuss trends and challenges in the implementation of the Ruggie Principles, and to further cooperation among stakeholders.⁸¹³ As such, both forums do not have any normative role and hence have no decision-making mandate. In line with these precedents, what follows describes the two roles of the privacy forum:

Facilitating consensus and cooperation: the primary mission of the forum should be encouraging the emergence of broader understanding on core digital privacy issues among States, civil society groups, technology companies and other potential stakeholders. Guided by the key digital privacy standards enunciated in the soft law considered in chapter 5, the forum would be a useful platform to develop consensus gradually. Such dialogue would especially be useful in leading to compromises on issues where there exists competing, and sometimes, conflicting interests.

Unlike litigation, dialogue is more likely to be useful in reconciling conflicting interests such as fundamental rights, national security and commercial interests. By bringing together actors with diverging interests and ideological positions around the table, mutual understanding can be established towards balancing these competing interests. Dialogue might not result in a radical and immediate change in ideological stance or business models of those actors. But the lack of any other better alternative such as robust adjudicative system at the international level makes it the best possible alternative.

Establishing broader understanding and consensus will have practical implications. Considering the transnational element in international privacy protection as well as

⁸¹¹ See *Forum on Minority Issues*, HRC Res 6/15 (28 September 2007). Cf Mandate indefinitely renewed by *Forum on Minority Issues*, HRC Res 19/23 (10 April 2012).

⁸¹² *Ibid*, [5].

⁸¹³ See *Human Rights and Transnational Corporations and Other Business Enterprises*, HRC Res 14/4 (6 July 2011) [12-18]. As discussed in chapter 1, the Ruggie Principles (and the Working Group that oversees the Principles) has not so far addressed the right to privacy — and perhaps would not in the long-run — due to the narrowly defined remit of the framework. This would not, therefore, make the proposed privacy forum a redundancy.

the role of the private actors, the active involvement of various stakeholders is key. As highlighted in the introductory part of the thesis, a key feature of the ‘privacy problem’ in the digital age is the increasing prominence of technology companies. Transnational corporations hold a unique position in the digital place that affects the enjoyment of human rights, including the right to privacy. Their central role in the governance, operation and provision of the Internet infrastructure and services thus reinforces the importance of the dialogue.

Worth emphasising here is the complex and dynamic nature of human rights protection in the digital age, which makes the case for a multi-stakeholder approach even more compelling. It requires the knowledge, experience and control of both State and non-State actors. The technical aspects of the subject make the role of the private sector as much important as that of States. States remain to be pivotal actors of international co-operation. But other actors too play an increasingly crucial role in supplementing, assisting, correcting and continuously challenging rules of international regulation.⁸¹⁴ This is particularly the case for (digital) privacy given the role of technology both in its protection and invasion.

Exchanging best practices: beyond reconciling competing interests, dialogue at the forum could be a useful platform for sharing best practices. Results of the dialogue among participants of the forum compiled through reports could provide useful insights to human rights bodies at many levels. From the HR Committee, the UPR mechanism, regional human rights courts to domestic courts and regulators, the recommendations of the forum would be useful. What makes this particularly useful is that privacy issues in the digital age are not only complex but also highly dynamic.

It is obviously a challenging undertaking for part-time bodies like the HR Committee to keep fully abreast with new developments in the digital arena. Add to that is the frequent turnover of Committee members,⁸¹⁵ and the fact that the Committee oversees an omnibus treaty containing a diverse array of rights, as opposed to a specialized treaty on a specific human right.⁸¹⁶ This is in a stark contrast to regional courts such as ECtHR, which at least does not operate on a part-time basis. And of course, the ECtHR is supported by a dedicated research division and judicial assistants as well as the Court’s Registry when, for instance, a need for

⁸¹⁴ See Joost Paulwelyn et al, ‘Informal International Lawmaking: An Assessment and Template to Keep It Both Effective and Accountable’ in Paulwelyn et al (eds), above 795, 504.

⁸¹⁵ See Anja Seibert-Fohr, ‘The Human Rights Committee’ in Oberleitner (ed), above n 611, 122 (noting that half of the Committee’s members are elected biannually and one third of members are replaced every two years).

⁸¹⁶ Treaty bodies, including the HR Committee, now face more challenges due to impending budgetary cuts. See ‘UN Budget Shortfalls Seriously Undermine the Work of the Human Rights Treaty Bodies’ (OHCHR Press Release, 17 May 2019).

research of international best practices arises.⁸¹⁷ The establishment of the forum, by providing timely expert advice, would assist in mitigating this inherent limitation of the treaty body system. Beyond treaty bodies, the privacy forum would also provide thematic contributions to the SRP.

Soft oversight: perhaps an incidental role for the forum is to serve as a platform to deliberate on and highlight the formal determinations on the right to privacy of the various UN bodies. This would be useful to consider whether and the extent to which they have been put into effect by relevant UN bodies, States and non-State actors. In a way, this would also complement the work of the Rapporteurs on Follow-up of Views and Concluding Observations of the HR Committee. These rapporteurs are selected among members of the Committee,⁸¹⁸ but the enormity of the task – due to years of backlog, added to the part-time nature of their role – makes the follow-up less effective.

In complementing the work of the rapporteurs, the forum thus would be a softer mechanism of oversight. In putting the work of the Committee in the spotlight, the ‘visibility’ concerns of the UN treaty body system would be mitigated, which is sometimes raised as one reason for its ineffectiveness.⁸¹⁹ As the work of the HR Committee is likely to feature in the agenda of the privacy forum, visibility of the Committee would accordingly increase. Visibility, in turn, would increase the profile of the Committee, stimulate its jurisprudence and ultimately contribute towards better compliance.

In sum, the forum would be a platform for all actors to deliberate on and narrow divergences on current and emerging issues of securing digital privacy.

C Procedural Considerations

In realizing the proposed forum, two procedural matters must be addressed. The first concerns the organizational structure of the body. Membership and participation procedures of the UN Forums on Minority Issues and Business and Human Rights can readily be adapted to the proposed privacy forum. There are two alternatives to creating the advisory body. One is that the proposed soft law on the right to privacy, explored in chapter 5, could create this forum, i.e. through a Resolution of the UNGA. The other alternative – and perhaps in line with the tradition – is that it could be established by a Resolution of the HR Council, as in the case of the Forums on Minority Issues and Business and Human Rights. In the

⁸¹⁷ See Angelika Nußberger, ‘The ECtHR’s Use of Decisions of International Courts and Quasi-Judicial Bodies’ in Amrei Muller and Hege Kjos (eds), *Judicial Dialogue and Human Rights* (Cambridge University Press, 2017) 420.

⁸¹⁸ See ‘Rules of Procedure of the Human Rights Committee’ (9 January 2019) 106.

⁸¹⁹ The former UN Secretary-General Annan had, for instance, noted that the UN treaty body system remains little known. See *In Larger Freedom: Towards Development, Security and Human Rights for All*, UN Doc A/59/2005 (21 March 2005) [147].

interest of being holistic, the former is perhaps more appropriate, more so to lift the authority of the forum with the imprimatur of the UNGA.

The Forum should meet at least once in a year for two days. A two-days meeting annually can be considered too short. Indeed, this point has been raised in relation to the Forum on Minority Issues.⁸²⁰ But given the resource strain that creation of a new forum may have as well as the impending budgetary cutbacks at the UN human rights system noted above, a two days meeting seems sensible. But one must not also lose sight of the fact that unlike the minority rights and/or the business and human rights forums, deliberations of the privacy forum would focus on a single right and hence would not be as prone to problems of time shortage.

Attendance at the privacy forum must be open to all stakeholders. But given the nature of the topic in question, all relevant UN bodies in the area of privacy should be made part of the forum. UN treaty bodies, particularly the HR Committee, should be represented in the forum by one or more of its members so as to draw relevant insights from discussions at the forum and to bring to more light the jurisprudence of the Committee. Engaging the Committee would, for instance, be one way to inculcate the soft law into the jurisprudence of the Committee. Fox reports that participation of treaty bodies in the Forum on Minority Issues has considerably increased reference to the UN Declaration on Minority Rights in their jurisprudence.⁸²¹ Similarly, the soft law on the right to privacy, explored in chapter 5, can shape the jurisprudence of the HR Committee through dialogue at the privacy forum.

As in the case of the Forum on Minority Issues,⁸²² the SRP should 'guide' the privacy forum and transmit its recommendations to the HR Council and perhaps the UNGA through the formal reporting procedure. Assigning a role for the SRP at the forum is plausible on many levels. One is that, as noted above, there is a precedent by which Special Rapporteurs are assigned to steer the dialogue in several forums established by the UN. But more crucially, the SRP is already 'encouraged' by UNGA Privacy Resolutions to contribute towards informal multi-stakeholder dialogues on the right to privacy.⁸²³ This would be also in line with the mandate's recognition of the fact that 'mutual cooperation and dialogue' play an important role in fostering global privacy protection.⁸²⁴

⁸²⁰ See Graham Fox, 'The United Nations Forum on Minority Issues and Its Role in Promoting the UN Declaration on the Rights of Persons Belonging to National or Ethnic, Religious and Linguistic Minorities' in Ugo Caruso and Rainer Hofmann (eds), *The United Nations Declaration on Minorities: An Academic Account on the Occasion of Its 20th Anniversary (1992-2012)* (Brill, 2015) 90, 94.

⁸²¹ Ibid, 93.

⁸²² See Res 19/23, above n 811, [10].

⁸²³ See, e.g., Res 71/199, above n 526, [8].

⁸²⁴ Report of Cannataci, above 454, [46(g)].

With that said, it is important to ensure that thematic priorities of the Special Rapporteur do not cloud, as Fox counsels in the context of the Forum on Minority Issues, the agenda items of the privacy forum.⁸²⁵ The role of the SRP must, thus, be restricted to channelling the discussion, not setting the agenda of the privacy forum. This would avoid the effect of changing thematic priorities of different mandate holders on the work of the privacy forum. And indeed, it is naturally aligned with the multi-stakeholder feature of the forum where agenda items are set collectively, in a spirit of consensus.

The Special Rapporteur has recently launched an initiative called 'International Intelligence Oversight Forum'. Created in 2016, this Forum is an annual event held for the purpose of 'collective identification of challenges to privacy and freedom of expression in the gathering of intelligence as well as best practices which could provide better safeguards and remedies'.⁸²⁶ But effectiveness of the intelligence forum may be affected by its constricted remit as well as lack of inclusiveness demonstrated so far. The thematic focus is on surveillance, and as such, leaves out other aspects of privacy in the digital age such as data protection. But more importantly, the level of participation in the first two events suggests lack of inclusiveness. In the first event in 2016, for example, only 20 countries took part in the forum and only 'some members of civil society'.⁸²⁷ No participation from the privacy sector, particularly the rather important stakeholders – i.e., Internet corporations – is reported. The lack of inclusive participation of relevant stakeholders reduce the capacity, and ultimately, legitimacy of the SRP's unilateral initiative.⁸²⁸ The privacy forum proposed in this chapter not only attends to this shortcoming by envisaging a multi-stakeholder forum where all voices are heard but one that brings a level of legitimacy and authority to the forum through clear legal basis and mission.

A question might arise as to why there should be a multi-stakeholder forum for privacy but not for other rights the protection of which faces no less significant challenges in the digital age. One such right is the right to freedom of expression. There is neither conceptual nor practical barrier for not extending the remit of the proposed forum to cover other digital rights, including freedom of expression. Indeed, there is already a parallel discourse, as highlighted in chapter 4, on freedom of expression on the Internet running at the HR Council since 2014. But it is vital to note that free speech jurisprudence at the UN is much advanced in

⁸²⁵ Fox, above n 820, 90, 105.

⁸²⁶ See *Report of the Special Rapporteur on the Right to Privacy, Joseph Cannataci*, UN Doc A/71/368 (30 August 2016) [12].

⁸²⁷ See *Report of Cannataci*, above n 158, [3]. Participation of States rose only to 30 in the 2017 event. See *Report of Cannataci*, above n 602, [12].

⁸²⁸ Moreover, the third event held in November 2018 was said to be a closed-door event. See details here: <<https://bit.ly/2CEMuLG>>

comparison with privacy. The HR Committee has, for instance, adopted an elaborate GC and this has been further advanced by the jurisprudentially influential work of successive Special Rapporteurs on Freedom of Expression. Otherwise, broadening the scope of human rights covered in the forum would not be problematic; only a privacy forum is argued here owing to the scope of the thesis.

Perhaps another question is one of desirability: what is the added value of installing a new forum while there is, for example, the IGF that could — and in fact does — consider privacy issues? Human Rights are, of course, important themes in Internet governance platforms such the IGF. But, as its name clearly indicates the IGF is meant to deal with a number of non-human rights related themes. The kind of vexing and dynamic privacy issues could not possibly be examined in an annual four-day meetings with the required level of depth and rigor. That the notion of ‘Internet governance’ embraces a broad range of topics means it opens up extremely broad and unstructured discussions.⁸²⁹ This is where the added value of the proposed privacy forum becomes evident as it offers the platform where more but focused discourse among stakeholders would occur.

D The Forum and Limits of Multistakeholderism

To a large extent, a multi-stakeholder approach to governance is new to international law. As noted above ‘informal international law’ is largely a new phenomenon.⁸³⁰ But the experiment in the past decade or so in the broader field of Internet governance, even where it is regarded as an ‘inchoate institution’,⁸³¹ reveals that risks are present. The relevant question here, then, is whether these concerns associated with multi-stakeholderism would apply to the proposed privacy forum. As shall be shown below, these concerns do not necessarily extend to the privacy forum due to its organizational mission and constitution. Like the forums on minority rights and on business and human rights, the proposed privacy forum would not have normative or decision-making role. But there are still some lessons to be drawn so as to pre-emptively lessen drawbacks of multi-stakeholderism in the broader Internet governance policy discourse.

Three concerns are often raised in relation to multi-stakeholder platforms. A primary concern is the lack of proportionate representation, particularly of actors from the

⁸²⁹ See Amanda Hubbard and Lee Bygrave, ‘Internet Governance Goes Global’ in Lee Bygrave and Jon Bing, *Internet Governance: Infrastructure and Institutions* (Oxford University Press, 2009) 232-234.

⁸³⁰ But see Christine Kaufmann, ‘Multi-stakeholder Participation in Cyberspace’ (2016) 26 *Swiss Review of International and European Law* 217, 218-221 (tracing multi-stakeholder trends in intergovernmental bodies in the 19th century).

⁸³¹ See Mary Raymond and Laura DeNardis, ‘Multistakeholderism: Anatomy of An Inchoate Global Institution’ (2015) 7 *International Theory* 572, 573.

global south including States and non-State Actors.⁸³² ICANN, a key player in the Internet's addressing system, is one organization that practices a multi-stakeholder approach to governance but often comes under criticism for inequitable representation. Part of the criticism is that its stakeholder groups are significantly dominated by States, members of civil society and the private sector from western countries, particularly the US. This sometimes gives the impression that multi-stakeholderism is used as a 'cover' for American 'techno-imperialism',⁸³³ and being used to sustain vested interests.⁸³⁴ Related to the problem of inclusion are language barriers and lack of technical expertise. The latter is particularly raised in connection with Internet technical bodies like the IETF.⁸³⁵ Other barriers include funding constraints and organizational capacity.⁸³⁶

Lack of representation is inevitable when it comes to the privacy forum. The all too known digital divide will come as a barrier to equitable representation from developing countries. Perhaps, these countries may be keen to invest towards bridging the divide than participating in the forum. But the fact that the forum is envisioned as a UN body, just like other forums currently running, means at least participation from State representatives would be broader. Resource constraints would rather be a hurdle to civil society groups from those countries. Unless some form of support towards correcting the imbalance is found, voices of non-State actors from the global south will be limited.⁸³⁷ In addressing this concern, the voluntary fund created by the OHCHR to increase participation from the developing part of the world in the Forum on Minority Issues could simply be emulated for the Privacy Forum.⁸³⁸ In that way, inclusivity of the privacy forum can be lessened over time.

With lack of inclusive participation comes a legitimacy problem. Actors not involved in the making of decisions at multi-stakeholder forum may resist its legitimacy and decisions.⁸³⁹ Legitimacy concerns then are more pronounced in multi-stakeholder fora like ICANN or IETF where consequential decisions – be it of policy or technical matters – are taken. Other multi-stakeholder forums like the IGF where no such decisions are made thus are mostly exempt from legitimacy deficit. Because the

⁸³² See Avri Doria, 'Use [and Abuse] of Multistakeholderism in the Internet' in Roxana Radu et al (eds), *The Evolution of Global Internet Governance* (Springer, 2013) 123.

⁸³³ See Richard Hill, 'Internet Governance: The Last Gasp of Colonialism, or Imperialism by other Means?' in Radu et al (eds), above n 832, 83, 85, 90-92.

⁸³⁴ See Raymond and DeNardis, above n 831, 611.

⁸³⁵ Ibid, 597.

⁸³⁶ See Hofmann, above n 518, 33.

⁸³⁷ See Besson and Marti, above n 516, 538 (advocating 'affirmative action' like quotas to civil society groups representing weaker or invisible groups).

⁸³⁸ See Res 19/23, above n 811, [3].

⁸³⁹ See Kaufmann, above n 830, 218, 224-225.

privacy forum is not a decision-making body, legitimacy would not, as such, be a concern.

But it is possible that outcomes the privacy forum may have a 'decisional potential', albeit indirectly. One such possibility is that outcomes of the dialogue at the privacy forum may earn 'legal effects' in practice. The HR Committee may, for instance, apply the ICCPR's privacy provision based on a view that prevailed at the forum in a case where States (and its citizens or civil society) did not take part. This would ultimately generate a legitimacy concern. But the best way to prevent such a concern is to work towards gradually increasing participation at the forum, as alluded to above.

The third concern relates to transparency and accountability in decision making processes. Once decisions are taken in a multi-stakeholder forum, there are limited avenues to challenge decisions and even to seek remedies.⁸⁴⁰ An aspect of this concern is that there is little room for periodic monitoring and review of decisions and policies. That the privacy forum is open to anyone and that outcome of its deliberations would be released in the form of regular reports add to its transparency. But accountability issues are unlikely to emerge because, again, the forum would not make strictly binding decisions.

In summary, most concerns associated with a multi-stakeholder approach to Internet governance do not fully extend to the privacy forum. However, where there are risks to inclusivity, transparency and accountability, a sensible way to mitigate such problems is through long-term initiatives of broadening participation from relevant actors.

IV CONCLUSION

This chapter explored virtues of a dialogical approach as a pragmatic way of lessening the institutional void in existing international law of privacy. It argued that installing a multi-stakeholder privacy forum would considerably address institutional aspects of international law's privacy problem. Drawing upon precedents in the UN human rights system and support for a multi-stakeholder approach in the ongoing UN privacy discourse, the chapter has outlined rationales and functions of the proposed forum.

As shown in this chapter, such a forum is especially suited to the international protection of digital privacy for two reasons. One is that it is a more practical way of addressing institutional problem present in international law. Unlike hitherto radical reform ideas proposed by scholars, installing a privacy forum would not require reinventing the wheel. That makes it politically as well as economically feasible. Secondly, as a dialogical mechanism, the privacy forum is more responsive to the

⁸⁴⁰ See Doria, above n 832, 129-130.

realities of the digital age where privacy threats are dynamic, complex and involve multiple actors. Orthodox means of human rights adjudication such as judicial process is not suited to attend to these peculiarities of the 'privacy problem'.

A prime role for the forum would, then, be to serve as a platform where all relevant stakeholders on the right to privacy would deliberate on current and emerging issues regarding the right to privacy and share best practices. A multi-stakeholder privacy forum would be a supplement to the existing institutional machinery by both providing expertise on the right to privacy and facilitating creation of a consensus and facilitating cooperation among stakeholders. In steering the dialogue at the forum, the soft law argued for in chapter 5 would provide a roadmap.

CONCLUSION, FINDINGS AND PROSPECTS

The Internet needs new rules ...

Zuckerberg, *The Washington Post* (online), 30 March 2019

[The UN system is able] to survive, grow and adapt but it achieves progress only through historical cycles of modest adaptation and change.

Weiss and Daws (eds), *The Oxford Handbook on the United Nations* (OUP, 2018) 19

I THE 'PRIVACY PROBLEM' AND THE ROLE OF INTERNATIONAL LAW

A In Search for a Role

This thesis examined the question of how best international law should respond to the challenges of securing the right to the privacy in digital age. It focused especially on two recent international privacy initiatives: IBRs and the ongoing UN discourse on the 'right to privacy in the digital age'. It investigated the role of such initiatives in reimagining current international law of privacy to accommodating the challenges of upholding digital privacy. In doing this, the thesis makes three contributions to the literature. First, it provides a sound foundation for practical reform by exploring the extent to which current international law of privacy is well-equipped in the digital age. The proliferation of reform initiatives is not matched by exploration of what really lacked in existing law. The thesis has demonstrated where, how and why current international law of privacy falters in securing digital privacy. Thus, it fills the void in the international law scholarship, and to an extent, the IBRs literature.

Second, the thesis makes an original contribution by investigating the role of international privacy initiatives in helping realize the long-sought international privacy framework. More particularly, it examined the extent to which such initiatives reimagine current international law of privacy in the digital age. In did so by situating such rather diverse and sporadic initiatives in international law. It has demonstrated the various ways in which the IBRs Project interacts with and shapes international privacy law. This lessens the gap in the international law scholarship as well as the IBRs literature.

Third, the thesis joins the debate on how international law should respond to the 'privacy problem'. In that sense, it contributes to the literature in showing a plausible way of reimagining international privacy law in the digital age. But going beyond the current debate, the thesis has built on the foundations of the existing legal

framework and progressive visions of global privacy initiatives in exploring the appropriateness of an international law response to the privacy problem. In addition, the thesis has adopted a holistic approach to privacy by combining the disparate regimes of international law – i.e. human rights law, data privacy law and IBRs – in considering the privacy problem. This builds the discursive bridge between the fragmented discourse on the right to privacy in the digital age by combining insights from the fields of data privacy law and IBRs to the broader international law discipline which, on its own, has rarely examined the question of how international law could, or should, respond to the ‘privacy problem’ in the digital age.

Related to the above is the thesis’s contribution to the privacy scholarship on the potential role of international law in upholding digital privacy. By and large, the (data) privacy literature has had a particular focus on the role, or the lack thereof, of national and regional law. In undertaking an international law examination of themes that cross-cut privacy and data protection law, the thesis introduces to the literature the role of international law in securing the right to privacy in the digital environment, alongside national and regional systems of protection. In a similar vein, the examination in the thesis shows that privacy and/ data protection in the ‘international’ context is not restricted to the privacy provisions of the UDHR and the ICCPR. Beyond these high-level principles, the international law of privacy – as considered in this thesis – consists of a broad range of norms and principles as well as sources.

B Looking Through the Lens of Global Emergent Law

The thesis was inspired by the proliferation of multi-level initiatives for a set of new or expanded human rights standards for the digital age. While such initiatives existed since the early days of the Internet, they have gained momentum in the wake of the Snowden revelations in mid-2013. Breaking away from its momentary tradition, the idea of a global privacy framework has since become more coherent and prominent in law and judicial making. Nothing better illustrates this point as the adoption of (or proposal for) IBRs legislation in several countries as well as the evolving UN privacy discourse. Nevertheless, the role of such privacy initiatives and their place in international law remain largely unexamined. With the recent prominence of such initiatives in lawmaking at various levels, there is a need for careful analysis. Even more so, given the urgent need for reform in international privacy law. This thesis represents an attempt in that direction, examining the role of global emergent norms in reimagining current international law of privacy. But a question might arise as to the rationale for choosing global privacy initiatives more generally and the two case studies in particular in this study.

At the most basic level, this case study approach offers a unique vantage point. As shown in this thesis, a common thread in global privacy initiatives is the emphasis

on the need for a new international privacy framework. Although not always overtly stated, such initiatives proceed from the premise that something is missing in the current framework that makes it unfit for the digital age. Zuckerberg's proclamation that the "Internet needs new rules", alluded to in the epigraph, is a good case in point. But this tendency to assume gap in existing law invites an examination of what really lack in the present legal framework. The role of emerging privacy initiatives in addressing gaps must thus be considered against the backdrop of current international law of privacy. Put differently, virtues of global privacy initiatives may not clearly be grasped unless the interplay with existing law is investigated.

As explored in chapters 3 and 4, IBRs and the ongoing UN privacy discourse imagine a relatively progressive vision for the right to privacy. Unlike high-level proposals of technology companies or academic commentaries, these initiatives provide normative contours of the right to privacy in the digital age. Moving beyond the rather vague and fragmented approach in present international law, these initiatives tend to reimagine the right to privacy in the light of new developments. IBRs, for instance, unpacks the right to privacy into a set of sub-rights while the UN Privacy discourse envisions (Internet) corporations as duty bearers. Using such progressive initiatives as case studies, thus, provides the angle from which international privacy law may be reimaged in the digital age.

At a practical level, the case study approach offers a fresh perspective on the way how to reimagine this area of law in the digital age. When considering the extent to which gaps in existing law may be filled with emergent norms, one gets a clearer picture of what approach is likely to be practical. If the gaps in existing law are clear – and the boundaries of emergent norms are evident, it is then possible to imagine a reform alternative that can lessen those gaps while drawing up on the progressive visions of emergent law. In that sense, the role of international law in securing the right to privacy can clearly be shown. This thesis, therefore, critically looked at the possibility of addressing the 'privacy problem' through the lens of two significant privacy initiatives.

II FINDINGS OF THE THESIS

Three key findings have emerged out of the thesis:

A International Law of Privacy and Its Shortcomings in the Digital Age

First, the thesis has found that current international law of privacy is ill-equipped to address the 'privacy problem' in the digital age. As demonstrated in chapter 1, the (international) human right to privacy framework is replete with legal and structural gaps. Not only are the scope and meaning of the right to privacy vaguely defined

but existing institutional arrangements are not best positioned to translate the vaguely-worded right to meet the new realities of the digital age. This has, in turn, resulted in a privacy jurisprudence that is thinner than its regional counterparts. The problem is more pronounced with respect to the UN data privacy framework which, as shown in chapter 2, is characterized by deep normative and institutional dispersion as well as comparatively outmoded data privacy norms. A characteristic feature of the UN data privacy framework is that it is largely a patchwork of data privacy norms scattered across a range of soft law instruments. With no dedicated institutional machinery, fragmentary UN data privacy norms are now superseded by modern data privacy rights, principles and norms elsewhere.

Putting this finding in a historical context, the thesis further located causes of international privacy law's weak structures in the drafting history of relevant instruments. As chapters 1 and 2 uncovered, Cold War politics that clouded the drafting, negotiation and adoption of relevant privacy instruments is largely responsible for the ambiguous formulation of privacy rights, principles and norms as well as the creations of a weaker implementation framework. More crucially, the thesis has traced marks of 'inattention' to the right to privacy – in contrast with other human rights – during the drafting of the UDHR and the ICCPR. Lesser attention meant ambiguous formulation of the right to privacy. That Article 17 of the ICCPR simply replicated UDHR's privacy provision meant that the mis-formulations not only remain unrectified but also are repeated in privacy provisions of the ICCPR and subsequent specialized human rights treaties. The thesis has similarly found traces of inattention during the protracted processes of installing the UN data privacy framework.

Regarding technology companies, the thesis has shown that current international law of privacy is yet to recognize and effectively constrain their unique role in the protection (and violation) of digital privacy. The current UN framework on 'business and human rights' has failed to put (Internet) corporations within its remit. While it theoretically applies to 'all' human rights, and regardless of the sector in which corporations operate, the evidence so far shows that only 'brick-and-mortar' corporations are still its sole focus. The thesis further demonstrated that (Internet) businesses are not within the sight of the ongoing treaty process that seeks to translate the Ruggie Principles into a binding treaty. And, the draft treaty maintains the same proviso in that it covers 'all' sectors as well as human rights, but nothing in the draft text seems to be geared towards corporations of 'cyberspace' and hence digital privacy.

By contrast, the role of (Internet) corporations is being addressed in the UN privacy discourse which, as considered in chapter 4, began around the same time as the treaty process. The absence of some symbiosis between the two processes may however ultimately affect prospects of a tangible global legislative response. More

critically, the UN privacy discourse has heralded a new front when envisioning corporate human rights obligation in a novel 'right-specific' fashion. This would invite challenging questions, for example: must the future of corporate human rights obligations in the digital context must be 'right-specific' – as opposed to the current 'generic' all-rights approach? What are the implications of the 'right-specific' approach to the current UN 'business and human rights' framework? What would it mean, in practice, if the Privacy Resolutions evolve into a treaty? Which corporations would be held to account, and how, under such treaty regime? Such questions are beyond the scope of the thesis but merit an in-depth research, both doctrinal and empirical.

B Global Privacy Initiatives and Their Limits

Second, the thesis has found that emerging privacy initiatives offer a progressive vision for digital privacy, but several shortcomings limit their legal significance. The role of these initiatives in reimagining international privacy law were examined based on a three-level framework of analysis: 'freestanding', 'contributory' and 'catalytic' roles. As shown in chapter 3, the IBRs Project envisions the right to privacy in an elaborate manner by which a 'subset of privacy rights' is often provided. This tendency to flesh out the content of the right to privacy clarifies the scope and meaning of the right based on its growing understandings in the digital age. To that extent, IBRs points towards a way in which normative obfuscations of the right in international law may be lessened. But, the 'freestanding' role of the IBRs Project is weakened by its fragmented and uncoordinated nature. That the IBRs Project is a constellation of multi-level, but momentary initiatives, means no freestanding legislative outcome, like an 'international IBRs', is likely. This leaves it only with a limited 'contributory role' of informing the substance of other practical initiatives. To some degree, signs of this role are visible; for example, in the content of the evolving UN Privacy Resolutions. But as shown in this thesis, the contributory role of IBRs has been negligible. What, then, remains of IBRs is the potential for a more focused global privacy reform initiative to draw from its progressive visions: a 'catalytic' role.

Like the IBRs Project, the UN Privacy discourse posits a progressive vision for the right to privacy with some modern privacy principles flagged in the Resolutions. More importantly, the role of Internet corporations in the protection of the right to privacy are, as shown in chapter 4, increasingly being foreshadowed in the latest Resolutions adopted as part of the discourse. But several factors limit the freestanding role of the discourse in reimagining existing international law of privacy. One relates to the normative composition of the Resolutions and the way in which the discourse is progressing. Privacy Resolutions adopted as part of this discourse exhibit ambivalence and lack of thematic focus. Themes currently in vogue

in international law discourse such as cybersecurity and cyber warfare risk side-tracking the rather progressive privacy norms flagged in the Resolutions.

Elements of the 'freedom of expression on the Internet' discourse at the HR Council are also increasing spilling over to the Privacy Resolutions. This suggests that the degree to which the Privacy Resolutions would address key privacy principles, including those concerning the human rights responsibilities of corporations as well as States, is (and will be) limited. Such loss of direction reduces prospects of the discourse in developing into a meaningful legislative response. The discourse's limited freestanding role further undercuts its contributory role. The restricted and fuzzy normative reach of the Privacy Resolutions reduce the possibility of gradual accretion of customary norms or shaping of lawmaking and case law at national and regional levels. This leaves it with a 'catalytic' role by which it may shape the normative and methodological directions of a more focused and practical reform.

Beyond its present predicaments, the future of the ongoing UN privacy discourse does not seem entirely clear. Almost five years since it began, there is no sign of culmination with the latest (and fourth!) UNGA Resolution urging the HR Council and the OHCHR to remain 'seized' of the matter. No effort that seeks to exploit the political capital of the discourse towards a more concrete international law measure appears to be forthcoming. One of the discourse's outcomes, the mandate of SRP, is yet to orient its work with the discourse. The mandate's surveillance treaty initiative and its several ambitious 'task forces', for instance, pay little heed to the discourse. But the catalytic role of the discourse, and the political capital exhibited in the discussions so far, would have offered some impetus to such initiatives. Thus, prospects of the privacy discourse are being frustrated not just by the usual difficulties of international lawmaking but also because of the disjoint with the mandate of the SRP.

C Reimagining International Privacy Law in the Digital Age

Third, the thesis has found that the best way forward is to adopt a pragmatic approach. A central argument of the thesis is that a pragmatic approach that is 'incremental and historically-minded', 'practical', 'multi-faceted' and 'programmatic' would make international privacy law better-equipped in the digital age. The 'incremental and historically-minded' nature of the approach reflects the aim of proposed reform ideas to build on existing international legal frameworks on the right to privacy and well-established precedents in international law. 'Practicality' describes the feasibility of the reform proposals not only in the present political reality but also other attendant determining factors. What makes the overall approach 'multi-faceted' is the deliberate attempt at drawing insights from multiple sources in mapping out the right to privacy in the new realities of the digital age. The approach also has a 'programmatic' orientation by which it seeks to position

international privacy law in manner able to continually adapt to dynamism in the digital space.

Organized around these four elements, the thesis argued for an international soft law on the right to privacy and a dialogical approach to digital privacy. It is argued that this suite of measures would respectively lessen normative and institutional gaps in present international law of privacy. First, the thesis explored virtues of a soft law that would 'supplement' the right to privacy in international (hard) law. It is argued that soft law would not only help clarify the scope of the right to privacy in the digital context, but also globalize emergent privacy standards and facilitate progressive development of privacy law. The thesis set out the possible normative content of the proposed soft law, including the respective obligations of States and (Internet) corporations in the promotion, respect and protection of the right to privacy.

Second, the thesis considered virtues of a dialogical approach that would lessen institutional gaps. It is argued that a dialogical approach is especially suited to address challenges associated with implementation of human rights in digital space for two reasons. One is that dialogue is a practical way forward because other radical means of addressing enforcement problems, for example through creation of a world human rights court, are unlikely to materialize in the present political reality. The other is that ongoing dialogue among key actors is a responsive and adaptive mechanism to the rather dynamic nature of the digital environment where privacy threats as well as protective mechanisms constantly change. Accordingly, the thesis argued for the creation of a multi-stakeholder privacy forum where current and emerging privacy issues are discussed on an ongoing basis. The thesis has emphasized the value of the forum towards building consensus, sharing best practices and fostering cooperation among stakeholders. It has elaborated the rationales, functions and structures of the forum. By building consensus on emerging issues, regular dialogue among relevant actors in the forum would be more effective than other avenues for ensuring implementation such as adjudication.

III SEIZING THE MOMENT FOR PRACTICAL REFORM

As shown throughout this thesis, the need for reform and that such reform must be pursued at the international level is widely acknowledged. This is partly illustrated by the flurry international privacy initiatives as well as calls for an international privacy framework. Nevertheless, while proliferation of initiatives suggests the need for reform, the nature, form and processes of such reform remain elusive. Common to most reform efforts is that they are not action-oriented and hence unlikely to result in a reform that realizes the much-desired international privacy framework. As demonstrated in this thesis, neither the IBRs Project and the ongoing UN privacy

discourse – either in their own right or through a cross-fertilized process – would evolve into an international law response to the ‘privacy problem’ in the digital age. In that sense, they do not respond to the exigencies of international privacy law reform.

There are at least two key factors that make global privacy initiatives less suited answers to the reform imperative. One is the occasional nature of the overall movement behind a new global privacy framework. More often than not, calls for and initiatives for such a framework emerge sporadically and then quickly disappear into obscurity. This particularly epitomizes the IBRs Project which, as shown in chapter 3, has been a sporadic digital rights movement. The urgency of a global privacy framework cannot thus be realized via IBRs. The other factor is that global efforts of introducing some form of an international privacy framework, thus far, often proceed in a fragmented manner. With almost each reform initiative following its own path, it is unlikely that one will succeed in addressing its stated objective. As highlighted above, there is already a treaty process initiated by the SRP on government surveillance but proceeds in isolation of other reform efforts like the UN privacy discourse. Such fragmentation further frustrates possibilities of reform in the foreseeable future. But more crucially, this feature – added to the characteristically occasional nature of reform efforts – reflects a lack of clear vision for reimagining current international law of privacy in the digital age.

The second factor is that the movement tends to overlook fundamental practical considerations. As argued in this thesis, while most global privacy initiatives (and the accompanying scholarship) seek to make existing law fit for a new age, they overlook an equally important feature of the digital age. That is the inherently dynamic and changing landscape of the digital space. The nature of privacy threats as well as actors involved in its protection and violation change constantly. Any international law response, thus, must be attentive to such reality. That is a major flaw of the movement behind, albeit sporadic, global privacy initiatives.

On top of being momentary and fragmented, most reform efforts are too ambitious to attend to the exigencies of reform. Any reform effort with any hard legalization approach in sight – in the present political reality of ideological contestations – is moot. What is urgently needed, as argued in this thesis, is a reform path that finds a way through this reality to an achievable alternative. A key component of the approach argued in this thesis is the ‘practical’ nature of the proposed reform ideas. In the face of limited political will on the part of some but decisive States – added to the inevitable lobbying efforts of non-State interest groups, more ambitious reform efforts are currently implausible.

But again, the concern is not limited to difficulties of having, for example a privacy treaty adopted. Even if one or more of the privacy initiatives materialize, there is no

guarantee that the state of global privacy protection would magically improve. A number of hurdles stand in the way of actually improving the enjoyment of the right to privacy (and other human rights that it enables). One is that orthodox human rights monitoring mechanisms have, time and again, proven to be inaccessible, time-taking and hence ineffective. With such conundrum comes the gradual decline of the momentum evoked by the Snowden revelations, which perhaps offered a historic opportunity towards rethinking the right to privacy in international law.

After a major post-ICCPR UN privacy agenda broached at the Teheran Conference on Human Rights in 1968 — which eventually led to the adoption of the UN Data Privacy Guidelines in 1990 as discussed in chapter 2 — the Snowden debacle offers probably the second ‘historical cycle’, to use Weiss and Daws’s words, of reimagining international privacy law in the digital age.⁸⁴¹ But this opportunity might be lost unless an achievable approach is pursued. This thesis was an attempt to point towards such practical reform ideas to adapt current international law of privacy to the new realities of the digital age. The reform ideas are suited to the fabric of the UN system which – in line with the apt observation noted in the epigraph – is adaptive only to modest changes. Moving beyond the piecemeal, ungrounded, and haphazard nature of hitherto reform paths, this thesis has argued for a modest but plausible reform approach that will make international privacy law better-equipped in the digital age.

⁸⁴¹ Thomas Weiss and Sam Daws, ‘The United Nations: Continuity and Change’ in Weiss and Daws (eds), *The Oxford Handbook on the United Nations* (Oxford University Press, 2018) 19.

BIBLIOGRAPHY

A Books and Chapters

Alpin, Tanya and Jason Bosland, 'The Uncertain Landscape of Article 8 of the ECHR: The Protection of Reputation as a Fundamental Rights?' in Andrew Kenyon (ed), *Comparative Defamation and Privacy Law* (Cambridge University Press, 2016)

Alston, Philip, 'Beyond Them and Us: Putting Treaty Body Reform into Perspective' in Philip Alston and James Crawford (eds), *The Future of UN Human Rights Treaty Monitoring* (Cambridge University Press, 2000)

Alston, Philip, 'The Commission on Human Rights' in Philip Alston (ed), *The United Nations and Human Rights: A Critical Appraisal* (Oxford University Press, 1992)

Armstrong, Mark et al, *Media Law in Australia* (Oxford University Press, 3rd ed., 1995)

Barelli, Mauro, *Seeking Justice in International Law: The Significance and Implications of the UN Declaration on the Rights of Indigenous Peoples* (Routledge, 2016)

Barendt, Eric, 'Privacy and Freedom of Speech' in Andrew Kenyon and Megan Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, 2006)

Benedetto, Conforti, *The Law and Practice of the United Nations* (Martinus Nijhoff Publishers, 3rd ed, 2004)

Bennett, Colin and Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, 2006)

Bignami, Francesca and Giorgio Resta, 'Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance' in Eyal Benvenisti and Georg Nolte (eds), *Community Interests Across International Law* (Oxford University Press, 2018)

Bonafe, Beatrice and Paolo Palchetti, 'Relying on General Principles in International Law' in Catherine Brölmann and Yannick Radi (eds), *Research*

Handbook on the Theory and Practice of International Law Making (Edward Elgar, 2016)

Boot, Eric, *Human Duties and the Limits of Human Rights Discourse* (Springer, 2017)

Bossuyt, Marc, *Guide to the “Travaux préparatoires” of the International Covenant on Civil and Political Rights* (Martinus Nijhoff Publishers, 1987)

Bourdieu, Pierre, ‘Political Representation: Elements for a Theory of the Political Field’ in Pierre Bourdieu (ed), *Language and Symbolic Power* (Polity Press, 1991)

Boutros-Ghali, Boutros, ‘Introduction’ in *United Nations and Human Rights (1945-1995)* (United Nations Blue Book, 1995)

Boyle, Alan and Christine Chinkin, *The Making of International Law* (Oxford University Press, 2007)

Brems, Eva, ‘Introduction: Rewriting Decisions from a Perspective of Human Rights Integration’ in Eva Brems and Ellen Desmet (eds), *Integrating Human Rights in Practice: Rewriting Human Rights Decisions* (Edward Elgar, 2017)

Brown, Gordon (ed), *The Universal Declaration of Human Rights in the 21st Century: A Living Document in A Changing World* (Open Book Publishers, 2016)

Burke, Ronald and James Kirby, ‘The Universal Declaration of Human Rights: Politics and Provisions (1945-1948)’ in Gerd Oberleitner (ed), *International Human Rights Institutions, Tribunals and Courts* (Springer, 2018)

Bygrave, Lee, ‘International Agreements to Protect Personal Data’ in James Rule and Graham Greenleaf (eds), *Global Privacy Protection: The First Generation* (Edward Elgar, 2008)

Bygrave, Lee, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014)

Bygrave, Lee, *Internet Governance by Contract* (Oxford University Press, 2015)

Casagran, Cristina, *Global Data Protection in the Field of Law Enforcement: An EU Perspective* (Routledge, 2016)

Cassese, Antonio, *International Law in a Divided World* (Clarendon Press, 1986)

Charlesworth, Hilary, 'A Regulatory Perspective on the International Human Rights System' in Peter Drhaos (ed), *Regulatory Theory: Foundations and Applications* (ANU Press, 2017)

Charlesworth, Hilary, 'Law Making and Sources' in James Crawford and Martti Koskenniemi (eds), *The Cambridge Companion to International Law* (Cambridge University Press, 2012)

Chauville, Roland, 'The Universal Periodic Review's First Cycle: Successes and Failures' in Hilary Charlesworth and Emma Larking (eds), *Human Rights and the Universal Periodic Review: Rituals and Ritualism* (Cambridge University Press, 2015)

Chesterman, Simon, *One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty* (Oxford University Press, 2011)

Chinkin, Christine, 'Normative Development in the International Legal System' in Dinah Shelton (ed), *Commitment and Compliance: The Role of Non-Binding Norms in the International Legal System* (Oxford University Press, 2000)

Clapham, Andrew, *Human Rights Obligations of Non-State Actors* (Oxford University Press, 2006)

Crawford, James, *Brownlie's Principles of Public International Law* (Oxford University Press, 2012)

Croce, Benedetto, 'The Rights of Man and the Present Historical Situation' in *Human Rights: Comments and Interpretations* (Columbia University Press, 1949)

Daly, Angela, *Mind the Gap: Private Power, Online Information Flows and EU Law* (Hart Publishing, 2016)

Danileko, Gennady, *Law-Making in the International Community* (Martinus Nijhoff Publishers, 1993)

De Hert, Paul and Vagelis Papakonstantinou, 'Moving Beyond the Special Rapporteur on Privacy with the Establishment of a New, Specialized United Nations Agency: Addressing the Deficit in Global Cooperation for the Protection of Data Privacy' in Dan Svantesson and Dariusz Kloza (eds), *Transatlantic Privacy Relations as a Challenge to Democracy* (Intersentia, 2017)

Deeks, Ashly, 'Regulating Foreign Surveillance Through International Law' in Fred Cate and James Dempsey (eds), *Bulk Collection: Systematic Government Access to Private-Sector Data* (Oxford University Press, 2017)

DeNardis, Laura, *The Global War for Internet Governance* (Yale University Press, 2014)

de Zwart, Melissa, 'Privacy for the Weak, Transparency for the Powerful' in Andrew Kenyon (ed), *Comparative Defamation and Privacy Law* (Cambridge University Press, 2016)

Doria, Avri, 'Use [and Abuse] of Multistakeholderism in the Internet' in Roxana Radu et al (eds), *The Evolution of Global Internet Governance: Principles and Policies in the Making* (Springer, 2013)

Dupuy, Pierre-Marie, 'Formation of Customary International Law and General Principles' in Daniel Dobansky et al (eds) *Oxford Handbook of International Environmental Law* (Oxford University Press, 2007)

Dupuy, René, 'Declaratory Law and Programmatic Law: From Revolutionary Custom to "Soft Law"' in R.J. Akkerman (ed), *Declaration on Principles: A Quest for Universal Peace* (Kluwer Law International, 1977)

Edmundson, William, *An Introduction to Rights* (Cambridge University Press, 2004)

Farer, Tom and Felice Gaer, 'The UN and Human Rights: At the End of the Beginning' in Adam Roberts and Benedict Kingsbury (eds), *United Nations, Divided World: The UN's Roles in International Relations* (Clarendon Press, 2nd ed, 1993)

Fidler, David (ed), *The Snowden Reader* (Indiana University Press, 2015)

Fidler, David, 'Cyberspace and Human Rights' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar, 2015)

Fidler, David, 'United Nations Resolution on the Right to Privacy in the Digital Age' in David Fidler (ed), *The Snowden Reader* (Indiana University Press, 2015)

Foot, Rosemary, 'The Cold War and Human Rights' in Melvyn Leffler and Odd Westad (eds), *The Cambridge History of the Cold War* (Cambridge University Press, Vol. 3, 2010)

Fox, Graham, 'The United Nations Forum on Minority Issues and Its Role in Promoting the UN Declaration on the Rights of Persons Belonging to National or Ethnic, Religious and Linguistic Minorities' in Ugo Caruso and Rainer Hofmann

(eds), *The United Nations Declaration on Minorities: An Academic Account on the Occasion of Its 20th Anniversary (1992-2012)* (Brill, 2015)

Franklin, Marianne, 'Mobilizing for Net Rights: The IRPC Charter of Human Rights and Principles for the Internet' in Jonathan Obar et al (eds), *Strategies for Media Reform: International Perspectives* (Fordham University Press, 2016)

Franklin, Marianne, *Digital Dilemmas: Power, Resistance and the Internet* (Oxford University Press, 2013)

Fuster, Gloria, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer, 2014)

Garfinkel, Simon, *Database Nation: The Death of Privacy in the 21st Century* (O'Reilly, 2000)

Glendon, Mary, *A World Made New: Eleanor Roosevelt and the Universal Declaration of Human Rights* (Random House, 2001)

Glendon, Mary, *Rights Talk: The Impoverishment of Political Discourse* (Free Press, 1991)

Goldsmith, Jack and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press, 2006)

Greenleaf, Graham, 'A World Data Privacy Treaty? 'Globalisation' and 'Modernisation' of Council of Europe Convention 108' in Normann Witzleb et al (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press, 2014)

Greenleaf, Graham, 'Data Protection in A Globalized Network' in Ian Brown (ed), *Research Handbook on Governance of the Internet* (Edward Elgar, 2012)

Griffin, James, *On Human Rights* (Oxford University Press, 2009)

Goldin, Ian, *Divided Nations: Why Global Governance is Failing, and What We Can Do About It* (Oxford University Press, 2013)

Gross, Leo, *Essays on International Law and Organization* (Springer, Vol. I/II, 2014)

Hale, Thomas et al, *Gridlock: Why Global Cooperation Is Failing When We Need It Most* (Polity Press, 2013)

Higgins, Rosalyn, *Problems and Process: International Law and How We Use It* (Oxford University Press, 1995)

Higgins, Rosalyn, *The Development of International Law Through the Political Organs of the United Nations* (Oxford University Press, 1963)

Higgins, Rosalyn, *Themes and Theories: Selected Essays, Speeches and Writings in International Law* (Oxford University Press, Vol. I, 2009)

Hill, Richard, 'Internet Governance, The Last Gasp of Colonialism, or Imperialism by other Means?' in Roxana Radu et al (eds), *The Evolution of Global Internet Governance: Principles and Policies in the Making* (Springer, 2013)

Hubbard, Amanda and Lee Bygrave, 'Internet Governance Goes Global' in Lee Bygrave and Jon Bing, *Internet Governance: Infrastructure and Institutions* (Oxford University Press, 2009)

Humphrey, John, 'The Universal Declaration of Human Rights: Its History, Impact and Juridical Character' in Bertrand Ramcharan (ed), *Human Rights Thirty Years After the Universal Declaration* (Brill, 1979)

Ignatieff, Michael, 'Human Rights as Politics and Idolatry' in Amy Gutmann (ed), *Human Rights as Politics and Idolatry* (Princeton University Press, 2001)

Joseph, Sarah and Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Materials and Commentary* (Oxford University Press, 3rd ed., 2013)

Jorgensen, Rikke, 'An Internet Bill of Rights?' in Ian Brown (ed), *Research Handbook on Governance of the Internet* (Edward Elgar, 2013)

Kalin, Walter and Jorg Kunzli, *The Law of International Human Rights Protection* (Oxford University Press, 2009)

Karavias, Markos, *Corporate Obligations Under International Law* (Oxford University Press, 2013)

Keck, Margaret and Kathryn Sikkink, *Activists Beyond Borders: Advocacy Networks in International Politics* (Cornell University Press, 1998)

Keller, Perry, *European and International Media Law: Liberal Democracy, Trade and the New Media* (Oxford University Press, 2011)

Martti, Koskenneimi, *From Apology to Utopia: The Structure of International Legal Argument* (Cambridge University Press, 2006)

Krotoszynski Jr, Ronald. *Privacy Revisited: A Global Perspective on the Right to Be Left Alone* (Oxford University Press, 2016)

Kubota, Yo, 'The Institutional Response' in Christopher Weeramantry (ed), *Human Rights and Scientific and Technological Development* (United Nations University Press, 1990)

Lagoni, Rainer, 'Resolution, Declaration, Decision' in Rudiger Wolfrum (ed), *United Nations: Law, Policies and Practice* (Springer, 1995)

Lauren, Paul, *The Evolution of International Human Rights: Visions Seen* (University of Pennsylvania Press, 3rd ed, 2011)

Lauterpacht, Hersch, *International Law and Human Rights* (Stevens and Sons Limited, 1950)

Lawson, Edward (ed), *Encyclopedia of Human Rights* (Taylor & Francis, 2nd ed, 1996)

Lynskey, Orla, *The Foundations of EU Data Protection Law* (Oxford University Press, 2015)

Madsen, Wayne, *Handbook of Personal Data Protection* (Macmillan Publishers, 1992)

Makulilo, Alex, 'The Context of Data Privacy in Africa' in Alex Makulio (ed), *African Data Privacy Laws* (Springer, 2016)

Makulilo, Alex, 'The Future of Data Protection in Africa' in Alex Makulilo (ed), *African Data Privacy Laws* (Springer, 2016)

Meckled-Garcia, Saladin, 'Specifying Human Rights' in Rowan Cruft et al (eds), *Philosophical Foundations of Human Rights* (Oxford University Press, 2015)

Mégret, Frédéric, 'Nature of Obligations' in Daniel Moeckli et al (eds), *International Human Rights Law* (Oxford University Press, 2nd ed, 2014)

Michael, James, *Privacy and Human Rights: An International and Comparative Study with Special Reference to Developments in Information Technology* (Dartmouth, 1994)

Millard, Christopher, 'Data Privacy in the Clouds' in Mark Graham and William Dutton (eds), *Society and the Internet: How Networks of Information and Communication are Changing Our Lives* (Oxford University Press, 2014)

Morsink, Johannes, *The Universal Declaration of Human Rights: Origins, Drafting and Intent* (University of Pennsylvania Press, 1999)

Moskowitz, Moses, *International Concern for Human Rights* (Oceana Publications, 1974)

Nowak, Manfred and Karolina Januszcwski, 'Non-State Actors and Human Rights' in Math Noortmann et al (eds), *Non-State Actors in International Law* (Hart Publishing, 2015)

Nowak, Manfred, 'A World Court of Human Rights' in Gerd Oberleitner (ed), *International Human Rights Institutions, Tribunals and Courts* (Springer, 2018)

Nowak, Manfred, 'It's Time for a World Court of Human Rights' in Cherif Bassiouni and William Schabas (eds), *New Challenges for the UN Human Rights Machinery: What Future for the UN Treaty Body System and the Human Rights Council Procedures?* (Intersentia, 2011)

Nowak, Manfred, *UN Covenant on Civil and Political Rights: CCPR Commentary* (NP Engel, 2005)

Nußberger, Angelika, 'The ECtHR's Use of Decisions of International Courts and Quasi-Judicial Bodies' in Amrei Muller and Hege Kjos (eds), *Judicial Dialogue and Human Rights* (Cambridge University Press, 2017)

O'Boyle, Michael and Michelle Lafferty, 'General Principles and Constitutions as Sources of Human Rights Law' in Dinah Shelton (ed), *The Oxford Handbook of International Human Rights Law* (Oxford University Press, 2013)

Ogata, Sadako, 'Introduction: United Nations Approaches to Human Rights and Scientific Developments' in Christopher Weeramantry (ed), *Human Rights and Scientific and Technological Development* (United Nations University Press, 1990)

Paulwelyn, Joost et al (eds), *Informal International Lawmaking* (Oxford University Press, 2012)

Paulwelyn, Joost et al, 'Informal International Lawmaking: An Assessment and Template to Keep It Both Effective and Accountable' in Joost Paulwelyn et al (eds), *Informal International Lawmaking* (Oxford University Press, 2012)

Posner, Eric, *The Twilight of Human Rights Law* (Oxford University Press, 2014)

Ramcharan, Bertrand, 'The Law-Making Process: From Declaration to Treaty and Custom' in Dinah Shelton (ed), *The Oxford Handbook of International Human Rights Law* (Oxford University Press, 2013)

Randall, Maya, 'The History of the Covenants: Looking Back Half a Century and Beyond' in David Moeckli et al (eds), *Human Rights Covenants At 50: The Past, Present and Future* (Oxford University Press, 2018)

Raz, Joseph, 'Human Rights in the Emerging World Order' in Rowan Cruft et al (eds), *Philosophical Foundations of Human Rights* (Oxford University Press, 2015)

Rechota, Vratislav, 'The Development of the Covenant on Civil and Political Rights' in Louis Henkin (ed), *The International Bill of Rights: The Covenant on Civil and Political Rights* (Columbia University Press, 1981)

Reed, Chris, *Making Laws for Cyberspace* (Oxford University Press, 2012)

Rehof, Lars, 'Article 12' in Asbjorn Eide et al (eds), *The Universal Declaration of Human Rights: A Commentary* (Scandinavian University Press, 1992)

Rengel, Alexandra, *Privacy in the 21st Century* (MartinusNijhoff, 2013)

Richardson, Megan, *The Right to Privacy: Origins and Influence of a Nineteenth Century Idea* (Cambridge University Press, 2017)

Risse, Thomas and Kathryn Sikkink, 'The Socialization of International Human Rights Norms in Domestic Practices: Introduction' in Thomas Risse et al (eds), *The Power of Human Rights: International Norms and Domestic Change* (Cambridge University Press, 1999)

Roberts, Christopher, *The Contentious History of the International Bill of Human Rights* (Cambridge University Press, 2014)

Rodotà, Stefano, 'Data Protection as a Fundamental Right' in Serge Gutwirth et al (eds), *Reinventing Data Protection?* (Springer, 2009)

Rodotà, Stefano, 'Protecting Informational Privacy: Trends and Problems' in Willem Ates et al (eds), *Information Law Towards The 21st Century* (Kluwer Law and Taxation Publishers, 1992)

Sartor, Giovanni, 'Human Rights and Information Technologies' in Roger Brownsword et al (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press, 2017)

Saul, Ben, *Indigenous Peoples and Human Rights: International and Regional Jurisprudence* (Hart Publishing, 2016)

Schabas, William (ed), *The Universal Declaration of Human Rights: The Travaux Préparatoires* (Cambridge University Press, Vol. I, 2013)

Schabas, William, *The European Convention on Human Rights: A Commentary* (Oxford University Press, 2015)

Schachter, Oscar, *International Law in Theory and Practice* (Martinus Nijhoff Publishers, 1991)

Schieder, Siegfried, 'Pragmatism and International Law' in Harry Bauer and Elisabetta Brighi (eds), *Pragmatism in International Relations* (Routledge, 2009)

Schmitt, Michael (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017)

Schmitt, Michael, 'Introduction' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar, 2015)

Seibert-Fohr, Anja, 'The Human Rights Committee' in Gerd Oberleitner (ed), *International Human Rights Institutions, Tribunals and Courts* (Springer, 2018)

Sheinine, Martin, 'The International Covenant on Civil and Political Rights' in Geir Ulfstein et al (eds), *Making Treaties Work: Human Rights, Environment and Arms Control* (Cambridge University Press, 2007)

Shelton, Dinah, 'Commentary and Conclusions' in Dinah Shelton (ed), *Commitment and Compliance: The Role of Non-Binding Norms in the International Legal System* (Oxford University Press, 2000)

Shelton, Dinah, 'Human Rights' in Dinah Shelton (ed), *Commitment and Compliance: The Role of Non-Binding Norms in the International Legal System* (Oxford University Press, 2000)

Shelton, Dinah, 'Introduction: Law, Non-Law and the Problem of Soft Law' in Dinah Shelton (ed), *Commitment and Compliance: The Role of Non-Binding Norms in the International Legal System* (Oxford University Press, 2000)

Shelton, Dinah and Paolo Carozza (eds), *Regional Protection of Human Rights* (Oxford University Press, Vol. I, 2nd ed, 2013)

Shorupski, John, 'Human Rights' in Samantha Besson and John Tasioulas (eds), *Philosophy of International Law* (Oxford University Press, 2010)

Ssenyonjo, Manisuli, *Economic, Social and Cultural Rights in International Law* (Hart Publishing, 2nd ed, 2016)

Steiner, Henry, 'Individual Claims in A World of Massive Violations: What Role for the Human Rights Committee?' in Philip Alston and James Crawford (eds), *The Future of the UN Human Rights Treaty Monitoring* (Cambridge University Press, 2000)

Tahzib, Bahiyyih, *Freedom of Religion Or Belief: Ensuring Effective International Legal Protection* (Martinus Nijhoff Publishers, 1996)

Thornberry, Patrick, *International Law and the Rights of Minorities* (Clarendon Press, 1991)

Tobin, John and Sarah Field, 'Article 16: The Right to Protection of Privacy, Family, Home, Correspondence, Honour and Reputation' in John Tobin (ed), *The UN Convention on the Rights of the Child: A Commentary* (Oxford University Press, 2019)

Tomuschat, Christian, *Human Rights: Between Idealism and Realism* (Oxford University Press, 3rd ed, 2014)

Tyagi, Yogesh, *The Human Rights Committee: Practice and Procedure* (Cambridge University Press, 2011)

Tzanou, Maria, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publishing, 2017)

Vandenhoe, Wouter and Willem van Genugten, 'Introduction: An Emerging Multi-Duty-Bearer Human Rights Regime?' in Wouter Vandenhoe (ed), *Challenging Territoriality in Human Rights Law: Building Blocks for a Plural and Diverse Duty-Bearer Regime* (Routledge, 2015)

Velu, Jacques, 'The European Convention on Human Rights and the Right to Respect for Private Life, The Home and Communications' in Arthur Robertson (ed), *Privacy and Human Rights* (Manchester University Press, 1973)

Volio, Fernando, 'Legal Personality, Privacy and the Family' in Louis Henkin (ed), *The International Bill of Rights: The Covenant on Civil and Political Rights* (Columbia University Press, 1981)

Wacks, Raymond, *Privacy: A Very Short Introduction* (Oxford University Press, 2015)

Weiss, Thomas and Sam Daws, 'The United Nations: Continuity and Change' in Weiss and Daws (eds), *The Oxford Handbook on the United Nations* (Oxford University Press, 2018)

Witzleb, Normann et al, 'An overview of Emerging Challenges in Privacy Law' in Norman Witzleb et al (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press, 2014)

Wouters, Jan and Anna-Luise Chance, 'Multinational Corporations in International Law' in Math Noortmann et al (eds), *Non-State Actors in International Law* (Hart Publishing, 2015)

Yamane, Hiroko, 'Impacts of Scientific and Technological Progress on Human Rights: Normative Response of the International Community' in Christopher Weeramantry (ed), *Human Rights and Scientific and Technological Development* (United Nations University Press, 1990)

B Journal Articles

Abbott, Kenneth and Duncan Snidal, 'Hard and Soft Law in International Governance' (2000) 54 *International Organization* 421

Abbott, Kenneth et al, 'The Concept of Legalization' (2000) 54 *International Organization* 401

Abbott, Kenneth, 'The Many Faces of International Legalization' (1998) 92 *Proceedings of the Annual Meeting of the ASIL* 57

Alston, Philip, 'Against a World Court for Human Rights' (2014) 28 *Ethics and International Affairs* 197

Alston, Philip, 'Conjuring Up New Human Rights: A Proposal for Quality Control' (1984) 78 *American Journal of International Law* 607

Alston, Philip, 'The Populist Challenge to Human Rights' (2017) 9 *Journal of Human Rights Practice* 1

Alwicker, Tilmann, 'Transnationalizing Rights: International Human Rights Law in Cross-Border Contexts' (2018) 29 *European Journal of International Law* 581

Asamoah, Obed, 'The Legal Effect of Resolutions of the General Assembly' (1965) 3 *Columbia Journal of Transnational Law* 210

Barton, John and Barry Carter, 'International Law and Institutions for a New Age' (1992/93) *Georgetown Law Journal* 535

Bayefsky, Anne, 'Making Human Rights Work' (1997) 26 *Studies in Transnational Legal Policy* 229

Besson, Samantha and Jose Marti, 'Legitimate Actors of International Law-making: Towards a Theory of International Democratic Representation' (2018) 9 *Jurisprudence: An International Journal of Legal and Political Thought* 504

Bleicher, Samuel, 'The Legal Significance of Re-Citation of General Assembly Resolutions' (1969) 63 *American Journal of International Law* 444

Bos, Maarten, 'Theory and Practice of Treaty Interpretation' (1980) 27 *Netherlands International Law Review* 135

Brennan, Kathrine et al, 'The Fortieth Session of the U.N. Sub-Commission on Prevention of Discrimination and Protection of Minorities' (1989) 11 *Human Rights Quarterly* 295

Brennan, William, 'Why Have a Bill of Rights?' (1989) 9 *Oxford Journal of Legal Studies* 425

Brown, Ian, 'The Feasibility of Transatlantic Privacy-protective Standards for Surveillance' (2015) 23 *International Journal of Law and Information Technology* 23

Brownlie, Ian, 'Legal Status of Natural Resources in International Law' (1979) 162 *Recueil des Cours* 1

Buerghenthal, Thomas, 'The UN Human Rights Committee' (2001) 5 *Max Planck Yearbook of United Nations Law* 341

Bygrave, Lee, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 *International Journal of Law and Information Technology* 247

Casacuberta, David and Max Senges, 'Do We Need New Rights in Cyberspace? Discussing the Case of How to Define Online Privacy in an Internet Bill of Rights' (2008) 40/41 *Enrahonar* 99

Cassel, Doug, 'The Third Session of the UN Inter-Governmental Working Group on a Business and Human Rights Treaty' (2018) 3 *Business and Human Rights Journal* 277

Castenada, Jorge, 'The Underdeveloped Nations and the Development of International Law' (1961) 15 *International Organizations* 38

Chander, Anupam and Molly Land, 'Introductory Note to United Nations General Assembly Resolution on the Right to Privacy in the Digital Age' (2014) 53 *International Legal Materials* 727

Clement, Dominique, 'Human Rights or Social Justice? The Problem of Rights Inflation' (2018) 22 *International Journal of Human Rights* 155

Cole, David and Federico Fabbrini, 'Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders' (2016) 14 *International Journal of Constitutional Law* 220

Cooper, Daniel and Christopher Kuner, 'Data Protection Law and International Dispute Resolution' (2017) 382 *Collected Courses of The Hague Academy of International Law* 1

d'Aspermont, Jean, 'Softness in International Law: A Self-Serving Quest for New Legal Materials' (2008) 19 *European Journal of International Law* 1075

de Burca, Grainne, 'Human Rights Experimentalism' (2017) 111 *American Journal of International Law* 277

De Hert, Paul and Vagelis Papakonstantinou, 'Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?' (2013) 9 *I/S: A Journal of Law and Policy for the Information Society* 271

De Minico, Giovanna, 'Towards an Internet Bill of Rights' (2015) 37 *Loyola of Los Angeles International and Comparative Law Review* 1

Deeks, Ashley, 'An International Legal Framework for Surveillance' (2015) 55 *Virginia Journal of International Law* 291

- Diggelmann, Oliver and Maria Nicole Cleis, 'How the Right to Privacy Become a Human Right' (2014) 14 *Human Rights Law Review* 441
- Donnelly, Jack, 'International Human Rights: A Regime Analysis' (1986) 40 *International Organization* 599
- Dupuy, Pierre-Marie, 'Soft Law and the International Law of Environment' (1990/91) 12 *Michigan Journal of International Law* 420
- Edwards, Lilian, 'Reconstructing Consumer Privacy Protection Online: A Modest Proposal' (2004) 18 *International Review of Law, Computers and Technology* 313
- Egan, Suzanne, 'Strengthening the United Nations Human Rights Treaty Body System' (2013) 13 *Human Rights Law Review* 209
- Eichensehr, Kristen, 'Digital Switzerlands' (2019) 167 *University of Pennsylvania Law Review* 1 (forthcoming)
- Fischer-Lescano, Andreas, 'Struggles for a Global Internet Constitution: Protecting Global Communication Structures Against Surveillance Measures' (2016) 5 *Global Constitutionalism* 145
- Forsythe, David, 'The United Nations and Human Rights: 1945-1985' (1985) 100 *Political Science Quarterly* 249
- Garibaldi, Oscar, 'The Legal Status of General Assembly Resolutions: Some Conceptual Observations' (1979) 73 *Proceedings of the Annual Meeting of the ASIL* 324
- Georgieva, Ilina, 'The Right to Privacy Under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR' (2015) 31 *Utrecht Journal of International and European Law* 104
- Greenleaf, Graham, 'Accession to Council of Europe Privacy Convention 108 by Non-European States' (2008) 94 *Privacy Laws and Business International Reports* 1
- Greenleaf, Graham, 'Global Analysis of Data Privacy Laws and Bills' (2017) 145 *Privacy Laws and Business International Report* 14
- Greenleaf, Graham, 'The UN Special Rapporteur: Advancing A Global Privacy Treaty?' (2015) 136 *Privacy Laws and International Business Report* 6

Gross, Leo, 'The United Nations and the Role of Law' (1965) 19 *International Organization* 537

Gruchalla-Wesierski, Tadeusz, 'A Framework for Understanding "Soft Law"' (1984) 30 *McGill Law Journal* 37

Hamilton, Michael and Antoine Buyse, 'Human Rights Courts as Norm-Brokers' (2018) 18 *Human Rights Law Review* 205

Handl, Guthrie et al, 'A Hard Look at Soft Law' (1988) 82 *Proceedings of the Annual Meeting of the ASIL* 371

Hannum, Hurst, 'Reinvigorating Human Rights for the 21st Century' (2016) 16 *Human Rights Law Review* 409

Higashi, Jutaro, 'The Role of Resolutions of the United Nations General Assembly in the Formative Process of International Customary Law' (1982) 25 *Japanese Annual of International Law* 11

Hofmann, Jeannette, 'Multi-stakeholderism in Internet Governance: Putting a Fiction into Practice' (2016) 1 *Journal of Cyber Policy* 29

Hohfeld, Wesley, 'Fundamental Legal Conceptions as Applied in Judicial Reasoning' (1917) 26 *Yale Law Journal* 710

Humphrey, John, 'The International Bill of Rights: Scope and Implementation' (1976) 17 *William and Mary Law Review* 527

Humphrey, John, 'The Universal Declaration of Human Rights' (1949) 4 *International Journal* 351

Huneus, Alexandra, 'Human Rights and the Future of Being Human' (2018) 112 *AJIL Unbound Symposium on UDHR at 70 and the Future of Being Human* 324

Jorgensen, Rikke, 'Can Human Rights Law Bend Mass Surveillance?' (2018) 3 *Internet Policy Review* 1

Joseph, Sarah, 'Social Media, Political Change and Human Rights' (2012) 35 *Boston College International and Comparative Review* 145

Joyner, Christopher, 'UN General Assembly Resolutions and International Law: Rethinking Contemporary Dynamics of Norm-Creation' (1981) 11 *California Western International Law Journal* 445

Kaufmann, Christine, 'Multi-stakeholder Participation in Cyberspace' (2016) 26 *Swiss Review of International and European Law* 217

Kerwin, Gregory, 'The Role of United Nations General Assembly Resolutions in Determining Principles of International Law in US Courts' (1983) 32 *Duke Law Journal* 876

Kirby, Michael, 'Human Rights and Bioethics: The Universal Declaration of Human Rights and UNESCO Universal Declaration of Bioethics and Human Rights' (2009) 25 *Journal of Contemporary Health Law and Policy* 309

Kirby, Michael, 'The History, Achievement and Future of the 1980 OECD Guidelines on Privacy' (2011) 1 *International Data Privacy Law* 6

Klabbers, Jan, 'The Undesirability of Soft Law' (1998) 67 *Nordic Journal of International Law* 381

Knox, John, 'Horizontal Human Rights Law' (2008) 102 *American Journal of International Law* 1

Koh, Harold, 'The 1994 Roscoe Pound Lecture: Transnational Legal Process' (1996) 75 *Nebraska Law Review* 181

Koops, Bert-Jaap and Ronald Leenes, 'Privacy Regulation cannot be Hardcoded: A Critical Comment on the 'Privacy by Design' Provision in Data Protection Law' (2014) 28 *International Review of Law, Computers and Technology* 159

Koops, Bert-Jaap et al (2017) A Typology of Privacy, 38 *University of Pennsylvania Journal of International Law* 438

Kuner, Christopher, 'An International Legal Framework for Data Protection: Issues and Prospects' (2009) 25 *Computer Law and Security Review* 307

Kuner, Christopher, 'The European Union and the Search for an International Data Protection Framework' (2014) 2 *Groningen Journal of International Law* 54

Lachmayer, Konard, 'Rethinking Privacy Beyond Borders: Developing Transnational Rights on Data Privacy' (2015) 20 *Tilburg Law Review* 78

Land, Molly, 'Toward International Internet Law' (2013) 54 *Harvard International Law Journal* 394

Landemore, Helen, 'Inclusive Constitution-making: The Icelandic Experiment' (2015) 23 *Journal of Political Philosophy* 166

Lauterpacht, Hersch, 'The Universal Declaration of Human Rights' (1948) 25 *British Yearbook of International Law* 354

Lynskey, Orla, 'Grappling with "Data Power": Normative Nudges from Data Protection and Privacy' (2019) 20 *Theoretical Inquiries in Law* 189

Magallona, Merlin, 'Some Remarks on the Legal Character of UN General Assembly Resolutions' (1976) 5 *Philippine Yearbook of International Law* 84

Malik, Charles, 'Human Rights in the United Nations' (1951) 6 *International Journal* 275

Malik, Charles, 'Human Rights in the United Nations with Text of Draft Covenants' (1952) 1 *United Nations at Work* 1

McDougal, Myres et al, 'Aggregate Interest in Shared Respect and Human Rights: The Harmonization of Public Order and Civic Order' (1977) 23 *New York Law School Law Review* 183

Milanovic, Marko, 'Human Right Treaties and Foreign Surveillance: The Right to Privacy in the Digital Age' (2014) 56 *Harvard International Law Journal* 81

Mitsilegas, Valsamis, 'Surveillance and Digital Privacy in the Transatlantic "War on Terror": The Case for A Global Privacy Regime' (2016) 47 *Columbia Human Rights Law Review* 1

Musiani, Francesca, 'The Internet Bill of Rights: A Way to Reconcile Natural Freedom Regulatory Needs?' (2009) 6 *Scripted* 505

Mutua, Makau, 'Looking Past the Human Rights Committee: An Argument for De-Marginalizing Enforcement' (1998) 4 *Buffalo Human Rights Law Review* 211

Nyst, Carly and Thomaso Falchatta, 'The Right to Privacy in the Digital Age' (2017) 9 *Journal of Human Rights Practice* 104

Oberg, Marko, 'The Legal Effects of Resolutions of the UN Security Council and General Assembly in the Jurisprudence of the ICJ' (2006) 16 *European Journal of International Law* 879

Paust, Jordan, 'Can You Hear Me Now? Private Communication, National Security, and the Human Rights Disconnect' (2015) 15 *Chicago Journal of International Law* 612

Pauwelyn, Joost et al, 'When Structures Become Shackles: Stagnation and Dynamics in International Law Making' (2014) 25 *European Journal of International Law* 733

Pettrachin, Andrea, 'Towards a Universal Declaration of Internet Rights and Freedoms?' (2018) 80 *International Communication Gazette* 337

Ratner, Steven, 'Corporations and Human Rights: A Theory of Legal Responsibility' (2001) 111 *Yale Law Journal* 443

Raustiala, Kal, 'Governing the Internet' (2016) 110 *American Journal of International Law* 491

Raymond, Mary and Laura DeNardis, 'Multistakeholderism: Anatomy of An Inchoate Global Institution' (2015) 7 *International Theory* 572

Redeker, Dennis et al, 'Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights' (2018) 80 *International Communication Gazette* 302

Richards, Neil, 'The Dangers of Surveillance' (2013) 126 *Harvard Law Review* 1934

Risse, Mathias Risse, 'Human Rights and Artificial Intelligence: An Urgently Needed Agenda' (2019) *Human Rights Quarterly* 1

Rodotà, Stefano, 'A Bill of Rights for the Internet Universe' (2008) 21 *The Federalist Debate* 1

Roessler, Beate, 'Privacy as a Human Rights' in (2017) 117 *Proceedings of the Aristotelian Society* 187

Rozenshtein, Alan, 'Surveillance Intermediaries' (2018) 70 *Stanford Law Review* 99

Saadat, Lauren and Shannon Ballard, 'A Way Ahead for a Global Privacy Standards? – Thoughts on a UN Convention on Data Protection, International Standards and International Agreements: Which is the Best Option?' (2007) 89 *Privacy Laws and Business* 14

Schieder, Siegfried, 'Pragmatism as a Path Towards A Discursive and Open Theory of International Law' (2000) 11 *European Journal of International Law* 663 [Translated by Iain Fraser]

Schulhofer, Stephen, 'An International Right to Privacy? Be careful What You Wish For' (2016) 14 *International Journal of Constitutional Law* 238

Simma, Bruno and Philip Alston, 'The Sources of Human Rights Law: Custom, Jus Cogens and General Principles' (1992) 12 *Australian Yearbook of International Law* 82

Sohn, Louis, 'The Human Rights Law of the Charter' (1977) 12 *Texas International Law Journal* 129

Leonor, Soriano, 'A modest Notion of Coherence in Legal Reasoning: A Model for the European Court of Justice' (2003) 16 *Ratio Juris* 296

Sourgens, Frédéric Gilles, 'The Privacy Principle' (2017) 42 *The Yale Journal of International Law* 345

Souza, Carlos et al, 'Notes on the Creation and Impacts of Brazil's Internet Bill of Rights' (2017) 5 *Theory and Practice of Legislation* 73

Tene, Omer, 'Privacy: The New Generations' (2011) 1 *International Data Privacy Law* 15

Tobin, John, 'Seeking to Persuade: A Constructive Approach to Human Rights Treaty Interpretation' (2010) 23 *Harvard Human Rights Journal* 201

Trujillo, Elizabeth, 'A Dialogical Approach to Trade and Environment' (2013) 16 *Journal of International Economic Law* 535

'Universal Periodic Review' (2013) 1 *Human Rights Monitor Quarterly* 1

Wade, Ariel, 'A New Age of Privacy Protection: A Proposal for An International Personal Data Privacy Treaty' (2010) 42 *George Washington International Law Review* 659

Watt, Eliza, 'The Right to Privacy and the Future of Mass Surveillance' (2017) 21 *International Journal of Human Rights* 773

Weeramantry, Christopher, 'Science, Technology and the Future of Human Rights' (1986) 13 *India International Centre Quarterly* 41

Zalnieriute, Monika, 'An International Constitutional Moment for Data Privacy' (2015) 23 *International Journal of Law and Information Technology* 99

C Treaties

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows, opened for signature 8 November 2001, 181 ETS (entered into force 1 July 2004)

Additional Protocol to the Convention on Human Rights and Biomedicine Concerning Biomedical Research, opened for signature 25 January 2005, 195 CETS (entered into force 1 September 2007)

Additional Protocol to the Convention on Human Rights and Biomedicine Concerning Genetic Testing for Health Purposes, opened for signature 27 November 2008, 203 CETS (entered into force 1 July 2018)

Charter on the Rights and Welfare of the Child, opened for signature 11 July 1990, OAU Doc CAB/LEG/24.9/49 (entered into force 29 November 1999)

AU Convention on Cybersecurity and Personal Data Protection Convention, opened for signature 27th June 2014, (not yet in force)

Charter of Fundamental Rights of the European Union, proclaimed on 7 December 2000, [2000] OJ C 326/393 (entered into force on 1 December 2009)

Charter of the United Nations (1945)

Convention Establishing the World Intellectual Property Organization, opened for signature 14 July 1967, (entered into force 1 June 1984) [as amended in 1979]

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, opened for signature 28 January 1981, ETS No. 108 (entered into force 1 October 1981)

Convention on Environmental Impact Assessment in a Transboundary Context, opened for signature 1 March 1991, 1989 UNTS 309 (entered into force 10 September 1997)

Convention on Human Rights and Bio-medicine, opened for signature 4 April 1997, 164 ETS (entered into force 1 December 1999)

Convention on the Rights of Persons with Disabilities, opened for signature 30 March 2007, 2515 UNTS 3 (entered into force 3 May 2008)

ILO Constitution (1919)

International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, opened for signature 18 December 1990, 2220 UNTS 3 (entered into force 1 July 2003)

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

International Covenant on Economic, Social and Cultural Rights, opened for signature 19 December 1966, 993 UNTS 3 (entered into force 3 January 1976)

Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data, opened for signature 10 October 2018, CETS No. 223 (not yet in force)

Optional Protocol to the CRC on the Sale of Children, Child Prostitution and Child Pornography, opened for signature 25 May 2000, 2171 UNTS 227 (entered into force 18 January 2002)

Statute of the International Court of Justice (18 April 1946)

Statute of the International Law Commission (21 November 1947)

Treaty of Lisbon, Amending the Treaty on EU and the Treaty Establishing the European Community, opened for signature 13 December 2007 [2007] OJ C 306/1 (entered into force 1 December 2009)

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, opened for signature 27 January 1967, 610 UNTS 205 (entered into force 10 October 1967)

UNESCO Constitution (16 November 1945) (as amended)

D Legislation/Constitution

Basic Law of the Federal Republic of Germany (1949) (as amended in 2014)

Brazilian Civil Framework for the Internet (2014)

Constitution of Ecuador (2008) (as amended)

Constitution of Mexico (1917) (as amended)

Directive (EC) 2002/58 of the European Parliament and of the Council of 12 July 2002 on the Protection of Privacy in the Electronic Communications Sector [2002] OJ L 201/37

Directive (EU) 2016/680 of the European Parliament and of Council of 27 April 2016 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 Offenses or the Execution of Criminal Penalties and on the Free Movement of such Data [2016] OJ L 119/89

FREEDOM Act of 2015, Pub L No 114-23, 129 Stat 268

Nigerian Digital Rights and Freedoms Bill (2016)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data [2016] OJ L 119/1

Regulation (EU) 2018/1725 of the European Parliament and of Council of 23 October 2018 on the Protection of Natural Persons with regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices and Agencies and on the Free Movement of such Data [2018] OJ L 295/39

The Australian Privacy Act 1988 (Cth)

US Presidential Policy Directive 28: Signals Intelligence Activities (17 January 2018)

E International Soft Law

‘African Declaration of Internet Rights and Freedoms’ (2014)

‘APEC Privacy Framework’ (2004)

‘Charter of Digital Fundamental Rights of the European Union’ (2016)

‘Charter of Human Rights and Principles for the Internet’ (5th ed, 2018)

‘Code of Practice on the Protection of Workers’ Personal Data’ (ILO, 1997)

‘Data Protection Manual’ (IOM, 2009)

‘Directive on Information Disclosure’ (WFP, 2010)

‘Global Principles on the Protection of Freedom of Expression and Privacy’ (Article 19, 2017)

Guidelines for the Alternative Care of Children, GA Res 64/142, 64th sess, UN Doc A/Res/64/142 (24 February 2010)

‘Information Disclosure Policy’ (UNDP, 1996) (as amended in 2017)

‘Information/Document Access Policy’ (ITU, 2016)

‘International Declaration on Information and Democracy’ (Reporters Without Borders, 2018)

‘Italian Declaration of Internet Rights’ (2015)

‘Joint Proposal for a Draft of International Standards on the Protection of Privacy and Personal Data: The Madrid Resolution’ (November 2009)

‘Madrid Privacy Declaration’ (3 November 2009)

‘Montreux Declaration: The Protection of Personal Data and Privacy in A Globalized World – A Universal Right Respecting Diversities’ (International Conference of Privacy and Data Protection Commissioners, Montreux, Switzerland, 2005)

‘Policy on the Protection of Personal Data of Persons of Concern to the UNHCR’ (The UN Refugee Agency, May 2015)

‘Principles on Freedom of Expression and Privacy’ (Global Network Initiative, 2008)

‘Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights’ (American Association for the International Commission of Jurists, 1988)

‘The Geneva Declaration of Principles’ (WSIS, 12 December 2003)

‘The Geneva Plan of Action’ (WSIS, 12 December 2003)

‘The Helsinki Final Act: Conference on Security and Cooperation in Europe Final Act’ (OSCE in Europe, 1 August 1975)

‘The Tunis Agenda for the Information Society’ (WSIS, 18 November 2005)

‘Universal Declaration of Digital Rights’ (Article 19, 2017)

Committee on the Rights of the Child, General Comment 3: HIV/AIDS and the Rights of the Child, 32 sess, UN Doc CRC/GC/2003/1 (17 March 2003)

Declaration of Legal Principles Governing the Activities of States in the Exploration and Uses of the Outer Space, GA Res 1962 (XVIII), 18th sess, Agenda item 28a, UN Doc A/Res/18/1962 (13 December 1963)

Declaration on the Elimination of All Forms of Intolerance and of Discrimination Based on Religion or Belief, GA Res 36/55, 93rd plenary mtg, UN Doc A/RES/42/97 (25 November 1981)

Declaration on the Elimination of Violence against Women, GA Res 48/104, 85th plenary mtg, UN Doc A/RES/48/104 (20 December 1993)

Declaration on the Granting of Independence to Colonial Countries and Peoples, GA Res 1514 (XV), 15th sess, UN Doc A/RES/1514(XV) (14 December 1960)

Declaration on the Rights of Persons Belonging to National or Ethnic, Religious and Linguistic Minorities, GA Res 47/135, 92nd plenary mtg, UN Doc A/RES/47/135 (18 December 1992)

Declaration on the Use of Scientific and Technological Progress in the Interest of Peace and for the Benefit of Mankind, GA Res 3384 (XXX), 2400th plenary mtg, UN Doc A/RES/3384(XXX) (10 November 1975)

Draft Recommendation on the Protection and Use of Health-Related Data (Mandate of the United Nations Special Rapporteur on the Right to Privacy – Task Force on Privacy and the Protection of Health-Related Data, June 2019).

Elaboration of an International Legally Binding Instrument on Transnational Corporations and other Business Enterprises with respect to Human rights, HRC Res 26/9, 26thsess, Agenda item 3, UN Doc A/HRC/RES/26/9 (14 July 2014)

Forum on Minority Issues, HRC Res 19/23, 19thsess, Agenda item 5, UN Doc A/HRC/RES/19/23 (10 April 2012)

Forum on Minority Issues, HRC Res 6/15, 6thsess, 21st mtg UN Doc A/HRC/RES/6/15 (28 September 2007)

Fundamental Principles of Official Statistics, GA Res 68/261, 68thsess, Agenda item 9, UN Doc A/RES/68/261 (29 January 2014)

Guidelines for the Regulation of Computerized Personal Data Files, GA Res 45/95, UNGAOR, 45thsess, 68thplen mtg, UN Doc A/Res/45/95 (14 December 1990)

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 23 September 1980) (as updated in 2013)

Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework, 17thsess, Agenda item 3, UN Doc A/HRC/RES/17/4 (6 June 2011)

Human Rights and Scientific and Technological Developments, GA Res 2450 (XXIII), 1748th plenary mtg, UN Doc A/RES/2450(XXIII) (19 December 1968)

Human Rights and Scientific and Technological Developments, GA Res 3149 (XXVIII), 2201st plenary mtg, UN Doc RES/3149(XXVIII) (14 December 1973)

Human Rights and Scientific and Technological Developments, Resolution XI, adopted at the Teheran Conference, 25th plenary mtg (12 May 1968)

Human Rights and the Follow-up to the Guidelines for the Regulation of Computerized Personal Data Files, Commission on Human Rights Decision 1997/122 (16 April 1997)

Human Rights and the Follow-up to the Guidelines for the Regulation of Computerized Personal Data Files, Commission on Human Rights Decision 1999/109 (28 April 1999)

Human Rights and Transnational Corporations and Other Business Enterprises, HRC Res 14/4 17thsess, Agenda item 3, UN Doc A/HRC/RES/17/4 (6 July 2011)

Human Rights and Transnational Corporations and other Business Enterprises, HRC Res 17/4, 17thsess, Agenda Item 3, UN Doc A/HRC/RES/17/4 (16 June 2011)

HR Committee, *General Comment 16: Art 17 (Right to Privacy): The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 32ndsess, UN Doc HRI/GEN/1/Rev.9 (Vol. I) (8 April 1988)

HR Committee, *General Comment 34: Art 19: Freedom of Opinion and Expression*, 102ndsess, UN Doc CCPR/C/GC/34 12 (September 2011)

HR Committee, *General Comment 35: Article 19 (Liberty and Security of Person)*, 112thsess, UN Doc CCPR/C/GC/35 (16 December 2014)

HR Committee, *General Comment No. 31: Nature of Legal Obligation Imposed on State Parties to the Covenant* 80thsess, UN Doc CCPR/C/21/Rev.1/Add.13 (26 May 2004)

Human Rights Council, GA Res 60/251, 60thsess, Agenda items 46 and 120, UN Doc A/RES/60/251 (3 April 2006)

Institution Building of the United Nations Human Rights Council, HRC Res 5/1, 5thsess, 9th mtg, UN Doc A/HRC/RES/5/1 (18 June 2007)

International Co-operation in the Peaceful Uses of Outer Space, GA Res 1721 (XVI)A-E, 1085th plenary mtg, UN Doc RES/1721(XVI) (20 December 1961)

Nigeria: Draft Resolution in Annex to the Final Act of the Teheran Conference on Human Rights UN Doc A/CONF.32/C.2/L.28 (May 1968)

Panel on the Right to Privacy in the Digital Age, Decision 25/117, 25thsess, Agenda item 3, UN Doc A/HRC/DEC/25/117 (27 March 2014)

‘Personal Data Protection and Privacy Principles’ (UN High-Level Committee on Management, 11 October 2018).

Question of the Follow-up to the Guidelines for the Regulation of Computerized Personal Data Files, Commission on Human Rights Decision 1995/114 (8 March 1995)

Question of the Follow-up to the Guidelines for the Regulation of Computerized Personal Data Files: Report of the Secretary General prepared Pursuant to Commission Decision 1997/122 (18 November 1998)

Right to Petition, GA Res 217 B(III), UNGAOR, 3rdsess, 183rdplen mtg, UN Doc A/810 (10 December 1948)

Rights of the Child: Information and Communications Technologies and Child Sexual Exploitation, HRC Res 31/7, 31stsess, Agenda Item 3, UN Doc A/HRC/RES/31/7 (23 March 2016)

'Rules of Procedure of the Human Rights Committee' (9 January 2019)

Sub-Commission on the Promotion and Protection of Human Rights, *Norms and Responsibilities of Transnational Corporations and other Business Enterprises with regard to Human Rights*, UN ESCOR, 55thsess, 22nd mtg, Agenda item 4, UN Doc E/CN.4/Sub.2/2003/12/Rev.2 (13 August 2003)

The Proclamation of Teheran, UN Doc A/CONF.32/41 (13 May 1968)

The Promotion, Protection and Enjoyment of Human Rights on the Internet, HRC Res 38/7, 38thsess, Agenda item 3, UN Doc A/HRC/38/L.10/Rev.1 (5 July 2018)

The Right to Freedom of Information and Expression on the Internet in Africa, ACHPR Res. 362(LIX)2016 (4 November 2016)

The Right to Privacy in the Digital Age, 69thsess, Agenda item 68(b), UN Doc A/RES/69/166 (18 December 2014)

The Right to Privacy in the Digital Age, GA Res 68/167, 60thsess, Agenda item 69(b), UN Doc A/RES/68/167 (18 December 2013)

The Right to Privacy in the Digital Age, GA Res 71/199, 70thsess, Agenda item 68(b), UN Doc A/RES/71/199 (19 December 2016)

The Right to Privacy in the Digital Age, GA Res 73/179, 73rdsess, Agenda item 74(b), UN Doc A/RES/73/179 (17 December 2018)

The Right to Privacy in the Digital Age, HRC Res 28/16, 28thsess, Agenda item 3, UN Doc A/HRC/RES/28/16 (26 March 2015)

The Right to Privacy in the Digital Age, HRC Res 34/7, 34thsess, Agenda item 3, UN Doc A/HRC/RES/34/7 (23 March 2017)

The Right to Privacy in the Digital Age, Res 37/2, 37thsess, Agenda item 3, UN Doc A/HRC/RES/37/2 (22 March 2018)

The Situation with regard to the Implementation of the Declaration on the Granting of Independence to Colonial Countries and Peoples, GA Res 1654 (XVI), 1066th plenary mtg (27 November 1961)

The United Nations Declaration on the Rights of Indigenous Peoples, GA Res 61/295, 61stsess Agenda item 68, UN Doc A/61/295 (2 October 2007)

The Use of Scientific and Technological Developments in the Interest of Peace and Social Development, GA Res 3150 (XXVIII), 2201st plenary mtg, UN Doc RES/3150 (XXVIII) (14 December 1973)

UN Guidelines for Consumer Protection, GA Res 70/186, 70thsess, Agenda item 18(a), UN Doc A/RES/70/186 (4 February 2016)

UN Principles and Guidelines on Access to Legal Aid in Criminal Justice Systems, GA Res 67/187, 60th plenary mtg, UN Doc A/RES/67/187 (20 December 2012)

UN Rules for the Protection of Juveniles Deprived of their Liberty (Havana Rules), GA 45/113, 68th plenary mtg, UN Doc A/RES/45/113 (14 December 1990)

UN Standard Minimum Rules for the Treatment of Prisoners (Nelson Mandela Rules), GA Res 70/175, 70thsess, Agenda item 106, UN Doc A/RES/70/175 (17 December 2015)

United Nations Guidelines for the Prevention of Juvenile Delinquency (Riyadh Guidelines), GA Res 45/112, 68th plenary mtg, UN Doc A/RES/45/112 (14 December 1990)

United Nations Millennium Declaration, GA Res 55/2, 55thsess, Agenda item 60(b) (8 September 2000)

Universal Declaration of Human Rights, GA Res 217A(III), UN GAOR, 3rdsess, 183rdplen mtg, UN Doc A/810 (10 December 1948)

Universal Declaration on Bio-ethics and Human Right (UNESCO, 19 October 2005)

F Cases

Barbulescu v Romania (ECtHR, Application No. 61496/08, 5 September 2017)

Big Brother Watch and Others v UK (ECtHR, Application Nos. 58170/13, 62322/14 and 24960/15, 13 September 2018)

Bundesverfassungsgericht (1983) *BVerfGE* 65

Bundesverfassungsgericht (2008) BVerfG 822

Chapman v The United Kingdom (ECtHR, Application No. 27238/95, 18 January 2001)

Digital Rights Ireland and Stetinger et alv Minister for Communication and et al (C-293/12 and C-594/12) [2014] ECLI 238

Ekimdzhev v Bulgaria (ECtHR, Application No. 62540/00, 28 June 2007)

Golder v The United Kingdom (ECtHR, Application No. 4451/70, 21 February 1975)

Google v Agencia Española de Protección de Datos (AEPD) v Mario Costeja González (C-131/12) [2014] ECLI 317

Hamalainen v Finland (ECtHR, Application No. 37359/09, 16 July 2014)

HR Committee, *A.B. v Canada* (Communication No. 2387/2014, 16 March 2017)

HR Committee, *Al-Gertani v Bosnia and Herzegovina* (Communication No. 1955/2010, 6 November 2013)

HR Committee, *Antonius Cornelis Van Hulst v The Netherlands* (Communication No.903/1999, 15 November 2004)

HR Committee, *D.T. v Canada* (Communication No. 2081/2011, 29 September 2016)

HR Committee, *Dušan Vojnović v Croatia* (Communication No. 1510/2006, 30 March 2009)

HR Committee, *H.S. v Australia* (Communication No. 2015/2010, 13 May 2015)

HR Committee, *Herbert Potter v New Zealand* (Communication No. 632/1995, 6 April 1995)

HR Committee, *I Elpida v Greece* (Communication No. 2242/2013, 26 February 2014)

HR Committee, *I.P. v Finland* (Communication No. 450/1991, 26 July 1993)

HR Committee, *Kalamiotis et al v Greece* (Communication No. 2242/2013, 3 January 2017)

HR Committee, *Marouf v Algeria* (Communication No. 1889/2009, 29 April 2014)

HR Committee, *N.K. v The Netherlands* (Communications No. 2326/2013, 10 January 2018)

HR Committee, *Nabil Sayadi and Patricia Vinck v Belgium* (Communication No. 1472/2006, 29 December 2008)

Karako v Hungary (ECtHR, Application No. 39311/05, 28 April 2009)

L.H. v Latvia (ECtHR, Application No. 52019/07, 29 April 2014)

Leander v Sweden (ECtHR, Application No 9248/81, 26 March 1987)

Legal Consequences for States of the Continued Presence of South Africa in Namibia (Advisory Opinion) [1971] ICJ Reports 16

Malone v UK (ECtHR, Application No. 8691/79, 26 April 1985)

Petr Gatilov v Russia (ECtHR, Communication No. 2171/2012, 30 August 2017)

Rachwalski and Ferenc v Poland (Application No. 47709/99, 28 July 2009)

Roman Zakharov v Russia, (ECtHR, Application No. 47143/06, 4 December 2015)

S and Marper v UK (ECtHR, Application Nos. 30562/04 & 30566/04, 4 December 2008)

South West Africa (Ethiopia v South Africa) [1962] ICJ Reports 319

STC 292/2000, de 30 de noviembre de 2000 del Tribunal Constitucional

Szabo and Vissy v Hungary (ECtHR, Application No. 37138/14, 12 January 2016)

Uner v The Netherlands (ECtHR, Application No. 46410/99, 18 October 2006)

Uzun v Germany (ECtHR, Application No. 35623/05, 2 September 2010)

G Reports

‘A Concerning State of Play for the Right to Privacy in Europe: National Data Retention Laws Since CJEU’s Tele-2/Watson Judgment’ (Privacy International, September 2017)

‘A World That Counts: Mobilizing the Data Revolution for Sustainable Development’ (Report Prepared at the Request of the UN Secretary General by the Independent Expert Advisory Group on a Data Revolution for Sustainable Development, November 2014)

‘Annex D: Protection of Personal Data in Transborder Flow of Information’ (Report on the Work of the International Law Commission, 58th sess, May-August 2006)

‘Australia: Addendum to the Report of the UPR Working Group’ (29 February 2016)

‘Australia: Report of the UPR Working Group’ (13 January 2016)

Commentary of the Working Group on Minorities to the United Declaration on the Rights of Persons Belonging to National or Ethnic, Religious and Linguistic Minorities, UN Doc E/CN.4/Sub.2/AC.5/2005/2 (4 April 2005)

‘Draft Report on the Proposed e-Privacy Regulation’ (Committee on Civil Liberties, Justice and Home Affairs, 2017/0003(COD), 9 June 2017)

‘Encryption: A Matter of Human Rights’ (Amnesty International, 2016)

‘Global Network Initiative: 2015 Annual Report’ (2015)

‘Guide on Art 8 of the European Convention on Human Rights: Right to Respect for Private and Family’ (Council of Europe, April 2017)

‘India: Report of the UPR Working Group’ (17 July 2017)

‘Preparatory Work on Art 8 of the European Convention on Human Rights’ (DH [56] 12, 1956)

‘Privacy and Freedom of Expression in the Age of Artificial Intelligence’ (Privacy International, April 2018)

‘Privacy in the Digital Age: A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights’ (ACLU, March 2014)

‘Report of the Dynamic Coalition for Internet Rights and Principles’ (2015)

‘The IRP Charter of Human Rights and Principles for the Internet: Five Years On’ (IRP Coalition Meeting Report: IGF 2014 Istanbul, 4 September 2014)

‘United States of America: Addendum to the Report of the UPR Working Group’ (14 September 2015)

Annual Report of the Human Rights Committee to the General Assembly, UN GAOR 70thsess, UN Doc A/70/40 (April 2015)

Annual Report of the Human Rights Committee to the General Assembly, UN GAOR, 72ndsess, UN Doc A/72/40 (March 2017)

Cannataci, Joseph et al, ‘Privacy, Free Expression and Transparency: Redefining their New Boundaries in the Digital Age’ (UNESCO Series on Internet Freedom, 2016)

Concept Paper on the High Commissioner’s Proposal for a Unified Standing Treaty Body, UN Doc HRI/MC/2006/2 (22 March 2006)

Existing and Proposed Texts which could be used in the Drafting of a Further International Instrument on Human Rights and Scientific and Technological Developments, Commission on Human Rights, 33rdsess, Item 8 of provisional agenda, UN Doc E/CN.4/1233 (16 December 1976)

In Larger Freedom: Towards Development, Security and Human Rights for All, Report of the UN Secretary General, UN Doc A/59/2005 (21 March 2005)

Pillay, Navanethem, ‘Strengthening the United Nations Human Rights Treaty Body System: A Report by the United Nations High Commissioner for Human Rights’ (June 2012)

Report of High Commissioner for Human Rights: The Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018)

Report of Special Rapporteur of the UN Sub-Commission on Prevention of Discrimination and Protection of Minorities, Francesco Capotorti, UN Doc E/CN.4/Sub.2/384/Add.5 (28 June 1977)

Report of Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Freedom of Expression, David Kaye, UN Doc A/HRC/29/32 (22 May 2015)

Report of Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Freedom of Expression, David Kaye, UN Doc A/HRC/32/38 (11 May 2016)

Report of Special Rapporteur on the Right to Privacy, Joe Cannataci, UN Doc A/HRC/31/64 (8 March 2016)

Report of the High Commissioner for Human Rights: The Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (30 June 2014)

Report of the Secretary-General, Respect for the Privacy of Individuals and Integrity and Sovereignty of Nations in the Light of Advances in Recording and Other Techniques, UN Doc E/CN.4/1116 (23 January 1973)

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin, UN Doc A/HRC/13/37 (28 December 2009)

Report of the Special Rapporteur on the Promotion and Protection of Human Rights while Countering Terrorism, Ben Emerson, UN Doc A/69/397 (23 September 2014)

Report of the Special Rapporteur on the Right to Privacy, Joseph Cannataci, UN Doc A/HRC/37/62 (28 February 2018)

Report of the Special Rapporteur on the Right to Privacy, Joseph Cannataci, UN Doc A/72/43103 (19 October 2017)

Report of the Special Rapporteur on the Right to Privacy, Joseph Cannataci, UN Doc A/71/368 (30 August 2016)

Report of the Working Group on the Issue of Human Rights and Transnational Corporations and other Business Enterprises, UN Doc A/71/291 (4 August 2016)

Report of the Working Group on the Issue of Human Rights and Transnational Corporations and other Business Enterprises, UN Doc A/HRC/26/25 (5 May 2014)

Report on the Second Session of the Open-ended Intergovernmental Working Group on Transnational Corporations and other Business Enterprises with respect to Human Rights, UN Doc A/HRC/34/47 (4 January 2017)

Report on the Third Session of the Open-ended Intergovernmental Working Group on Transnational Corporations and other Business Enterprises with Respect to Human Rights, UN Doc A/HRC/37/67 (24 January 2018)

The Road to Dignity by 2030: Ending Poverty, Transforming All Lives and Protecting the Planet, Synthesis Report of the UN Secretary-General on the Post-2015 Agenda, UN Doc A/69/700 (December 2014)

Use of the Terms "Declaration" and "Recommendation", Memorandum by the Office of Legal Affairs, UN Doc E/CN.4/L.610 (2 April 1962)

Uses of Electronics which may Affect the Rights of the Person and the Limits which Should be Placed on such Uses in a Democratic Society, Report of the UN Secretary-General UN Doc E/CN.4/1142 (31 January 1974)

Vilanova, Pere, 'The Right to Privacy in the Case Law of the ECtHR' (Proceedings of the High-Level Seminar on International Case Law in Bioethics: Insight and Foresight, 2016)

H Other Sources

'Address Delivered by the Secretary-General of the United Nations, U Thant, at the Commemoration of the Twentieth Anniversary of the Adoption of the Universal Declaration of Human Rights' (Teheran, Islamic Republic of Iran, 22 April 1968)

'An Inclusive Dialogue for the Internet Bill of Rights in Guatemala' (Web We Want Foundation, 27 January 2017) <<http://ow.ly/hvMx30c7zdC>>

'Change Britain's Future: Liberal Democrat Manifesto' (2017)

'Comments of the HR Committee: Russian Federation' (26 July 1995)

'Concluding Observation of the HR Committee: Italy' (1 May 2017)

'Concluding Observations of the HR Committee: Bulgaria' (19 August 2011)

'Concluding Observations of the HR Committee: France' (13 July 2008)

'Concluding Observations of the HR Committee: France' (17 August 2015)

'Concluding Observations of the HR Committee: Hungary' (16 November 2010)

‘Concluding Observations of the HR Committee: Jamaica’ (19 November 1997)

‘Concluding Observations of the HR Committee: New Zealand’ (28 April 2016)

‘Concluding Observations of the HR Committee: Poland’ (29 July 1999)

‘Concluding Observations of the HR Committee: Poland’ (31 October 2016)

‘Concluding Observations of the HR Committee: Sweden’ (2 April 2009)

‘Concluding Observations of the HR Committee: The Netherlands’ (25 August 2009)

‘Concluding Observations of the HR Committee: The United Kingdom of Great Britain and Northern Ireland’ (17 August 2015)

‘Concluding Observations of the HR Committee: The United States of America’ (23 April 2014)

‘Data Revolution Advisory Group Named by UN Secretary General’ (UN Media Release, 29 August 2014) <<http://bit.ly/2mycqzs>>

‘Elements of the Draft Legally Binding Instrument on Transnational Corporations and Other Business Enterprises with respect to Human Rights’ (September 2017) <<https://bit.ly/2fF5crq>>

‘European Parliament Recommendation to the Council on Strengthening Security and Fundamental Freedoms on the Internet [2008/2160(INI)]’ (EU, 26 March 2009)

‘Explanatory Memorandum Privacy Bill 1988’ (Cth) [1988]

‘Explanatory Memorandum Privacy (Private Sector) Amendment Bill 2000’ (Cth)

‘Forward, Together: Our Plan for Stronger Britain and a Prosperous Future’ (The Conservative and Unionist Party Manifesto, 2017)

‘Gareth Hughes MP: Government Must Do More to Close the Digital Divide’ (The Green Party of New Zealand, 3 February 2015)

‘Google: Framework for Responsible Data Protection Regulation’ (September 2018) <<https://bit.ly/2DoNt5m>>

‘How Private Are Your Messaging Apps?’ (Amnesty International, 3 November 2016) <<https://bit.ly/2HnJ4y7>>

‘Joint Declaration (of the Minister of Culture of Brazil and Undersecretary of Communication of Italy) on Internet Rights’ (The Second Internet Governance Forum, Rio de Janeiro, 12-15 November 2007) <<https://bit.ly/2qiWvuI>>

‘Launch of the Philippine Declaration on Internet Rights and Principles’ (Foundation for Media Alternatives, September 2015) <<http://104.236.169.13/FMA/?p=416>>

‘Legally Binding Instrument to Regulate, in International Human Rights Law, the Activities of the Transnational Corporations and Other Business Enterprises’ (Zero Draft, 16 July 2018) available at <<https://bit.ly/2Ly1nT0>>

‘Letter from David Bethlehem, Legal Advisor to UK’s Foreign and Commonwealth Office, to John Ruggie, Special Representative of the Secretary General on Human Rights and Transnational Businesses and Other Business Enterprises’ (9 July 2009)

‘New Zealand Must Respect Its International Human Rights Obligations’ (Privacy International, 2018)

‘Observation of the United States on General Comment 31 of the Human Rights Committee’ (December 2007)

‘Protecting Your Data Online with a Digital Rights Bill’ (Liberal Democrats, 11 April 2015)

‘Secret Global Surveillance Networks: Intelligence Sharing Between Governments’ (Privacy International, 2018)

‘Surveillance Technologies’ (EFF) <<https://bit.ly/1fFUph9>>

‘The Digital Democratic Manifesto’ (The Labour Party, August 2016)

‘The Snowden Treaty: A New International Treaty on the Right to Privacy, Protection Against Improper Surveillance and Protection of Whistle-blowers’ (September 2015) <<http://www.snowdentreaty.org/>>

‘The WTO and Internet Privacy’ (Fact and Fiction: Misunderstanding and Scare Stories) <<https://bit.ly/2P9arPD>>

'Toward a Social Compact for Digital Privacy and Security: Statement by the Global Commission on Internet Governance' (Chatham House, 2015)

'UN Budget Shortfalls Seriously Undermine the Work of the Human Rights Treaty Bodies' (OHCHR Press Release, 17 May 2019)

'UN Human Rights Committee Publishes New General Comment on the 'Right to Life'' (OHCHR Press Release, 1 November 2018) <<https://bit.ly/2P41uvm>>

'United States Response to OHCHR Questionnaire on the 'Right to Privacy in the Digital Age' (2014) available at <<https://bit.ly/1FNq6r4>>

Alexander, Adam, 'Digital Surveillance 'worse than Orwell', says new UN Privacy Chief', *The Guardian* (Online), 25 August 2015 <<http://bit.ly/2h2bEYF>>

Anderson, Nate, 'New Internet Bill of Rights Contender Comes from...Pirates?', *Arts Technica* (Online), (12 December 2012) <<http://bit.ly/2iv6SDg>>

Apple-FBI Case Could Have Serious Global Ramifications for Human Rights: Zeid' (Office of the High Commissioner Press Release, 4 March 2016) <<https://bit.ly/2H7vX4x>>

Benedek, Wolfgang et al, 'The Humanization of Internet Governance: A Roadmap Towards a Comprehensive Global (Human) Rights Architecture for the Internet' (Paper presented at the 3rd Annual GigaNet Symposium, Hyderabad, India 2 December 2008)

Brandsom, Russell, 'Tim Cook Wants a Federal Privacy Law — but so do Facebook and Google', *The Verge* (online), 24 October 2018 <<https://bit.ly/2qaAYSg>>

Brown, Ian et al, 'Towards Multilateral Standards for Surveillance Reforms' (Oxford Internet Institute Discussion Paper, 2015)

Bukovska, Barbora and Niels ten Oever, '#InternetofRights: Creating the Universal Declaration of Digital Rights' on *Article 19 Blog* (24 March 2017) <<http://bit.ly/2q5wji2>>

Burgess, Matt, 'Tim Berners-Lee: 'We Need to Rethink the Web to Stop the Spread of Mean Ideas'', *Wired UK* (online), 11 April 2017 <<https://bit.ly/2oyapHE>>

DeNardis, Laura and Mark Raymond, 'Thinking Clearly About Multi-stakeholder Internet Governance' (Paper Submitted at the 8th Annual GigaNet symposium, Bali, Indonesia, 21 October 2013)

Drzemczewski, Andrew and Kanstantsin Dzehtsiarou, 'Painful Relations between the Council of Europe and Russia' on *EJIL: Talk!* (28 September 2018) <<https://bit.ly/2RTBfoD>>

Ekwealor, Victor, 'Nigeria's President Refused to Sign Its Digital Rights Bill, What Happens Now?', *Techpoint.africa* (online), 27 March 2019 <<https://bit.ly/2UZhGRG>>

Falcon, Ernesto and Jeremy Gillula, 'The Hypocrisy of AT&T's "Internet Bill of Rights"' (EFF, 1 February 2018) <<https://bit.ly/2qgTGY9>>

Ferrari, Elisabeth, 'Italy Issues a Declaration of Internet Rights – Now Let's Improve It' on *Center for Global Communication Studies Media Wire* (4 August 2015) <<https://bit.ly/2qqyLQB>>

Godwin, Mike, 'The Great Charter for Cambodian Internet Freedom' on *LinkedIn* (8 March 2015) <<https://bit.ly/2GEF2UR>>

Goodman, Ryann, 'Sociological Insights into International Human Rights Law' (Presented at the International Legal Theory Colloquium: Interpretation in International Law, NYU School of Law, 3 April 2008)

Greenleaf, Graham, 'The UN Should Adopt Data Protection Convention 108 as Global Treaty' (Law Research Series No 24, University of New South Wales, 2018)

Harper, Keith, 'Establishment of an HRC Mandate on Privacy Rights Comes at a Critical Time: Explanation of Position by the Delegation of the United States of America' (26 March 2015) <<http://bit.ly/2fHI53O>>

Hussain, Murtaza, "'Snowden Treaty' Calls for End to Mass Surveillance, Protections for Whistle-blowers', *The Intercept*, (25 September 2015) <<http://bit.ly/1OZZn3I>>

Kaye, David, 'Encryption and Anonymity Follow-up Report' (Research Paper 1/2018, June 2018)

Kingsbury, Benedict, 'Indigenous Peoples' in *Max Planck Encyclopedia of Public International Law* (2015)

Kiss, Jemima, 'An Online Magna Carta: Berners-Lee Calls for Bill of Rights for the Web', *The Guardian* (online), 12 March 2014, <<https://bit.ly/2wz93jL>>

Kleijssen, Jan, 'A Magna Carta for the Internet?' on *LinkedIn Pulse* (17 September 2014) <<http://bit.ly/2qtNTOH>>

Kleinwächter, Wolfgang 'Internet Governance Outlook 2014: Good News, Bad News, No News?' on *Circle ID* (31 December 2013) <<https://bit.ly/1k8uufl>>

Kulesza, Joanna, 'Protecting Human Rights Online: An Obligation of Due Diligence' (New York University School of Law Jean Monnet Working Paper No 24/14, 2014)

Leach, Philip, 'The Continuing Utility of International Human Rights Mechanisms?' on *EJIL: Talk!* (1 November 2017) <<http://bit.ly/2z9IEeu>>

McCarthy, Kieren, 'Dutch Govt Says No to Backdoors, Slides \$540k into OpenSSL Without Breaking Eye Contact', *The Register* (online), 4 January 2016 <<https://bit.ly/2EYKuNs>>

Opsahl, Kurt, 'A Bill of Rights for Social Network Users' (EFF, 19 May 2010) <<http://bit.ly/2s2PMFp>>

Peters, Anne, 'Surveillance Without Borders: The Unlawfulness of the NSA Panopticon – Part II' on *EJIL: Talk!* (4 November 2013) <<http://bit.ly/2vElrhK>>

Rampell, Catherine, 'Google Calls for International Standards on Internet Privacy', *The Washington Post* (online), (15 September 2007) <<http://wapo.st/2kXZAZz>>

Rodotà, Stephano, 'Towards a Declaration of Internet Rights' on *European Area of Freedom Security and Justice* (18 November 2014) <<https://bit.ly/2luWmxw>>

Rossini, Carolina et al, 'The Strength and Weaknesses of the Brazilian Internet Bill of Rights' (Chatham House, 2015)

Ruggie, John, 'Comments on the "Zero Draft" Treaty on Business and Human Rights' (Business and Human Rights Resource Center, August 2018) <<https://bit.ly/2DcDv75>>

Ruiz, Carlos, 'La Configuración Constitucional del Derecho a la Intimidad' (1992)

Scheinin, Martin, 'Privacy and Security can be Reconciled', *The Guardian* (online), (21 January 2010) <<https://bit.ly/2OmKY4C>>

Scheinin, Martin, 'Towards a World Court of Human Rights: Research Report within the Framework of the Swiss Initiative to Commemorate the 60th Anniversary of the Universal Declaration of Human Rights' (22 June 2009)

Seibert-Fohr, Anja, 'Digital Surveillance, Meta Data and Foreign Intelligence Cooperation: Unpacking the International Right to Privacy' (April 2018) <<https://bit.ly/2GSm3FP>>

Shany, Yuval, 'Online Surveillance in the Case Law of the Human Rights Committee' (The Hebrew University of Jerusalem Center for Cybersecurity Research, 13 July 2017) <<https://bit.ly/2MECR7m>>

Simoncini, Andrea, 'The Constitutional Dimensions of the Internet: Some Research Paths' (EUI Working Papers, LAW 2016/16, 2016)

Sinnreich, Aram, 'An International Approach to Data Privacy' (Policy Briefing Note, Center for Media and Social Impact, American University, August 2018)

'Special Rapporteur on the Right to Privacy Presents Draft Legal Instrument on Government-led Surveillance and Privacy' (February 2018), available at <<https://bit.ly/2ZcNe4Y>>

Stephenson, Randall, 'Consumers Need an Internet Bill of Rights' (AT&T Media Release, 24 January 2018) <<https://soc.att.com/2DHA7ki>>

Sumption, Lord, 'The limits of Law' (27th Sultan Azlan Shah Lecture, Kuala Lumpur, 20 November 2013)

'The Global Surveillance Industry' (Privacy International) <<https://bit.ly/2Isuqde>>

von Weizsäcker, Franz and Norman Schräpel, 'Why We Should Support the "European Charter of Digital Fundamental Rights"' on *Internet Policy Review Blog* (14 December 2016) <<http://bit.ly/2qBgl2N>>

Zittrain, Jonathan, 'A Bill of Rights for the Facebook Nation' on *The Chronicle of Higher Education* (20 April 2009) <<https://bit.ly/2Jj8gpq>>

Zuckerberg, Mark, 'The Internet Needs New Rules: Let's Start in Four Areas', *The Washington Post* (online), 30 March 2019 <<https://wapo.st/2uEbrTT>>

Zuckerberg, Mark, 'A Privacy-Focused Vision for Social Networking' *on Facebook*
(6 March 2019) <<https://bit.ly/2TmiQWv>>

APPENDICES

Appendix 1: The Italian Declaration of Internet Rights (July 2015)

Preamble

The Internet has played a decisive role in redefining public and private space, structuring relationships between people and between people and institutions. It has erased borders and has created new ways of generating and utilizing knowledge. It has expanded the scope for people to participate directly in the public domain. It has changed how people work. It has fostered the development of a more open and free society. The Internet must be treated as a global resource and must satisfy the criterion of universality.

The European Union is currently the world region with the greatest constitutional protection of personal data, which is explicitly enshrined in Article 8 of the EU Charter of Fundamental Rights. This serves as a necessary point of reference for specifying the principles governing the operation of the Internet, including from a global perspective.

This Declaration of Internet Rights is founded on the full recognition of the liberty, equality, dignity and unique diversity of each individual. Preserving these rights is crucial to ensuring the democratic functioning of institutions and avoiding the predominance of public and private powers that may lead to a society of surveillance, control and social selection.

The Internet is an increasingly important space for the self-organization of individuals and groups, and it is a vital tool for promoting individual and collective participation in democratic processes as well as substantive equality.

The principles underpinning this Declaration also take account of the function of the Internet as an economic space that enables innovation, fair competition and growth in a democratic context.

A Declaration of Internet Rights is crucial to laying the constitutional foundation for supranational principles and rights.

Art. 1

(Recognition and protection of rights)

1. The fundamental rights of every individual enshrined in the Universal Declaration of Human Rights of the United Nations, the Charter of Fundamental Rights of the European Union, national constitutions and other relevant international declarations shall be protected on the Internet.
2. These rights shall be interpreted so as to ensure their enforceability on the Internet.
3. The recognition of rights on the Internet shall be based on comprehensive respect for the dignity, freedom, equality and diversity of each individual, which constitute the underlying principles for balancing these with other rights.

Art. 2

(Right to Internet Access)

1. Access to the Internet is a fundamental right of all persons and a condition for their individual and social development.
2. Every person shall have the same right to access the Internet on equal terms, using appropriate and up-to-date technologies that remove all economic and social barriers.
3. The fundamental right to Internet access must be ensured with respect to its substantive prerequisites, not only as the mere possibility of connecting to the Internet.
4. Access shall include freedom of choice with regard to devices, operating systems, and applications, including distributed software.
5. Public institutions shall take the necessary measures to overcome all forms of digital divide, including those created by gender, economic condition or a situation of personal vulnerability or disability.

Art.3

(Right to online knowledge and education)

1. Public institutions shall ensure the creation, the use and the dissemination of online knowledge, construed as a good accessible to and usable by all.
2. The rights arising from the recognition of the moral and material interests connected with the production of knowledge shall be given due consideration.
3. Every person has the right to be placed in the condition to acquire and update the skills necessary to use the Internet in an informed manner for the exercise of his or her rights and fundamental freedoms.
4. Public institutions shall promote, especially through the educational and training system, the informed use of the Internet and shall take steps to eliminate any form of cultural lag that might preclude or limit the use of the Internet by any person.
5. The informed use of the Internet is an essential guarantee of the development of equal opportunities for individual and collective growth; the democratic rebalancing of disparities in power on the Internet between economic players, institutions and citizens; the prevention of discrimination and risky behavior as well as conduct detrimental to the freedoms of others.

Art. 4

(Net neutrality)

1. Every person has the right that the data he/she transmits and receives over the Internet be not subject to discrimination, restrictions or interference based upon the sender, recipient, type or content of the data, the device used, applications or, in general, the legitimate choices of individuals.
2. The right to neutral access to the Internet in its entirety is a necessary condition for the effectiveness of the fundamental rights of the person.

Art. 5
(Protection of personal data)

1. Everyone has the right to the protection of the data that concern them in order to ensure respect for their dignity, identity and privacy.
2. Such data consist of information that allows someone to trace the identity of a person and includes data pertaining to and generated by devices, as well as any data gathering and processing, such as that involved in the development of profiles.
3. Everyone has the right to access data that concern them, and to obtain the rectification or erasure of such data for legitimate reasons.
4. Data must be processed in accordance with the principles of necessity, purpose limitation, relevance, proportionality and, in any case, the right of every individual to informational self-determination shall prevail.
5. Data may be collected and processed only with the informed consent of the data subject or on the basis of another legitimate motivation enshrined in law. Consent shall in principle be revocable. With regard to the processing of sensitive data, the law may establish that the consent of the data subject must be accompanied by a specific authorization.
6. Consent does not constitute a legal basis for the processing of data when there is a significant imbalance of power between the data subject and the data processor.
7. Access to and processing of data for discriminatory purposes, whether directly or indirectly, is prohibited.

Art. 6
(The right to informational self-determination)

1. Every person has the right to access his or her data, irrespective of the data controller and the place where the data are stored, in order to request the supplementation, rectification or erasure of the data in the manner provided for by law. Every person has the right to know the technical procedures used in processing data that concern them.
2. Data may be collected and stored only for the length of time necessary, in any event respecting the principles of purpose limitation and proportionality and the right to self-determination of the data subject.

Art. 7

(Inviolability of electronic systems, devices and domiciles)

The IT systems and devices of every person and the freedom and confidentiality of their electronic information and communications are inviolable. Exceptions are possible only in the circumstances and in the manner established by law and with the reasoned authorization of the courts.

Art. 8

(Automated processing)

No act, judicial or administrative order or decision that could significantly impact the private sphere of individuals may be based solely on the automated processing of personal data undertaken in order to establish the profile or personality of the data subject.

Art. 9

(Right to one's identity)

1. Every person has a right to the complete and up-to-date representation of his or her identities on the Internet.
2. The definition of identity regards the free construction of personality and cannot take place without the intervention and the knowledge of the data subject.
3. The use of algorithms and probabilistic techniques shall be disclosed to the data subject who, in any case, has the right to oppose the construction and dissemination of profiles regarding him or her.
4. Every person has the right to provide only the information which is strictly necessary for complying with legal obligations, for the supply of goods and services or for accessing Internet platforms.
5. The attribution and management of digital identities by public institutions shall be governed by appropriate guarantees, especially with regard to security.

Art. 10
(Protection of anonymity)

1. Every person may access the Internet and communicate electronically using instruments, including technical systems, which protect their anonymity and prevent the collection of personal data, in particular with a view to exercising civil and political freedoms without being subject to discrimination or censorship.
2. Restrictions may be imposed only when they are based on the need to safeguard a major public interest and are necessary, proportional and grounded in law and in accordance with the basic features of a democratic society.
3. In the event of violations of the dignity and fundamental rights of any person, as well as in other cases provided for by the law, the courts may require the identification the author of a communication with a reasoned order.

Art. 11
(Right to be forgotten)

1. Every person has the right to obtain the removal from search engines of references to information that, due to their content or the time elapsed from the moment of collection, no longer have public relevance.
2. The right to be forgotten cannot restrict the freedom of search and the right of the public to be informed, which are necessary conditions for the functioning of a democratic society. This right may be exercised by public figures or those who hold public functions only if the data concerning them are irrelevant with regard to their activities or the public functions they perform.
3. Where a request to be removed from search engines is granted, any person may appeal the decision before the courts to ensure that the public interest in the information is preserved.

Art. 12

(Rights and safeguards of people on platforms)

1. Digital platform operators are required to behave with integrity and fairness in dealing with users, suppliers and competitors.
2. Every person has the right to receive clear and simple information on how the platform operates, not to have contractual terms arbitrarily altered and not to be subjected to conduct that could make accessing the platform difficult or discriminatory. Every person shall be in any case notified of changes in contractual terms. In this case, they have the right to terminate the relationship, to receive a copy of the data concerning them in interoperable form and to have the data concerning them removed from the platform.
3. Platforms that operate on the Internet, if they provide services essential to the lives and activities of people, shall ensure conditions – also in accordance with the principle of competition – for the appropriate interoperability, under equal contractual terms, of their main technologies, functions and data with other platforms.

Art. 13

(Network security)

1. Network security must be guaranteed in the public interest, ensuring infrastructure integrity and protection from attacks, and in the interest of individuals.
2. Restrictions on the freedom of expression are not permitted. The protection of the dignity of persons from abuses connected with such behavior as incitement to hate, discrimination and violence, shall be guaranteed.

Art. 14
(Internet governance)

1. Every person has the right to both national and international recognition of their rights.
2. The Internet requires rules consistent with its universal, supranational scope, aimed at fully implementing the principles and rights set out above, to safeguard its open and democratic nature, to prevent all forms of discrimination and to prevent the rules governing its use from being determined by those who hold the greatest economic power.
3. Internet rules shall take into account the various territorial levels (supranational, national, regional), the opportunities created by a variety of forms of self-regulation consistent with the above principles, the need to preserve the capacity for innovation, including through competition, as well as the manifold actors operating on the Internet, and shall encourage involvement in ways that ensure the widespread participation of all concerned. Public institutions shall adopt the appropriate instruments to ensure such participation.
4. In any case, the regulatory innovations regarding the Internet shall be subject to an assessment of their impact on the digital ecosystem.
5. The Internet shall be managed so as to ensure compliance with the principle of transparency, accountability for decisions, accessibility to public information, and the representation of those concerned.
6. Access to and the reuse of data generated and held by the public sector shall be ensured.
7. The establishment of national and international authorities is essential to effectively ensure observance of the above criteria, including through an evaluation of the compliance of the new rules with the principles of this Declaration.



General Assembly

Distr.: General
21 January 2019

Seventy-third session
Agenda item 74 (b)

Appendix 2: Resolution adopted by the General Assembly on 17 December 2018

[on the report of the Third Committee ([A/73/589/Add.2](#))]

73/179. The right to privacy in the digital age

The General Assembly,

Reaffirming the purposes and principles of the Charter of the United Nations, the human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights¹ and relevant international human rights treaties, including the International Covenant on Civil and Political Rights² and the International Covenant on Economic, Social and Cultural Rights,² as well as the Vienna Declaration and Programme of Action,³

Recalling General Assembly resolutions [68/167](#) of 18 December 2013, [69/166](#) of 18 December 2014 and [71/199](#) of 19 December 2016 on the right to privacy in the digital age, and resolution [45/95](#) of 14 December 1990 on guidelines for the regulation of computerized personal data files, as well as Human Rights Council resolutions 28/16 of 26 March 2015⁴ and 34/7 of 23 March 2017⁵ on the right to privacy in the digital age and resolutions 32/13 of 1 July 2016⁶ and 38/7 of 5 July 2018⁷ on the promotion, protection and enjoyment of human rights on the Internet,

Recalling also the outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society,⁸

¹ Resolution 217 A (III).

² See resolution 2200 A (XXI), annex.

³ [A/CONF.157/24 \(Part I\)](#), chap. III.

⁴ See *Official Records of the General Assembly, Seventieth Session, Supplement No. 53 (A/70/53)*, chap. III, sect. A.

⁵ Ibid., *Seventy-second Session, Supplement No. 53 (A/72/53)*, chap. IV, sect. A.

⁶ Ibid., *Seventy-first Session, Supplement No. 53 (A/71/53)*, chap. V, sect. A.

⁷ Ibid., *Seventy-third Session, Supplement No. 53 (A/73/53)*, chap. VI, sect. A.

⁸ Resolution [70/125](#).



Taking note of the reports of the Special Rapporteur of the Human Rights Council on the right to privacy⁹ and the reports of the Special Rapporteur of the Human Rights Council on the promotion and protection of the right to freedom of opinion and expression,¹⁰

Welcoming the work of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, noting with interest the report of the High Commissioner thereon,¹¹ and recalling the panel discussion on the right to privacy in the digital age held during the twenty-seventh session of the Human Rights Council,

Noting that the rapid pace of technological development enables individuals all over the world to use new information and communications technologies and at the same time enhances the capacity of Governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and is therefore an issue of increasing concern,

Noting also that violations and abuses of the right to privacy in the digital age may affect all individuals, with particular effects on women, as well as children and those who are vulnerable and marginalized,

Recognizing that the promotion of and respect for the right to privacy are important to the prevention of violence, including gender-based violence, abuse and sexual harassment, in particular against women and children, which can occur in digital and online spaces and includes cyberbullying and cyberstalking,

Reaffirming the human right to privacy, according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference, and recognizing that the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference and the right to freedom of peaceful assembly and association, and is one of the foundations of a democratic society,

Noting with appreciation general comment No. 16 of the Human Rights Committee on article 17 of the International Covenant on Civil and Political Rights, on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation,¹² while also noting the vast technological leaps that have taken place since its adoption and the need to discuss the right to privacy in view of the challenges of the digital age,

Recognizing the need to further discuss and analyse, based on international human rights law, issues relating to the promotion and protection of the right to privacy in the digital age, procedural safeguards, effective domestic oversight and remedies, the impact of surveillance on the right to privacy and other human rights, as well as the need to examine the principles of non-arbitrariness, lawfulness, legality, necessity and proportionality in relation to surveillance practices,

Noting the holding of the Global Multi-stakeholder Meeting on the Future of Internet Governance (NETmundial) and the multi-stakeholder discussions that take place annually in the Internet Governance Forum, which is a multi-stakeholder forum

⁹ [A/HRC/34/60](#) and [A/72/540](#).

¹⁰ [A/HRC/38/35](#) and [A/73/348](#).

¹¹ [A/HRC/39/29](#).

¹² *Official Records of the General Assembly, Forty-third Session, Supplement No. 40 (A/43/40)*, annex VI.

for discussions of Internet governance issues and whose mandate was extended by the General Assembly in 2015 for another 10 years,⁸ and recognizing that effectively addressing the challenges relating to the right to privacy in the context of modern communications technology requires an ongoing, concerted multi-stakeholder engagement,

Emphasizing that the protection and promotion of, and respect for, the right to privacy benefit from sustained engagement, including through informal dialogues, among all stakeholders, including States, business enterprises, international organizations and civil society,

Recognizing that the discussion on the right to privacy should be based upon existing international and domestic legal obligations, including international human rights law, as well as relevant commitments, and should not open the path for undue interference with an individual's human rights,

Stressing the importance of full respect for the freedom to seek, receive and impart information, including the fundamental importance of access to information and democratic participation,

Recognizing that the right to privacy is important for the enjoyment of other rights and can contribute to an individual's ability to participate in political, economic, social and cultural life, and noting with concern that violations or abuses of the right to be free from unlawful or arbitrary interference with the right to privacy might affect the enjoyment of other human rights, including the right to freedom of expression and to hold opinions without interference, and the right to peaceful assembly and freedom of association,

Noting that, while metadata may provide benefits, certain types of metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of communications and can give an insight into an individual's behaviour, social relationships, private preferences and identity,

Expressing concern that individuals often do not and/or cannot provide their free, explicit and informed consent to the sale or multiple resale of their personal data, as the collecting, processing, use, storage and sharing of personal data, including sensitive data, have increased significantly in the digital age,

Noting with concern that profiling, automated decision-making and machine-learning technologies, sometimes referred to as artificial intelligence, without proper safeguards, may lead to decisions that have the potential to affect the enjoyment of human rights, including economic, social and cultural rights, and recognizing the need to apply international human rights law in the design, evaluation and regulation of these practices,

Emphasizing that unlawful or arbitrary surveillance and/or interception of communications, as well as the unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the right to privacy, can interfere with the right to freedom of expression and may contradict the tenets of a democratic society, including when undertaken extraterritorially or on a mass scale,

Recognizing that the same rights that people have offline must also be protected online, including the right to privacy,

Noting in particular that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that any interference with the right to privacy must not be arbitrary or unlawful, bearing in mind what is reasonable with regard to the pursuance of legitimate aims, and recalling that States that are parties to

the International Covenant on Civil and Political Rights must take the necessary steps to adopt laws or other measures as may be necessary to give effect to the rights recognized in the Covenant,

Expressing concern about the spread of disinformation and propaganda, including on the Internet, which can be designed and implemented so as to mislead, to violate human rights, including the right to privacy and to freedom of expression, and to incite violence, hatred, discrimination or hostility, and emphasizes the important contribution of journalists in countering this trend,

Emphasizing that States must respect international human rights obligations regarding the right to privacy when they intercept digital communications of individuals and/or collect personal data, when they share or otherwise provide access to data collected through, inter alia, information- and intelligence-sharing agreements and when they require disclosure of personal data from third parties, including private companies,

Noting the increase in the collection of sensitive biometric information from individuals, and stressing that States must respect their human rights obligations and that business enterprises should respect the right to privacy and other human rights when collecting, processing, sharing and storing biometric information by, inter alia, considering the adoption of data protection policies and safeguards,

Noting also that general comment No. 16 recommends that States take effective measures to prevent the unlawful retention, processing and use of personal data stored by public authorities and business enterprises,

Welcoming measures taken by business enterprises, on a voluntary basis, to provide transparency to their users about their policies regarding requests by State authorities for access to user data and information,

Deeply concerned at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights,

Emphasizing that, in the digital age, technical solutions to secure and to protect the confidentiality of digital communications, which may include measures for encryption, pseudonymization and anonymity, can be important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association, and recognizing that States should refrain from employing unlawful or arbitrary surveillance techniques, which may include forms of hacking,

Noting with deep concern that, in many countries, persons and organizations engaged in promoting and defending human rights and fundamental freedoms, journalists and other media workers may frequently face threats and harassment and suffer insecurity, as well as unlawful or arbitrary interference with their right to privacy, as a result of their activities,

Noting that, while concerns about public security may justify the gathering and protection of certain sensitive information, States must ensure full compliance with their obligations under international human rights law,

Noting also, in that respect, that the prevention and suppression of terrorism is a public interest of great importance, while reaffirming that States must ensure that any measures taken to combat terrorism are in compliance with their obligations under international law, in particular international human rights, refugee and humanitarian law,

Recognizing that an open, secure, stable, accessible and peaceful information and communications technology environment is important to the realization of the right to privacy in the digital age,

1. *Reaffirms* the right to privacy, according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference, as set out in article 12 of the Universal Declaration of Human Rights¹ and article 17 of the International Covenant on Civil and Political Rights;²

2. *Recognizes* 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, including in achieving the Sustainable Development Goals;¹³

3. *Affirms* that the same rights that people have offline must also be protected online, including the right to privacy;

4. *Recalls* that any interference with the right to privacy should take into account its legality, necessity and proportionality;

5. *Encourages* all States to promote an open, secure, stable, accessible and peaceful information and communications technology environment based on respect for international law, including the obligations enshrined in the Charter of the United Nations and human rights instruments;

6. *Calls upon* all States:

(a) To respect and protect the right to privacy, including in the context of digital communications;

(b) To take measures to put an end to violations of the right to privacy and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law;

(c) To review, on a regular basis, their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

(d) To establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data;

(e) 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;

(f) To consider developing or maintaining and implementing adequate legislation, in consultation with all relevant stakeholders, including civil society, with effective sanctions and appropriate remedies, that protects individuals against violations and abuses of the right to privacy, namely through the unlawful and arbitrary collection, processing, retention or use of personal data by individuals, Governments, business enterprises and private organizations;

¹³ See resolution [70/1](#).

(g) To consider adopting and implementing data protection legislation, regulation and policies, including on digital communication data, that complies with their international human rights obligations, which could include the establishment of national independent authorities with powers and resources to monitor data privacy practices, investigate violations and abuses and receive communications from individuals and organizations, and to provide appropriate remedies;

(h) To further develop or maintain, in this regard, preventive measures and remedies for violations and abuses regarding the right to privacy in the digital age that may affect all individuals, including where there are particular effects on women, as well as children and those who are vulnerable and marginalized;

(i) To consider developing, reviewing, implementing and strengthening gender-responsive policies that promote and protect the right of all individuals to privacy in the digital age;

(j) To provide effective guidance to business enterprises on how to respect human rights by advising on appropriate methods, including human rights due diligence, and on how to consider effectively issues of gender, vulnerability and/or marginalization;

(k) To promote quality education and lifelong educational opportunities for all to foster, inter alia, digital literacy and technical skills to effectively protect privacy;

(l) To refrain from requiring business enterprises to take steps that interfere with the right to privacy in an arbitrary or unlawful way;

(m) To take steps to enable business enterprises to adopt adequate voluntary transparency measures with regard to requests by State authorities for access to private user data and information;

(n) To consider developing or to maintain legislation, preventive measures and remedies addressing harm from the processing, use, sale or multiple resale or other corporate sharing of personal data without the individual's free, explicit and informed consent;

7. *Calls upon* business enterprises:

(a) To meet their responsibility to respect human rights in accordance with the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework,¹⁴ including the right to privacy in the digital age;

(b) To inform users in a clear and easily accessible way about the collection, use, sharing and retention of their data that may affect their right to privacy and to establish transparency policies, as appropriate;

(c) To implement administrative, technical and physical safeguards to ensure that data are processed lawfully and to ensure that such processing is limited to what is necessary in relation to the purposes of the processing and that the legitimacy of such purposes, as well as the accuracy, integrity and confidentiality of the processing, is ensured;

(d) To ensure that respect for the right to privacy and other international human rights is incorporated into the design, operation, evaluation and regulation of automated decision-making and machine-learning technologies and to provide for

¹⁴ A/HRC/17/31, annex.

remediation of the human rights abuses that they have caused or to which they have contributed;

8. *Encourages* business enterprises to work towards enabling secure communications and the protection of individual users against arbitrary or unlawful interference with their privacy, including by developing technical solutions;

9. *Encourages* all relevant stakeholders to participate in informal dialogues about the right to privacy, and takes note with appreciation of the contribution of the Special Rapporteur of the Human Rights Council on the right to privacy to this process;

10. *Encourages* the Human Rights Council and the Office of the United Nations High Commissioner for Human Rights to remain actively seized of the debate, and invites all relevant stakeholders to further discuss how profiling, automated decision-making and machine-learning technologies, sometimes referred to as artificial intelligence, without proper safeguards, impact the enjoyment of the right to privacy, for the purpose of clarifying existing principles and standards and identifying best practices regarding the promotion and protection of the right to privacy;

11. *Decides* to continue its consideration of the question at its seventy-fifth session.

*55th plenary meeting
17 December 2018*

Appendix 3:

A Précis of the (International) Soft Law on the Right to Privacy

1. Legislative Objective

The soft law aims to achieve three mutually-reinforcing legislative objectives:

- 1.1. To refine scope of the right to privacy in international law in a manner that addresses its gaps and accommodates modern understandings of the right in the digital age;
- 1.2. To ground the right to privacy in international law in a manner able to respond to continuing changes in the digital space; and
- 1.3. To facilitate and guide global dialogues on emerging and current issues affecting the enjoyment of digital privacy.

2. Subject-matter Focus

The soft law seeks to address the respect, protection and promotion of the right to privacy in the digital ecosystem. The subject-matter of focus, therefore, is digital privacy broadly understood and covering two regulatory regimes:

- 2.1. Protection of data privacy in the course of processing of personal data in the public and privacy sectors; and

Caveat: Since regulatory details of data protection law cannot be enshrined in an (international) soft law, only baseline data privacy principles are envisaged. Such principles would serve as ‘enabling law’ for further national and/or international legislation.

- 2.2. Protection of privacy in the course of government surveillance measures.

3. Scope of the Right to (Digital) Privacy

With a view to accommodate nuances of the digital landscape and embrace emergent privacy norms worldwide, the scope of the right to privacy must be drawn widely. The soft law must clearly indicate protected interests, ‘subsets’ of the right to privacy and grounds of permissible restriction.

3.1. Protected Interests

The spheres or zones of protection under the right to privacy include one's home, communications, family and personal information. The protection of these private spheres of protection extend to their digital equivalents.

3.1.1. Privacy of the Home, Communications, Family, Reputation and Personal Data

The right to privacy in the digital context extends to the protection from interference with the 'digital home' which includes one's online accounts and electronic equipment.

The right to privacy in the digital age protects from interference with one's digital communications.

The right to privacy protects from attacks against reputation online that cause or are likely to cause prejudice to the private life of a person.

The right to privacy protects privacy of personal data against unlawful collection, storage, analysis and disclosure.

The right to privacy provides protection from interference with the privacy of the family, including in the digital context.

3.2. Subsets of the Right to Privacy

3.2.1. Right to use Privacy-enhancing Technologies

The right to privacy includes a right to use and access privacy-enhancing technologies and services without unlawful interference.

3.2.2. Freedom from Surveillance

The right to privacy includes a right to be free from unlawful surveillance, tracking and monitoring in digital spaces.

3.2.3. Right to the Confidentiality and Integrity of Information Systems

The right to privacy includes protection from unlawful interference with the security, integrity and confidentiality of information systems, devices and services.

3.2.4. Right to Protection of Personal Data

The right to privacy includes a right to the protection of personal data collected and processed both in the private and public sectors. Protection of data privacy must be guaranteed through the adoption of legislation regulating the processing of personal data and government surveillance measures.

3.3. Restrictions of the Right to Privacy

The right to privacy is not absolute but it must be restricted either by States or corporations when the following conditions are cumulatively met:

Legality

Where the impinged interference is made by the State, the requirement of legality is satisfied when the restriction is mandated by law that is sufficiently clear, accessible and specific.

Where the impinged interference is by (Internet) corporations, the requirement of legality is satisfied when the restriction is mandated by law that is sufficiently clear, accessible and specific or mandated by contract that is entered into with clear and revocable consent.

Legitimate Aim

Where the purported interference is made by the State, the requirement of legitimate aim is satisfied when the restriction is necessary in a democratic society to achieve aims such as maintaining public security.

Where the interference is made by (Internet) corporations, the requirement of legitimate aim is satisfied when the restriction is pursued to achieve aims such as legitimate business interests.

Proportionality

Where the interference is made by both States and corporations, the requirement of proportionality is met when the restriction taken is proportional to legitimate aim pursued that is necessary in a democratic society.

4. Core Privacy Principles

4.1. General Principles

4.1.1. Extraterritoriality of the Right to Privacy

The right to privacy applies extraterritorially when a State exercises jurisdiction or control outside its physical territory over all or an aspect of a person's digital communication or personal data.

4.1.2. Dialogical Approach to Digital Privacy

With the view to attend to the complexities of securing privacy in the digital space, the international protection of the right to privacy in the digital environment must be supported by and complemented with multi-level dialogue among relevant stakeholders including States, the private sector and civil society groups.

4.2. Baseline Privacy Principles

The following four principles are key for the protection of the right to privacy in the digital environment:

4.2.1. Prohibition of Mass Surveillance

Mass surveillance in the form of collecting data *en masse* or bulk hacking of communication devices must be prohibited under all circumstances.

4.2.2. Mere Data Collection as Interference

Interference with the right to privacy occurs with the mere collection of personal data irrespective of whether further analysis or processing followed.

4.2.3. Protection of Metadata

The right to privacy applies to all types of personal data regardless of whether it is a metadata or content data.

4.2.4. Independent Oversight

4.2.4.1. Surveillance and Third-party Data Access

All State digital surveillance measures must be undertaken with prior judicial warrant and independent oversight.

All requests for user personal data from third parties, including (Internet) corporations, for law enforcement purposes must be undertaken with prior judicial warrant and independent oversight.

4.2.4.2. Intelligence Sharing

When intelligence containing personal data is shared among States, a two-level independent oversight shall be mandated in the relevant domestic legislation. In the first instance, the sharing of intelligence must be endorsed by a court or tribunal of the source State. Once shared, the approval of a court or tribunal in the receiving State must be sought to prevent new privacy harms due to repurposing of the intelligence containing personal data.

5.Obligations under the Right to Privacy

The tripartite obligations of States and (Internet) corporations under the right to privacy are the following:

5.1. Obligations of States

5.1.1. Obligation to Respect

- 5.1.1.1. States must refrain from interfering with the use of privacy-enhancing technologies, including from compelling creation of backdoors, provision of encryption key escrows or disclosure of keys.
- 5.1.1.2. States must not engage in mass surveillance or bulk hacking of devices under all circumstances.
- 5.1.1.3. States must refrain from measures that weaken or otherwise make ineffective the security, confidentiality and integrity of information systems.

5.1.2. Obligation to Protect

- 5.1.2.1. States must put in place appropriate legislation regulating processing of personal data in all sectors and government surveillance measures.
- 5.1.2.2. States must ensure that the legitimate use of privacy-enhancing technologies is not obstructed by third parties, including by measures that restricts their interoperability in digital platforms or services.
- 5.1.2.3. States must ensure that everyone is protected against unlawful surveillance, monitoring, tracking and profiling online by third parties through appropriate legislative and administrative mechanisms.
- 5.1.2.4. States must regulate by law the sale and export of surveillance technologies by the private sector, including through appropriate licensing regime that involves regular review and monitoring.
- 5.1.2.5. States must ensure that the security, integrity and confidentiality of information systems operated by its agencies to prevent attacks from third parties.

5.1.3. Obligation to Fulfil

- 5.1.3.1. States must eliminate unnecessary barriers to access and use of privacy-enhancing technologies, including import/export restrictions or discriminatory tariffs.
- 5.1.3.2. States must take all reasonable steps to raise awareness on the importance and use of privacy-enhancing technologies.
- 5.1.3.3. States must take all reasonable steps to promote best practices on the security of information systems operated by the private sector.
- 5.1.3.4. States must make relevant legislation regulating surveillance accessible to any interested party.
- 5.1.3.5. States must provide *ex post facto* notice to a person subjected to targeted surveillance, and where appropriate, provide appropriate remedies.

5.2. Obligations of (Internet) Corporations

5.2.1. Obligation to Respect

- 5.2.1.1. Corporations must refrain from any measure that obstructs the use of privacy-enhancing technologies on their platforms, applications or services.
- 5.2.1.2. Corporations must refrain from disclosing user personal data to States without appropriate judicial authorization.
- 5.2.1.3. Corporations must refrain from selling or otherwise making available technologies to third-parties that undermine the enjoyment of privacy where there is an apparent risk of abuse.
- 5.2.1.4. Corporations must not engage in or assist the unlawful surveillance of users.

5.2.2. Obligation to Protect

- 5.2.2.1. Corporations must ensure the security, confidentiality and integrity of their communication services and computer systems.
- 5.2.2.2. Corporations must inform users where the security breach of their computer systems or communication services is likely to

affect the privacy of users and provide remedies where appropriate.

- 5.2.2.3. Corporations must take all reasonable steps to prevent unlawful requests for user personal data from third parties.
- 5.2.2.4. Corporations must take all reasonable steps to protect their users from unlawful surveillance or unreasonable request for personal data by third parties.
- 5.2.2.5. Corporations must be guided by applicable international privacy standards in designing and operating technologies used in the collection and processing of personal data.

5.2.3. Obligation to Fulfil

- 5.2.3.1. Corporations must take all reasonable steps to enable the use of privacy-enhancing technologies on their platforms, devices and services.
- 5.2.3.2. Corporations must provide clear information to users as to the nature and type of security features available in their computer systems or communication services.
- 5.2.3.3. Corporations must issue regular transparency reports on government requests for user personal data and regarding provision of surveillance technologies to third parties. Where applicable, corporations must inform individual users whose data has been disclosed to law enforcement agencies.

5.3. The Role of Other Non-State Actors

5.3.1. Civil Society

The international protection of the right to privacy must involve the active participation, advocacy and expertise of relevant civil society organizations.

5.3.2. International-governmental Organizations

International governmental organizations that engage in routine collection and processing of personal data must adopt internal data protection policies in line with international standards.

5.3.3. Technical communities

International organizations involved in setting Internet and web technical standards must support the global effort for the protection of digital privacy, including in designing secure global communication standards and protocols.

6. Miscellaneous Provisions

6.1. A Multi-stakeholder Privacy Forum

A multi-stakeholder privacy forum shall be created as a subsidiary body of the Human Rights Council to complement and reinforce the work of existing institutional arrangements in upholding the right to privacy in the digital age.

6.1.1. Purposes

The privacy forum shall be a platform to deliberate on an ongoing basis emerging and current issues affecting the protection of the right to privacy in the digital environment.

Held at least once in a year, the forum shall facilitate dialogue, consensus and cooperation among actors that play a role in the respect, protection and promotion of the right to privacy in the digital space.

6.1.2. Composition

All relevant stakeholders particularly States, (Internet) corporations, civil society groups, intergovernmental organizations and members of the technical community shall take part in the forum.

The UN and other relevant actors shall take all reasonable steps towards ensuring fair representation, including geographic representation, at the forum.

6.1.3. Role of the Special Rapporteur on the Right to Privacy

The forum shall be chaired and facilitated by the Mandate of the Special Rapporteur on the Right to Privacy.

The thematic priorities of the Mandate must not be dictated by the Special Rapporteur.

...