EXTRATERRITORIAL ALGORITHMIC SURVEILLANCE AND THE INCAPACITATION OF INTERNATIONAL HUMAN RIGHTS LAW

Arindrajit Basu[*]

Our networked data trails dictate, define and modulate societies in hitherto inconceivable ways. The ability to access and manipulate that data is a product of stark power asymmetry in geo-politics, leading to a dynamic that privileges the interests of a few over the right to privacy and dignity of the many. I argue that the persistent de facto violation of human rights norms through extraterritorial surveillance conducted by western intelligence agencies, compounded by the failure of judicial intervention in the West has lead to the incapacitation of international human rights law. Despite robust jurisprudence including case law, comments by the United Nations, and widespread state practice on the right to privacy and the application of human rights obligations to extraterritorial stakeholders, extraterritorial surveillance continues with aplomb. Procedural safeguards and proportionality tests regularly sway towards a 'ritual incantation' of national security even in scenarios where a less intrusive option is available. The vulnerable citizen abroad is unable to challenge these processes and becomes an unwitting victim of nefarious surveillance practices that further widens global power asymmetry and entrenches geo-political fissures.

Table of Contents

[*] Arindrajit Basu, BA.LLB (NUJS), LLM (Cambridge) is a Research Manager at the Centre for Internet & Society.
This paper is largely, the first half of a thesis submitted in completion of the LLM Program at the University of Cambridge. The author would like to thank Prof. Eyal Benvenisti and Agnidipto Tarafder for their comments and insight on the draft.

I. INTRODUCTION

In today's era of the Internet of Things ('IoT'), we live in a world of ubiquitous network communications that define our relationships, aid our daily activities and are inextricably integrated into our existence—in many ways defining who we are.[1] At the same time, our networked data trails have made it possible for governments and corporations to conduct networked surveillance.[2]

The élan vital of cyberspace is in its borderless existence. It is possible for a government to conduct surveillance on and utilise data generated by individuals who are physically very distant. The specific policy problem of extraterritorial surveillance that this paper chooses to tackle, acts as an ideal case study to evaluate future approaches to international law in a world where technological advancement is increasing the divide between entities that possess the capacity to harness this technology and those that do not.

Intelligence agencies collect all data generated by individuals located extraterritorially and retain them at a data-centre for the purpose of finding a 'needle in a haystack'[3] that might lead them to suspicious activity.[4] While human beings do not view the data at this stage, algorithms filter data trails that reveal patterns of suspicious activity, following which closer surveillance by human operators is conducted on individuals who are deemed 'suspicious' by the algorithm.[5]

This form of surveillance is being conducted on individuals who reside abroad and resultantly lack the power to alter state policy either through democratic participation or litigation.[6] The vulnerability and powerlessness of an individual whose data is being surveilled by humans or machines located in another territory is precisely the sort of scenario that the tenets of international law, in particular international human rights law, were designed to shield against. This is because these constructs have their origins in a shared moral conception of human dignity irrespective of the individual's nationality.[7]

---

[1] JOHN CHENEY-LIPPOLD, WE ARE DATA: ALGORITHMS AND THE MAKING OF OUR DIGITAL SELVES (2017).

[2] BRUCE SCHNEIER, THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD (2015).

[3] J.D. Tuccille, *Why spy on everybody? You need the haystack to find the needle*, REASON, July 19, 2013, available at http://reason.com/blog/2013/07/19/why-spy-on-everybody-because-you-need-th (Last visited on June 11, 2019).

[4] *See* Peter Margulies, *Surveillance By Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights*, 68(4) FLORIDA LAW REVIEW 1055-1063 (2016).

[5] Paul Bernal, *Data gathering, surveillance and human rights: recasting the debate*, 1(2) JOURNAL OF CYBER POLICY 249 (2016).

[6] *See also* Amos Toh et al, *Overseas Surveillance in an Interconnected World*, 5-8(2016), available at https://www.brennancenter.org/sites/default/files/publications/Overseas_Surveillance_in_an_Interconnected_World.pdf (Last visited on June 11, 2019).

[7] RONALD DWORKIN, IS DEMOCRACY POSSIBLE HERE? 48 (2006). ("The domain of human rights has no place for passports")

This shared moral conception leads to a doctrinal understanding of international human rights that protects the vulnerable foreigner from unwanted surveillance. First, there exists sufficient jurisprudence and scholarship that justifies the incorporation of a right to privacy in international human rights law, which has been applied to cases of surveillance till date. Human rights law allows for the balancing act of proportionality[8] between national security[9] and the right to privacy—a tool which policy makers use, albeit in a flawed manner, to justify mass surveillance. Second, notwithstanding United States of America's opposition to the notion, most scholarship and United Nations reports have acknowledged that sovereign States owe some form of obligation to extraterritorial stakeholders.[10] Yet, the bulk targeting of foreigner's data continues with aplomb, justified by the trump card of national security[11] and legitimised by law and policy that contain supposedly sufficient procedural safeguards.

The objective of this thesis is not to re-embark on any of the above mentioned doctrinal expeditions, as these have already been robustly articulated elsewhere. Instead, after broadly surveying these conclusions and highlighting some relevant trends and gaps in existing jurisprudence, this paper seeks to highlight why doctrinal or jurisprudential certainty has failed to genuinely protect the vulnerable in the context of this specific policy problem.

The paper is structured into five chapters. The next chapter defines the contours of the policy problem. It has two sub-parts. The first sub-part explains the process of algorithmic surveillance and the second surveys domestic law in the United States of America and the United Kingdom that enables this process. Chapter 3 broadly surveys existing commentary on mass surveillance and identifies patterns and gaps in recent jurisprudence in this respect. It is divided into three sub-parts. The first section surveys the law and scholarship on the extraterritorial application of human rights. The second section considers the international human rights law applicable to mass surveillance and identifies certain gaps in the existing jurisprudence. Finally, Chapter 4 analyses why institutional mechanisms alone cannot protect human rights. The first sub-part therein explores the deficiencies in procedural safeguards and the second sub-part asserts why arguments calling for an international code of conduct might also not be entirely successful.

This paper attempts to explore several apparently disconnected strands of law and political thought including discrimination, privacy, extraterritoriality and even critiques of the human rights regime itself. It does not do justice to the jurisprudence in either of the sections when severed, but taken together hopes to understand the possible role of international law in a

---

[8] *See* Michael Kirby, *National Security: Proportionality, Restraint and Commonsense*, 11(6) PRIVACY LAW AND POLICY REPORTER, 151 (2005).

[9] Richard A. Posner, *Privacy, Surveillance, and Law*, 75 UNIVERSITY OF CHICAGO LAW REVIEW 245, 246 (2008). ("Civil libertarians want government to be transparent but private individuals opaque; national security hawks want the reverse.")

[10] *See* Evan J. Criddle & Evan Fox-Decent, *The Fiduciary Character of Sovereignty* in FIDUCIARIES OF HUMANITY: HOW INTERNATIONAL LAW CONSTITUTES AUTHORITY 2 (2016); Maastricht Principles on Extraterritorial Obligations of States in the Area of Economic, Social and Cultural Rights, 2011; *Working Paper Human Rights Law Sources: UN Pronouncements on Extra-Territorial Obligations*, THE GLOBAL INITIATIVE FOR ECONOMIC, SOCIAL AND CULTURAL RIGHTS, July 2015, available at https://www.etoconsortium.org/nc/en/main-navigation/library/documents/detail/?tx_drblob_pi1%5BdownloadUid%5D=163 (Last visited on June 11, 2019).

[11] Jennifer A. Chandler, *Personal Privacy versus National Security: Clarifying and Reframing the Trade-off* in ON THE IDENTITY TRAIL: ANONYMITY, PRIVACY AND IDENTITY IN A NETWORKED SOCIETY 121, 122 (Orin Kerr, Carole Lucock &Valerie Steeves, ed., 2009).

policy question that straddles multiple dimensions. Indeed, most global challenges in today's networked world are so convoluted that demarcating the policy questions themselves is an arduous task. This paper does not aim to arrive at any certain answers but by using this broad lens hopefully succeeds at highlighting the correct issues, which may then be considered in future legal scholarship.

II. THE POLICY PROBLEM DEFINED

This chapter seeks to explore the complex contours of the policy problem so that it can act as a frame of reference for analysis that will be undertaken in the rest of the paper. It first explains the nature of algorithmic surveillance as conducted by intelligence agencies and then explores the law and policy that legitimises and enables this surveillance

A. HOW SURVEILLANCE WORKS

This section seeks to delve briefly into the operational details of algorithmic surveillance conducted both by the National Security Agency ('NSA') in the United States of America ('US') and the Government Communications Headquarters ('GCHQ') in the United Kingdom ('UK'). These details have been drawn from the media leaks orchestrated by Edward Snowden through Guardian correspondent Glenn Greenwald,[12] most of which were contained in the hitherto undisclosed NSA Management Directive #424.[13]

Algorithmic surveillance can broadly be divided into two stages,[14] which we may refer to as dataveillance and bulk collection, and algorithmic processing and targeting.

1. Dataveillance and bulk collection

In the first stage, vast tracts of data are accumulated through the 'bulk collection' of data generated online by individuals, in what has been popularly termed 'mass surveillance.'[15] The proliferation and increased sophistication of information and communication technologies ('ICTs') in today's age of the Internet of Things ('IoT') has lead to a large proportion of human interaction and therefore, aspects of the human persona itself being extended to the cyber realm.[16] The nature of surveillance conducted by the intelligence agencies exemplifies the process of 'dataveillance', a term coined by Roger Clarke in 1988, which refers to the systematic

[12] See *The NSA Files*, THE GUARDIAN, available at www.theguardian.com/us-news/the-nsa-files (Last visited on June 11, 2019); *see also* GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA AND THE SURVEILLANCE STATE (2014) for a detailed explanation of the operational procedures.

[13] George R. Lucas Jr., *NSA Management Directive #424: Secrecy and Privacy in the aftermath of Edward Snowden*, 28 ETHICS AND INTERNATIONAL AFFAIRS 1, 29 (2014).

[14] Maria Helen Murphy, *Algorithmic Surveillance: the collection conundrum*, 31 INTERNATIONAL REVIEW OF LAW, Computers and Technology, 225, 226 (2017).

[15] Benson Egwuonwu, *What is Mass Surveillance and what does it have to do with Human Rights*, RIGHTS INFO, April 11, 2016, available at https://rightsinfo.org/explainer-mass-surveillance-human-rights/ (Last visited on June 11, 2019).

[16] *See* Jeremy Crampton, *Collect it All: National Security, Big Data and Governance*, 80 GEOJOURNAL 4, 519 (2015).

monitoring and surveillance of an individual's action and behaviour through the use of information technology.[17]

To appreciate the implications of dataveillance in the modern era, we must understand the shift from what Ferguson terms 'small data'[18] (vertical surveillance) to what Hu terms as modern day 'big data cyber-surveillance' (horizontal surveillance).[19] Before the dawn of the age of 'big data', the use of 'small data' entailed zeroing in on a possible suspected target and subsequently monitoring of the target's communications or other personal details.[20] This targeted approach needed to be adopted because the computational ability to evaluate infinite data sets simply did not exist.[21] In contrast, in today's world of big data, we "move the question (on identification of the target itself) to the data",[22] which serves as the edifice for targeting and predictive analytics.

While big data has no set definition, technologists and legal scholars agree that the term refers to both the technology and the process of sifting through colossal quantities of data while identifying patterns in the data collected[23] and subsequently applying these patterns to newly generated or collected data.[24] The process is anchored in the 3 Vs—volume, velocity and variety[25]—that require innovative forms of efficient and cost-effective decision-making to be used pragmatically.[26]

Dataveillance may be conducted on two types of data sets. The first kind of data is metadata, which only provides information on the time and length of the communication between two individuals and does not reveal the language (content) of what is being communicated.[27] While the NSA is a public authority, it has multiple partnerships with private sector corporations including Microsoft, Intel, Verizon, Quest and AT&T.[28] The NSA intercepts

---

[17] Roger A. Clarke, *Information Technology and Dataveillance*, 31 COMMUNICATIONS OF THE ACM 498 (1988); *see also* Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance* 42 PEPPERDINE LAW REVIEW 773, 776-777 (2015).

[18] Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 UNIVERSITY OF PENNSYLVANIA LAW REVIEW 327, 329 (2015). (Indicated the reasonable definition of 'small data' used here.)

[19] Hu, *supra* note 17, 804,832.

[20] Ferguson, *supra* note 18, 329.

[21] *See* William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEXAS LAW REVIEW 1633, 1661 (2010).

[22] Ira "Gus" Hunt, *Presentation at Gigaom Structure Data Conference: The CIA's "Grand Challenges" with Big Data* (summarised in Mathew Ingram, *Even the CIA is struggling to deal with the volume of real-time social data*, GIGAOM, March 20, 2013, available at https://gigaom.com/2013/03/20/even-the-cia-is-struggling-to-deal-with-the-volume-of-real-time-social-data (Last visited on June 12, 2019).

[23] Danah Boyd & Kate Crawford, *Critical questions for Big Data: Provocations for a cultural, technological and scholarly phenomenon*, 15(5) INFORMATION, COMMUNICATION AND SOCIETY 662,663 (2012).

[24] Julie E. Cohen, *What Privacy Is For*, 126 HARVARD LAW REVIEW, 1904, 1920–1921 (2013); BRUCE SCHNEIER, THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 56 (2015).

[25] Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 BOSTON COLLEGE LAW REVIEW 93, 94 (2014).

[26] Hu, *supra* note 17, 794.

[27] *A Guardian Guide to Your Metadata*, THE GUARDIAN, June 12, 2013, available at www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsasurveillance (Last visited on June 12, 2019).

[28] Slide displayed in GREENWALD, *supra* note 12, 102.

data communication from these platforms and redirects the data to their data repositories.[29] One such repository is located in Bluffdale, Utah and is recognised through its code name 'Mainway' which has been acting as an amassment of two billion 'record events' a day, since 2010.[30]

In conjunction with its private partners, the NSA is able to gain access to data generated in foreign territories through various programs.[31] 'BLARNEY' is one such program which relied on the NSA's relationship with AT&T to gain access to "high capacity international fiber optic cables, switches and/or routers throughout the world".[32] The countries targeted by this program included Brazil France, Germany, Greece, Italy, Japan, Mexico, South Korea and Venezuela.[33] A comparable program by the name of 'FAIRVIEW' engaged in similar practices with the aid of a 'corporate partner'.[34] Its operation was made blatantly clear through a leaked slide, which highlighted its unique aspects as "Access to massive amounts of data; (c)ontrolled by variety of legal authorities and (m)ost accesses are controlled by partner."[35] 'STORMBREW' is yet another program conducted in close conjunction with the US Federal Bureau of Investigation and provides the NSA access to data travelling through various 'choke points' on US territory,[36] as much of the world's communication passes through these said choke points—testament to the talismanic role the United States has played in the development of the world's infrastructure and the disproportionate number of data processors located in the United States.[37]

The NSA's surveillance endeavours also target data containing the content of communications gained directly from nine biggest internet companies.[38] Unlike other programs that used 'upstream' collection using fiber optic cables and other infrastructure, the 'PRISM' programme enabled the NSA to directly obtain content from the servers of private internet service providers in the US.[39] The relevant slide revealed by the Snowden leaks encourages the NSA operators to use both 'upstream' surveillance and the content garnered through the 'PRISM' programme.[40]

The Snowden revelations also disclosed enthusiasm among personnel at the GCHQ working on these programs, although the information available is not as detailed.[41]

---

[29] *Id.*, 103.
[30] GEORGE LUCAS, ETHICS AND CYBER WARFARE: THE QUEST FOR RESPONSIBLE SECURITY IN THE AGE OF DIGITAL WARFARE 144 (2014).
[31] GREENWALD, *supra* note 12, 102.
[32] *Id*., 103.
[33] *Id*.
[34] Bernard E. Harcourt, *The Surveillance State* in EXPOSED: DESIRE AND DISOBEDIENCE IN THE DIGITAL AGE 72 (2015).
[35] Slide available on GREENWALD, *supra* note 12, 104.
[36] *Id*.
[37] See 'US choke points for Australian Telecommunications Data no surprise', (*The Conversation*, 15 July 2013) <http://theconversation.com/us-choke-points-for-australian-telecoms-data-are-no-surprise-16070 (Last visited on June 13, 2019).
[38] GREENWALD, *supra* note 12, 108.
[39] Glenn Greenwald & Ewen McAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN, June 7 2013, available at http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Article:in%20body%20link (Last visited on June 12, 2019).
[40] Slide available on GREENWALD, *supra* note 12, 108.
[41] Ewen McAskill et al, *GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications*, THE GUARDIAN, June 21, 2013, available at www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (Last visited on June 13, 2019); GREENWALD, *supra* note 12, 119.

Notably, the GCHQ is involved in the operation of the 'Tempora' program which intercepts data on fibre-optic cables transmitting data between US and Europe.[42] This is important as the majority of fibre-optic cables carrying transatlantic data land in the UK.[43]

It is important to note that at the dataveillance stage, the data is not supposed to be viewed by human operators and remains stored in the data repositories for future analysis.[44]

2. Algorithmic Processing and Targeting

In the second stage, this trove of data is processed using algorithmic data mining techniques[45] to identify potential suspects, whose profiles are then examined in detail. This process is known as 'data-chaining', which links up the recorded events into a topographical mapping of patterns, most of which is excluded or filtered out by the algorithm unless the data reflects a pattern that the algorithm reveals to be suspicious.[46]

Machine learning searches using the above mentioned techniques may be either directed or autonomous.[47] In the case of directed searches, human operators input the 'identifiers' needed for the machine to search through the data available.[48] Autonomous searches go beyond merely executing parameters set by humans and frame their own parameters through processes that closely resemble human reasoning and discretion.[49]

Autonomous searches typically use artificial neural networks that are software applications which function autonomously like the human brain.[50] Neural networks generally have hidden layers that connect inputs and outputs, which facilitate greater mathematical precision.[51] The models underlying autonomous systems can be further divided into supervised learning systems, where data is pre-labelled at the discretion of an expert and unsupervised learning systems, which does not use a labelled training data set simply because the operator does not know what to expect.[52]

'XKeyscore'[53] and 'TreasureMap'[54] are analytical programs used by the NSA for the purpose of algorithmic targeting. The surveillance capabilities of 'XKeyScore' are very

[42] *Id*.
[43] *Id*.
[44] *Id*.
[45] *See* IAN WITTEN ET AL, DATA MINING: PRACTICAL MACHINE LEARNING TOOLS AND TECHNIQUES (2011).
[46] Lucas, *supra* note 30, 145.
[47] Margulies, *supra* note 4, 1061.
[48] David S. Kris, *On the bulk collection of tangible things*, 7 JOURNAL OF NATIONAL SECURITY LAW & POLICY 209, 217-18 (2014) (quoted in Margulies, *supra* note 4, 1061).
[49] STUART J RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH 728 (1995).
[50] Michael Aikenhead, *The uses and abuses of neural networks in law*, 12 SANTA CLARA COMPUTER AND HIGH TECHNOLOGY LAW JOURNAL 31, 35-36 (1996).
[51] Russell, *supra* note 49, 729.
[52] Alan Blackwell, *Interacting with an inferred World: The Challenge of Machine Learning for Humane Computer Interaction*, 8 (Paper presented at the 5TH DECENNIAL AARHUS CONFERENCE ON CRITICAL ALTERNATIVES, August 17-21, 2015).
[53] Glenn Greenwald, *XKeyScore: NSA Tool collects nearly everything a user does on the internet*, THE GUARDIAN, July 31, 2013, available at www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (Last visited on June 13, 2019).

broad and allow for the surveillance of individuals based on suspicious patterns of behaviour deduced from the aggregated processing of information such as nationality, location or websites visited.[55] For example, one declassified NSA slide displays a query called "germansinpakistn" that enables an analyst to examine residents in Pakistan who may be surfing certain German language messaging systems.[56] 'Treasure Map' constructs the data in recognisable patterns as a "constellation of intricate communication nodes"[57] while 'XKeyscore' assigns a risk-analysis score to each node in the constellation.[58] The patterns and the respective score of each resulting data cluster help analysts determine the 'surveillance-worthiness' of certain individuals or chains of communication.[59]

Through these methods, suspect profiles are developed, which enable the NSA to make predictions about his or her future behaviour. [60] For example, if during ISIS' reign in Syria and Iraq, an individual was boarding a flight bound for Turkey with cash using an unregistered mobile number and had, over the past few months visited webpages containing the teachings of Islamic preachers online, an algorithmic profile might indicate that the individual wanted to join ISIS as a foreign fighter.[61] The use of big data therefore, throws up several legal and policy questions within the surveillance paradigm, some of which have been dealt with by domestic legislators.

B. APPLICABLE DOMESTIC LAW AND POLICY IN THE UNITED STATES AND UNITED KINGDOM

This section considers domestic legislation in the United States and United Kingdom that permits the bulk targeting of non-citizens data and enables the programmes detailed above. Surveying such legislation is crucial before we move onto considering the international human rights dimension, because it charts out the obligations of political decision-makers to domestic citizens who have the democratic right to hold them accountable for their actions.

The authority for NSA's surveillance programmes ostensibly emanates from §702 of the Foreign Intelligence Surveillance Amendment Acts, 2008 ('FISAA').[62] The FISAA adopts differing approaches depending on whether the targets are 'US persons' or 'Non US persons'.[63]

---

[54] Harrison Weber, *The NSA has a plan to map the entire internet and it's called treasure map*, VENTURE BEAT, September 14, 2014), available at https://venturebeat.com/2014/09/14/the-nsa-has-a-plan-to-map-the-entire-internet-its-called-treasure-map/ (Last visited on June 11, 2019).

[55] Morgan Marquis et al, *XKeyScore: NSA's Google for the World's Private Communications*, THE INTERCEPT, July 1, 2015, available at https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/ (Last visited on June 13, 2019).

[56] *Id*.

[57] Lucas, *supra* note 30, 146.

[58] *Id*.

[59] *Id*.

[60] John Cheney-Lippold, *supra* note 1, 54.

[61] Example adapted from the facts of United States v. Sokolow, 490 U.S. 1, 109 S. Ct. 1581 (1989), which dealt with a 'drug trafficker', as discussed in Michael Rich, *Machine Learning, Automated Suspicion Algorithms and the Fourth Amendment*, 164 UNIVERSITY OF PENNSYLVANIA LAW REVIEW 871,902 (2016).

[62] *See* Foreign Intelligence Surveillance Amendment Acts, 2008, 50 U.S.C ch. 36 § 1801 et seq, § 1881(a).

[63] *Id*., §1881(c); Eliza Watt, *The right to privacy and the future of mass surveillance* 21(7)THE INTERNATIONAL JOURNAL OF HUMAN RIGHTS 773 (2017).

US persons include either American citizens or non-American citizens who permanently reside in the United States. US persons can be targeted only if there is probable cause to believe that the individual is a foreign agent and a warrant is issued by the Foreign Intelligence Surveillance Court ('FISC').[64] Non-US persons may be surveilled under a lower 'reasonable belief' standard without a judicial warrant from the FISC,[65] although they must sign off on the government's 'high level' operation plan annually.[66] Further, the minimisation mandates that apply when tapping communications of US persons do not apply in their entirety to non US persons.[67] Even though the relevant provision was set to expire in January 2018, Congress voted to re-authorise §702 for another six years[68] and thereby gave tacit approval to the NSA's bulk-targeting programs despite opposition from civil liberties groups[69] and legal academics.[70]

Further, Executive Order 12333 ('EO 12333') promulgated by erstwhile US President Ronald Reagan has for long empowered the President to order surveillance activities abroad at his discretion.[71] While there has been a cloud of opacity around EO 12333, the Snowden revelations exerted some pressure[72] on then President Barack Obama to issue the Presidential Policy Directive ('PPD-28').[73] It is worth exploring this Directive in some detail as it is a unique set of guidelines published by the US executive, which seeks to lend some transparency and legitimacy to the Signals Intelligence process and is important for assessing the institutional surveillance framework, even though it is probably a symbolic response to the aftermath of the Snowden revelations rather than a document that the NSA considers robust policy.[74] PPD-28 clearly mandates privacy protections for all individuals by stating,

---

[64] LAURA DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE:PRIVACY AND SURVEILLANCE IN A DIGITAL Age 59 (2016).

[65] CASS SUNSTEIN ET AL, THE NSA REPORT: LIBERTY AND SECURITY IN THE CHANGING WORLD: THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 86-87 (2013).

[66] Andrew Crocker & David Ruiz, *How Congress's extension of Section 702 may expand the NSA's warrantless surveillance authority*, ELECTRONIC FRONTIER FOUNDATION, February 1, 2018, available at www.eff.org/deeplinks/2018/02/how-congresss-extension-section-702-may-expand-nsas-warrantless-surveillance (Last visited on June 13, 2019).

[67] *Id*.

[68] Louis Matsakis, *Congress Renews Warrantless Surveillance and Makes it Worse*, WIRED, February 11, 2018, available at https://www.wired.com/story/fisa-section-702-renewal-congress/ (Last visited on June 14, 2019).

[69] *ACLU Letter for the Record on House Judiciary Committee Hearing on* "*Section 792 of the Foreign Intelligence Surveillance Act*", ACLU, available at https://www.aclu.org/letter/aclu-letter-record-house-judiciary-committee-hearing-section-702-foreign-intelligence (Last visited on June 14, 2019); *Fact Sheet: Impact of Warrantless Section 702 Surveillance on People in the United States*, HUMAN RIGHTS WATCH, March 1, 2017, available at https://www.hrw.org/news/2017/03/01/fact-sheet-impact-warrantless-section-702-surveillance-people-united-states (Last visited on June 14, 2019).

[70] *See e.g*. Elizabeth Goiten, *Statement before the United States House of Representatives Committee on Judiciary Hearing on Section 702 of the FISA Amendments Act*, available at https://judiciary.house.gov/wp-content/uploads/2017/02/Goitein-Testimony.pdf (Last visited on June 14, 2019).

[71] Executive Order No. 12333, 3 C.F.R. 200 (1981).

[72] *See* Peter Margulies, *Global Cybersecurity, Surveillance and Privacy:The Obama Administration's Conflicted Legacy*, 24(2) INDIANA JOURNAL OF GLOBAL LEGAL STUDIES 459 (2017).

[73] The White House, Presidential Policy Directive No.28, 2014, *Signals Intelligence Activities*, January 17, 2014, available at https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (Last visited on June 14, 2019).

[74] Francesca Bignami & Giorgio Resta, *Human Rights Extraterritoriality: The Right to Privacy and National Security* in SURVEILLANCE IN COMMUNITY INTERESTS ACROSS INTERNATIONAL LAW (Eyal Benvenisti and Georg Nolte ed., forthcoming).

> "…Our signals intelligence activities must take into account that all individuals must be treated with dignity, regardless of their nationality or wherever they reside and that all persons have legitimate privacy interests in the handling of their personal information."[75]

It goes on to recognise that ICTs hold great scope for signals intelligence in the modern world[76] although the risks posed specifically by the use of algorithms have not been mentioned. It goes on to pay lip-service to the idea that signals intelligence will not be collected for the purpose of suppressing criticism or discriminating against persons based on their identity.[77] While endorsing bulk collection as necessary to decipher threats in today's complex network of global communications,[78] the Directive states that data would only be collected where there exists a "foreign intelligence or counterintelligence purpose and departmental missions and not for other purposes"[79] and goes on to mention six cases where bulk targeting is permissible.

These include cases of espionage, terrorist threats to the United States, threats due to proliferation of weapons, cybersecurity, threats to the US or allied armed forces, and transnational criminal threats.[80] While the categories such as 'terrorist threats' or 'cybersecurity' are in themselves broad and ambiguous, the list of purposes appear to be exhaustive. Finally, the Directive includes safeguards drawn from the broad parameters of any standard data protection framework[81] both for US and non-US persons,[82] which include minimization of data collection, limits on dissemination, use and retention, proportionality and oversight.[83] Thus, without going into an in-depth analysis of the modalities, PPD-28 stressed that signals intelligence activities must comply with international human rights law.

The UK's extraterritorial surveillance programme was similarly laid out in legislation—initially the Regulation of Investigatory Powers Act, 2000 ('RIPA') which has been replaced by the Investigatory Powers Act, 2016 ('IPA') that provides a far broader mandate for mass surveillance. Like §702 of FISAA, the RIPA also makes a distinction between 'internal' and 'external' communications (referred to as 'Overseas-related communication' in IPA)[84] which refers to communication "sent or received outside the British Islands."[85] Surveillance of the former sets of data is subject to an individualised warrant, whereas overseas data can be intercepted using a bulk targeting warrant with no cap on the quantity of data that may be collected.[86]

---

[75] The White House, Presidential Policy Directive No.28, 2014, §1.
[76] *Id*.
[77] *Id*., §1(b).
[78] *Id*., §2.
[79] *Id*.
[80] *Id*., §2.
[81] Pam Dixon, *A Brief Introduction to Fair Information Practice Principles*, WORLD PRIVACY FORUM, June 5, 2006, available at https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-informationpractices/ (Last visited on June 15, 2019).
[82] The White House, Presidential Policy Directive No.28, 2014, §4
[83] *Id*.
[84] Investigatory Powers Act, 2016, §136(3).
[85] Regulation of Investigatory Powers Act, 2000, §8 (4)-8(6).
[86] Investigatory Powers Act, 2016, §136(4).

The UK government's policy approach to the bulk targeting of overseas communication is similar to the approach taken in the PPD-28. An examination of the government's response drafted to the findings of the Parliament's Intelligence and Security Committee's Report on Privacy[87] in 2016 when Theresa May was Home Secretary is useful for discerning UK policy on this matter.[88] It stresses on the need for strong safeguards that are built into the IPA and re-enforces the idea that bulk interception is to be done for preserving legitimate national security interests.[89]

As apparent, the human rights reflected in these government policies are couched in the language of safeguards rather than substantive moral doctrine. The approach seems to indicate that the policy focus is on national security while the procedural safeguards play the role of balancing the security-oriented priorities with civil liberties.

III. SURVEY OF APPLICABLE INTERNATIONAL HUMAN RIGHTS LAW

This chapter attempts to broadly survey the law applicable to each element of the policy problem explained in Chapter II. It begins with a survey of jurisprudence and scholarship exploring the scope of extraterritorial obligations. The subsequent section explores the applicable international human rights law on privacy that may be applicable to mass surveillance.

A. EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS OBLIGATIONS

The jurisdiction of the International Covenant on Civil and Political Rights ('ICCPR') is stipulated in Article 2(1) which articulates that State parties are obligated to "respect and ensure to all individuals within its territory and subject to its jurisdiction, the rights recognised in the present Covenant."[90] As per a dubious interpretation of the language of this provision, the United States has argued that individuals who are not both within their territory and subject to their State jurisdiction are not entitled to protections afforded by the Covenant.[91] For this purpose, the US relies on the rules of the Vienna Convention on the Law of Treaties which state that a treaty must be interpreted using the ordinary meaning of its terms.[92] The US position also extends its reference to the *travaux preparatoires* of the treaty and its own earlier statements made before the United Nations Human Rights Committee ('UNHRC').[93]

---

[87] Intelligence and Security Committee of Parliament, *Privacy and Security: A modern and transparent legal framework*, March 12, 2015, available at https://www.pdpjournals.com/docs/88433.pdf (Last visited on June 14, 2019).

[88] *Government Response to the ISC Report on Privacy and Security*, available at http://data.parliament.uk/DepositedPapers/Files/DEP2016-0081/Gov_response_to_PS_report_excluding_IP_Bill_provisions.pdf (Last visited on June 14, 2019).

[89] *Id*.

[90] International Covenant on Civil and Political Rights, December 16, 1966 (entered into force 23 March 1976), 999 UNTS 171 (ICCPR), Art. 2.

[91] Harold Hongju Koh, 'Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights' (*Just Security*, 19 October 2010) https://www.justsecurity.org/wp-content/uploads/2014/03/state-department-iccpr-memo.pdf (Last visited on June 14, 2019).

[92] *Id.*

[93] *Id*; For a critical assessment *see* Beth Van Schaak, *The United States*' *Position on the Extraterritorial Application of Human Rights Obligations: Now Is the Time for Change*, 90 INTERNATIONAL LAW STUDIES 20 (2014).

There has been significant pushback against the US position at the institutional level as Watt has documented.[94] The Human Rights Committee in its 1994,[95] 2006[96] and 2014[97] periodic reports on the US have repeatedly denounced the position adopted by the US. It also indicated in General Comment No. 31, that this notion would not be in consonance with the 'object and purpose' of the Covenant.[98] Further, the UN High Commissioner for Human Rights report on 'The Right to Privacy in the Digital Age' considered situations when extraterritorial obligations may come into play in the context of extraterritorial surveillance.[99] The report concluded that these obligations would be borne to individuals regardless of their nationality, or physical location as long as 'effective control' is exercised by the State in a manner that violates their right to privacy.[100] As articulated by Special Rapporteur Ben Emmerson, this would include within its purview measures currently being pursued by the NSA such as tapping into their fibre-optic cables or using the location of internet architecture within their territory to intercept communications.[101] Furthermore, as Wilde has adequately documented, jurisprudence of the International Court of Justice recognises that the obligations contained in human rights treaties apply extraterritorially.[102]

The European Court of Human Rights ('ECtHR') has been possibly the greatest champion of extraterritorial application of human rights and has the most developed jurisprudence on the matter.[103] Article 1 of the European Convention on Human Rights ('ECHR') obliges State parties "secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention." Even though there is a lack of complete consistency in the case law of the ECHR, it has largely been held that State parties must respect the Convention rights even when they operate extraterritorially.[104] In 2008, in the case of *Liberty* v. *UK*, the ECtHR entertained the claim of a violation of the right to privacy by two Irish Non-Governmental Organisations though they were not present in the United Kingdom, since the UK had monitored their private communications.[105]

Yet in the high profile *Big Brother Watch* v. *United Kingdom*, that clubbed a batch of petitions challenging UK's surveillance programs, the ECtHR ducked the direct

[94] Watt, *supra* note 63, 777.
[95] UNHRC, *Report of the Human Rights Committee*, UN Doc. A/50/40), ¶284 (1995).
[96] UNHRC, *Concluding Observations on the US Report Under the ICCPR*, UN Doc CCPR/C/USA/CO/3 (2006).
[97] UNHRC, *Concluding Observations on the Fourth Periodic Report of the United States of America*, UN Doc. CCPR/C/USA/CO/4 (2014).
[98] UNHRC, General Comment No. 31, *Nature of the General Legal Obligation on State Parties to the Covenant*, U.N. Doc. CCPR/C/21/Rev.1/Add.13), ¶10 (26 May, 2004).
[99] UNGA, *Report of the Office of the United Nations High Commissioner for Human Rights the Right to Privacy in the Digital Age*, UN Doc. A/HRC/27/37), ¶30 (2014).
[100] *Id*.
[101] UN-GA, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms whilst Countering Terrorism Ben Emmerson QC*, UN Doc. A/69/397), ¶41 (September 23, 2014).
[102] Ralph Wilde, *Human Rights Beyond Borders at the World Court:The Significance of the International Court Jurisprudence on the Extraterritorial Application of International Human Rights Law Treaties*, 12 CHINESE JOURNAL OF INTERNATIONAL LAW 639 (2013).
[103] Bignami, *supra* note 74, 16.
[104] *Id*; *see* for example, Loizidou v. Turkey, 310 Eur. Ct. H.R. (ser. A) (1995); Al-Skeini v. United Kingdom, 53 Eur. Ct. H.R. 18 (2011).
[105] Liberty v. United Kingdom, Eur. Ct. H.R. (2008).

question of extraterritorial surveillance.[106] The case involved a consolidated challenge to surveillance in the UK through the 'Tempora' program described above and receipt of US intelligence gathered through the 'PRISM' program.[107] In this case, the ECtHR avoided the question of the circumstances under which the Convention would protect individuals located outside the UK but surveilled by the UK government authorities. As there was no contestation made by the UK government on the grounds of extraterritoriality, the court simply assumed that the Convention applied and moved on from there.[108]

Several scholars have also refuted the US position on various grounds.[109] Margulies disputes the US understanding by referring to the ordinary rules of treaty interpretation and grammar.[110] Grammatically, he argues that the phrase "respect to…..all individuals" would be incorrect syntax because the English or French language in which the ICCPR was originally drafted does not envisage respecting rights 'to' right holders but would instead be 'respecting rights with regard to right holders.'[111] Instead, unless we assume that the drafters used poor syntax,[112] a more technically correct textual interpretation of the treaty would imply that Article 2(1) could be severed into two separate sentences—firstly, 'Respect the rights recognized in the present Covenant' and secondly, 'Ensure to all individuals within its territory and subject to its jurisdiction, the rights recognised in the present Covenant'.

As Margulies points out, this interpretation makes the use of the word 'respect' redundant.[113] He argues that it is unlikely that the drafters would have added superfluous words into the treaty without any purpose.[114] Therefore, as the phrase 'ensure' encompasses a broader obligation that already contains the less onerous duty to respect, the rule against superfluity would dictate that both terms be taken into account.[115]

A possible implication of this idea, endorsed by Milanovic is that States are bound by a negative duty to not violate the rights of individuals extraterritorially[116] but have a positive obligation to guarantee obligations to individuals within its territory i.e. wherever they have

---

[106] Big Brother Watch v. United Kingdom, European Court of Human Rights, Applications nos. 58170/13, 62322/14 and 24960/15, September 13, 2018.

[107] Chinmayi Sharma, *Summary: Big Brother Watch and Others. v the United Kingdom*, LAWFARE, October 12, 2019, available at https://www.lawfareblog.com/summary-big-brother-watch-and-others-v-united-kingdom (Last visited on June 15, 2019).

[108] Marko Milanovic, *ECtHR Judgment in Big Brother Watch v UK*, EJIL TALK, September 17th, 2018, available at https://www.ejiltalk.org/ecthr-judgment-in-big-brother-watch-v-uk/ (Last visited on June 15, 2019).

[109] *See* for example, *id*; Van Schaak, *supra* note 93; Margulies, *supra* note 4, 1084.

[110] Margulies, *supra* note 4, 1084.

[111] *Id*.

[112] *Id.*

[113] *Id*.

[114] *Id*.

[115] *Id*. (He also documents interestingly that the US Representative to the ICCPR negotiations also adopted this view during the negotiation process.) *See* U.N. ESCOR Human Rights Committee 6th Session, 193rd meeting, 13, U.N. Doc E/CN/4/SR.193 (May 15, 1950).

[116] But *See*.U.S. Dep't of State, Office of the Legal Advisor, *Memorandum Opinion on the Geographic Scope of Application of the Convention Against Torture and Its Application in Situations of Armed Conflict* (Jan. 21, 2013), available at http://justsecurity.org/wp-content/up loads/2014/03/state-department-cat-memo.pdf in Marko Milanovic, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, (2015)56 Harv Int'l LJ 81, 86, 121 (2015)

overall effective control.[117] By violating the rights of citizens abroad, the United States is therefore, not only violating its own negative obligation under the ICCPR but also preventing other signatories to the ICCPR from discharging the obligations owed to their own citizens under the ICCPR. Further, this leads to the possibility of an anarchic situation globally where the intelligence agencies of each country are legally spying on the citizens of other countries with the end result being that every individual human being has their rights violated.

Bignami and Resta suggest a flexible approach to the preservation of the rights of individuals located extraterritorially where the State has 'virtual control' of information infrastructure, because it is tough to justify a mechanism that denies autonomy and personhood, even to outsiders.[118] By similarly relying on the notions of shared communities and the equal moral worth of individuals, Benvenisti has articulated a credible theory of sovereigns as trustees, where he argues that the minimal obligations sovereigns owe to foreign stakeholders should be as per a restricted Pareto optimal outcome.[119] The minimal obligations should be owed to the extent that discharging those obligations makes the beneficiary better off without making the host State worse off, in the absence of compensation.[120] Policy hawks would argue that not conducting surveillance for national security purposes would violate this restricted Pareto criteria as the 'national security' interests of States may be harmed. However, as we will explore later, a 'ritual incantation' of national security as an excuse for surveillance is not only illegitimate but also harmful for the State concerned.

Margulies argues that the minimal obligations owed in the context of extraterritorial surveillance undertaken by States for national security must be judged by a deferential proportionality standard[121] on the basis of the margin of appreciation doctrine.[122] He justifies his position by citing the promotion of national security interests such as combating terrorist groups or countering the threat posed by foreign fighters. Further, by citing Pozen, Margulies claims that conducting surveillance may shield privacy interests of innocent victims from foreign State or non-state actors.[123] The 'national security' argument will be engaged with, in the next section.

In this section, I have tried to demonstrate that there is some doctrinal certainty on the principle that States are bound to respect the rights of individuals abroad in some form although the modalities are still a point of discussion among scholars.

---

[117] 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*, 31 UTRECHT JOURNAL OF INT'L& EUROPEAN LAW 104, 110 (2015).

[118] Bignami, *supra* note 74, 20.

[119] Eyal Benvenisti, *Sovereigns as trustees of humanity: On the Accountability of States to Foreign Stakeholders*, 107(2) AMERICAN JOURNAL OF INTERNATIONAL LAW 295,297 (2013).

[120] *Id*., 320.

[121] Margulies, *supra* note 4, 1085.

[122] *Id*; Handyside v United Kingdom, 24 Eur Ct. H.R (ser A) (1976), ¶47.

[123] *Id*; David E. Pozen, Essay, 'Privacy-Privacy Tradeoffs' (2016) 83 University of Chicago L.Rev 221, 221-22 (2016), at 229.

B. SURVEY OF JURISPRUDENCE ON RIGHT TO PRIVACY AND MASS SURVEILLANCE

Even though the focus of this paper is on the extraterritorial dimension of surveillance, it is important to understand what international human rights law has to say on the domestic contours of the right when applied to citizens. An institutional framework that caters to citizens can then form a part of the collective discourse. The purpose of this section is to highlight that some amount of doctrinal certainty also exists on the contours of the right to privacy in the context of mass surveillance, although there are some gaps which the jurisprudence is yet to explore.

Article 17 of ICCPR protects the right to privacy against interferences that are 'unlawful' and 'arbitrary'. In General Comment No. 31, the UNHRC has specified that such interference can take place only on the basis of a law that is well-defined and specifies the precise circumstances under which surveillance may be permitted.[124] The notion of arbitrary interference essentially refers to the principle of proportionality and states that any intrusion must be proportionate to the end sought.[125] The relevant UN High Commissioner's report stated that the law enabling a surveillance measure must be accessible to the public, pursue legitimate aims, be precise enough in terms of detailing the limits of this interference and provide for effective remedies against abuse of that right.[126] Any policy that impinges on the right to privacy must thus, never be applied in a manner that impairs the 'essence of that right.'[127]

The operation of Article 8 of the ECHR, concerning the right to respect for private and family life, is similar to that of Article 17, except for the fact that the grounds of limitation are listed in the Article itself. It is provided that interference with the right must be in accordance with law and if it is necessary in a democratic society. As identified by commentators,[128] both the European Court of Justice and the European Court of Human Rights have long stressed that while States enjoy a margin of appreciation in devising surveillance programs in a manner that suits their national security needs, there must also be adequate and effective safeguards against abuse of this right. The assessment has generally considered the nature, scope and duration of the measures in question.[129] In *Szabo* v. *Hungary*,[130] *Zakharov* v. *Russia*[131] and *Liberty* v. *UK*,[132] the ECtHR found that the authorisation requirements mandated by the ECHR had not been met and the executive had virtually unfettered discretion in conducting surveillance in the programs under judicial scrutiny, which lead to those programs being rendered illegal.

[124] UNHRC, *supra* note 98.
[125] Sarah Joseph et al, *The International Covenant on Civil and Political Rights*, 476-477, 533 (3rd ed, 2013).
[126] High Commissioner for Human Rights, *Rep. on the Right to Privacy in the Digital Age*, ¶¶34-35, U.N. Doc. A/HRC/27/37 (June 30, 2014).
[127] UNHRC, *supra* note 98.
[128] Watt, *supra* note 63, 776; Bignami, *supra* note 74, 19; Georgieva, *supra* note 117, 122; Milanovic, *supra* note 116, 137.
[129] Bignami, *supra* note 74, 19.
[130] Szabo and Vissy v. Hungary (App. No. 37138/14) (2016).
[131] Roman Zakharov v. Russia (App. No. 47143/06) (2015) ECHR 1065.
[132] Liberty v. United Kingdom (App. No. 58243/00) (2009) 48 EHRR 1.

In *Weber and Saravia* v. *Germany*,[133] the ECtHR drew a distinction between individualised and strategic surveillance and recognised that safeguards outlined in the German legislation, which was challenged, were adequate for meeting the thresholds of accessibility and foreseeability required by a law authorising strategic surveillance. Interestingly, the court endorsed the use of 'catchwords' which were suitable for filtering data collected through the surveillance mechanisms,[134] which may be an implicit endorsement of algorithmic surveillance.[135]

In summary, the courts have generally provided States with a margin of appreciation in balancing privacy with national security while stressing on safeguards that curtail abuse. There are three major issues with the existing jurisprudence. First, as Benvenisti notes,[136] a 'margin of appreciation' doctrine that reverts policy questions back to national courts defeats the essence of the international human rights project which was designed to protect groups who do not have a say in the domestic democratic process.[137] Benvenisti's logic can be extended to external stakeholders as well. The margin of appreciation doctrine prioritises state sovereignty and the ability to take key decisions on national security over the constraining impact of international human rights law and thereby reduces the protection that foreigners should receive. Use of the doctrine reduces the role of international tribunals that are supposed to ensure the vitality of the human rights project.[138]

In the context of algorithmic surveillance, granting a margin of appreciation is particularly dangerous. This brings me onto my second point of contention with established law and policy—a flawed but 'ritual incantation'[139] of national security. Granting a margin of appreciation allows States to continuously exert their sovereign right to provide security for their citizens. However, strategically the link between mass surveillance and the prevention of security threats is highly questionable.

As highlighted by 'security guru' Bruce Schneier, surveillance makes the internet less secure as it legitimises the exploitation of data and eavesdropping, both by States and non-state actors.[140] This effectively means that the data of US citizens may be subject to surveillance by foreign actors which could cause them to repose less trust in the architecture of the internet, which may then have a detrimental impact on the extent to which the internet plays a role in global commerce and trade flows. Therefore, a world without mass surveillance conducted by any country may theoretically meet Benvenisti's criteria of restricted Pareto optimality which was discussed in the previous section.

---

[133] Weber and Saravia v. Germany, (2006) ECHR 1173 97.
[134] *Id*.
[135] Murphy, *supra* note 14, 229.
[136] Eyal Benvenisti, *Margin of Appreciation, Consensus and Universal Standards*, 31 INTERNATIONAL LAW AND POLITICS 843,844 (1993).
[137] *See* Fionnuala Ni Aolain, *The Emergence of Diversity: Differences in Human Rights Jurisprudence*, 19 FORDHAM INTERNATIONAL LAW JOURNAL, 101, 114, 119 (1995) (Argues that States that supposedly adhere to democratic principles are granted a wider margin) quoted in Benvenisti 844
[138] Benvenisti, *supra* note 138, 852.
[139] Phrase adapted from Christine Gray's 'ritual incantation of a magic formula of self-defense'. CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 125 (4th ed., 2018).
[140] Bruce Schneier, *How the NSA makes the internet less secure*, THE ATLANTIC, January 6, 2014, available at https://www.theatlantic.com/technology/archive/2014/01/how-the-nsa-threatens-national-security/282822/ (Last visited on June 21, 2019).

It is crucial to note here that the 'national security' value of bulk targeting is grossly exaggerated. A pioneering study by the New American Foundation found that NSA surveillance of all kinds on both US citizens and foreigners played an initiating role in 7.5% of terror cases.[141] The bulk collection of metadata may have played a role only in 1.8% of cases, if at all.[142] In *Klayman* v. *Obama*, the US District Court for the District of Columbia stated that the NSA had failed to show even one instance where the bulk targeting program had succeeded in preventing an imminent terrorist attack.[143]

As identified by Donohue, the problem with the bulk collection and subsequent algorithmic processing is that these processes rely on variables that link the individual with a network of some sort.[144] It would be easy to profile someone who regularly attends or communicates with members of Al-Qaeda. Further, his pattern of actions would derive correlatory profiles with other Al-Qaeda members by extrapolating his pattern of actions. Unfortunately, most terrorists operate in individual cells, not in social networks.[145] They also operate in unfamiliar geographic and cultural contexts, which enable them to obfuscate their 'digital selves' by incorporating false inputs that might confuse the algorithm that has been bred in the West. Thus, the same limitations of algorithms that could lead to the illegitimate profiling of innocent individuals might allow terrorists to get away unidentified. Therefore, the portrayal of national security as a definite benefit of mass surveillance is an argument which we must take with many pinches of salt.

In fact, the converse may be true. A focus on national security may actually cause insecurity in two ways. First, excessive discourse on 'securitisation' makes the average citizen more fearful of unknown security threats and thus, likely to be subjected to a feeling of being less secure.[146] The citizen fears an outsider who is unknown and thus, constituted to be the 'other.'[147] The constituting of 'the other' is through a conglomeration of complex gendered and racialized pathologies which evoke fear of any entity that deviates from the normal.[148] Second, the reason for a feeling of insecurity lies in a lowered trust of the state machinery itself due to the layers of uncertainty that pervade the surveillance production process.[149] There is a perceived security threat not just from 'the other' but also from the 'known unknown' of the government machinery that threatens the democratic values which a person's conception of a dignified life may also be founded on.[150]

---

[141] Peter Bergen et al, *Do NSA's Bulk Surveillance Programs Stop Terrorists?*, NEW AMERICA, January 2014, available at https://www.newamerica.org/documents/871/Do-NSAs-Bulk-Surveillance-Programs-Stop-Terrorists.pdf (Last visited on June 21, 2019).

[142] *Id*.

[143] Klayman v. Obama, 957 F Supp 2d. 1 (2013).

[144] DONOHUE, *supra* note 64, 44.

[145] *Id*.

[146] Lucia Zedner, *The Pursuit of Security* in CRIME RISK AND SECURITY 200, 202 (Tim Hope & Richard Sparks, ed., 2000).

[147] Claudia Aradau & Tobias Blanke, *Governing others: Anomaly and the algorithmic subject of security*, 3 EUROPEAN JOURNAL OF INTERNATIONAL SECURITY 1,5 (2017).

[148] *Id*; DAVID CAMPBELL, WRITING SECURITY: UNITED STATES FOREIGN POLICY AND THE POLITICS OF IDENTITY 7 (1992).

[149] Chandler, *supra* note 11, 123.

[150] Arnold Wolfers, *National Security as an Ambiguous Symbol*, 67(4) POLITICAL SCIENCE 481,485 (1952) (cited in Chandler, *supra* note 11, 122).

Finally, as validly identified by Hughes, courts have refrained from an analysis of privacy as an integral aspect of modern democratic society.[151] After a rigorous survey of the jurisprudence of the ECtHR, she concludes that the court's analysis of the value of privacy of democracy is highly limited and its exploration of privacy as a gateway right to intellectual development is largely unexplored.[152] Not defining the social value of privacy reduces the costs of surveillance to a mere intrusion that can be balanced out with the need for national security.[153] It misses entirely the multiple and diverse benefits that a well-defined right to privacy has for both individual and collective well-being.[154] This gap, along with the margin of appreciation gifts policy makers the discretion to subvert privacy protection to an exercise in legal compliance rather than an endeavour to respond to broader social processes.

These gaps in jurisprudence need to be rectified for the universal human rights project to have genuine meaning. Correcting through the jurisprudence of supra-national institutions is particularly crucial for the protection of the rights of foreigners, for whom they are the sole mechanisms for rights enforcement. This would be a crucial first step. However, as the next Chapter of the paper will demonstrate, such rectification would not be enough by itself to genuinely guarantee protection due to difficulties of enforcement.

IV. CHALLENGES IN ENFORCING AN INSTITUTIONAL FRAMEWORK RELIANT ON PROCEDURAL SAFEGUARDS

As will be explored in this Chapter, there seems to be a point of departure between legal scholarship and jurists who view the solution in procedural terms and seek to extend the rights-based project for this purpose, and social scientists who theorise on the basis of the subjective lived experiences without referring to the institutional framework that endeavours to protect these lived experiences. Policy makers tend to rely on legal scholarship as it is easier to justify policy through procedural safeguards without having to enter the contentious and politicised realm of lived experiences. PPD-28 for example, claims that national security implications of mass surveillance can be balanced by developing a framework of procedural safeguards. Symbiosis between these two elements is required for the development of a common framework that seeks to further the universal human rights project.

This Chapter considers in its first section why procedural safeguards may not be an entirely adequate mechanism for protecting human rights and then uses this analysis in the following section to respond to literature that endeavours to use these procedural safeguards to create a code of conduct for the regulation of extraterritorial surveillance.

A. THE LACUNAE IN PROCEDURAL SAFEGUARDS

The issue with using 'procedural safeguards' as a solution to the problem lies perhaps in the nature of rights themselves. There are, broadly speaking, two facets of a human right—the right as codified in the Constitution or international convention which can be litigated

[151] Kirsty Hughes, *The social value of privacy, the value of privacy to society and human rights discourse* in SOCIAL DIMENSIONS OF PRIVACY: INTER-DISCIPLINARY PERSPECTIVES 225, 236 (Beate Rossler & Dorota Mokrosinska, ed., 2015).
[152] *See* NEIL RICHARDS, INTELLECTUAL PRIVACY (2015).
[153] Hughes, *supra* note 151, 240.
[154] *Id*.

in a court in the case of violation of that right, and the lived experiences, subjective emotions or normative moral dogma that lead to the deliberative discourse which prompted the creation of that right. Cass Sunstein notes in his pioneering paper, 'Incompletely Theorized Agreements in Constitutional Law' that the Universal Declaration of Human Rights emerged despite disagreement and uncertainty on the foundations of the rights that were ultimately codified in the instrument.[155]

Claims of violations through litigation are against codified versions of the right, not the lived experiences that were violated as a consequence of the violation. For example, if an individual is denied a job by the State on account of his race, the court will have to decide whether the employer discriminated on one of the prohibited grounds and if at all, this discrimination was justified. The judge does not have to tread the murky waters of the impact of this violation on the emotional state of the victim since this impact could be entirely subjective. Obviously, all plaintiffs will recognise that there has been a violation of their right to equality but some plaintiffs may be angrier or more saddened by this violation than others.

In the case of privacy, most courts have adopted a 'reasonable expectation of privacy' approach to adjudicating cases where they simply decide whether an objective individual would have desired privacy in the defined context and whether the violation amounted to an arbitrary or unlawful interference into the individual's private sphere.[156] However, we must bear in mind that the reasons behind the codification of both these rights were the lived experiences of human beings that lead to the genesis of the universal rights-creation project. People wanted a right to free speech for the experience of being able to express their thoughts freely. Similarly, a right to privacy has its origins in the experience of being able to carve out the boundaries of one's private sphere and delimit the contours of one's public personality.

Indeed, at the domestic institutional level, it may be argued validly, as Sunstein does, that there is no need to debate the multifarious reasons behind the existence of a right and the subjective experiences that shape it.[157] This is because the courts exist as a mechanism for enforcement of codified rights. The recognition of a violation and the granting of a remedy would likely validate the purpose of the right and redress the victim's emotional grievance as well. Extraterritorial surveillance driven by big data and algorithmic processing alters this construct due to the interplay between the multiple components of the policy problem.

Strategically adhering to extraterritorial human rights obligations may not be in the State's best interests. Robert Axelrod had constructed an 'iterative prisoner's dilemma' situation to model multilateral cooperation in such circumstances.[158] He argued that States would have an incentive to not defect from the co-operative equilibrium in case of repeated encounters as the reputation of being defectors would cause other State to engage in 'tit-for-tat' punishment against them. This is already being seen in the surveillance context with States expressing dissent

[155] Cass R. Sunstein, *Incompletely Theorized Agreements in Constitutional Law*, 74(1) SOCIAL RESEARCH 1, 7 (2007).
[156] Frederic Sourgens, *The Privacy Principle*, 42(2) YALE JOURNAL OF INTERNATIONAL LAW 345, 351 (2017).
[157] Sunstein, *supra* note 155, 11.
[158] ROBERT AXELROD, THE EVOLUTION OF CO-OPERATION 174 (1984).

against the US[159] and using it as a justification for 'data localisation.'[160] Brazil and the European Union have chosen to relay $185 million worth of fiber optic cables towards this effort.[161] However, the attainment of co-operative equilibrium is conditional on the other States being able to adequately punish the defector such that the payoffs from defecting are outweighed.

That is not the case in the present scenario of extraterritorial surveillance. There is a wide power imbalance driven by both technological and economic factors between the US along with its 'Five Eyes' partners[162] and the rest of the world. This means that it is unlikely that India will develop surveillance capabilities akin to that of the NSA, re-orient internet infrastructure or relocate 'choke points' to weed out American influence in the global technological sphere. Outrage at the United Nations may be symbolically beneficial but it is unlikely that it would change State policy at the institutional level in the absence of the nature of political outrage that we witnessed at the aftermath of the Snowden revelations. Therefore, the likelihood of occurrence of a 'tit for tat' scenario, where the defector is punished is low.

The payoffs from continuing to engage in surveillance outweigh the reputational costs which the United States might suffer, simply because the prospective mechanisms of punishment are not strong enough. This is precisely why the United States has not altered its mass surveillance program in response to institutional pushback. PPD-28 is a policy document that sought to respond more to public pressure from American who were angered by the Snowden revelations[163] rather than international pressure. In order to elicit any form of change in the policy framework, attention must be devoted to bottom up extitutional approaches rather than relying on notions of extraterritorial human rights obligations that boast of doctrinal certainty but do little to alter incentive structures for the framing of national policy.

Additionally, the question of surveillance has taken on a whole new dimension. The information we generate digitally has taken the 'production process' of surveillance outside traditional institutional spaces and transformed it into a post-panopticonic phenomenon[164] as a "form of enclosure that does not depend on interiors."[165] It is no longer simply a 'right to be left alone,' as originally conceptualised by Warren and Brandeis, but additionally a process of

---

[159] U.S. spy scandal triggers outrage, paranoia in Germany, NBC NEWS, April 2, 2014, available https://www.nbcnews.com/storyline/nsa-snooping/u-s-spy-scandal-triggers-outrage-paranoia-germany-n170366 (Last visited on June 21, 2019).

[160] Arindrajit Basu et al, *The Localisation Gambit: Unpacking policy oves for the sovereign control of data in India*, CENTRE FOR INTERNET & SOCIETY, March 19, 2019, available at https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf (Last visited on June 21, 2019).

[161] Angelica Mari, *High Expectations for Brazil undersea cable to Europe*, BRAZIL TECH, February 12, 2014, available at https://www.zdnet.com/article/high-expectations-for-brazil-undersea-cable-to-europe/ (Last visited on June 21, 2019).

[162] *See also* Corey Pfluke, *A history of the Five Eyes Alliance: Possibility for reform and additions*, 38(4) COMPARATIVE STRATEGY 304-305 (2019).

[163] *See* David R. Shedd, *How Obama Unilaterally Chilled Surveillance*, WALL STREET JOURNAL, November 29, 2015, available at https://www.wsj.com/articles/how-obama-unilaterally-chilled-surveillance-1448833262 (Last visited on June 22, 2019).

[164] Thomas Mathiesen, *The viewer society: Michel Foucault's "Panopticon" revisited*, 1(2) THEORETICAL CRIMINOLOGY 215 (1997).

[165] William Bogard, *Simulation and post-panopticon* in ROUTLEDGE HANDBOOK OF SURVEILLANCE STUDIES 30-37 (Kirstie Ball et al, ed., 2012).

'boundary management'[166] that enables us to thrive autonomously in a digital world.[167] The wording of the ICCPR, which defines the right to privacy merely as an 'arbitrary or unlawful' interference into the lives of individuals is important but the contours of arbitrariness and unlawfulness have taken on a new avatar—something that international institutions or even the codification of international human rights law is ill-equipped to handle completely in its present state.

B. THE FALLACY OF INTERNATIONAL CODES

Deeks advocates for a procedural safeguards driven framework regulating international surveillance. She cautions against attempting to develop consensus on the substantive law, as harmonising the subjectivities of privacy across cultural contexts to come up with an 'international right to privacy' may not be possible.[168] Instead, she identifies six procedural safeguards that could make up this code.[169] First, she calls for legality and notice of applicable rules which envisages that individuals know the extent to which all States conduct surveillance and which entities within these States are responsible for these operations.[170] Second, she stresses on the limits to data collection by identifying a clear set of purposes.[171] Third, she calls for a periodic review of the authorisation of surveillance.[172] Fourth, there must be a limit placed on data retention.[173] In her fifth norm, she articulates that States should give preference to the State where the action is taking place, to conduct surveillance.[174] Finally, she recommends the setting up of an international neutral oversight body to ensure the implementation of this code.[175] Watt recommends the same set of guidelines in her conception of an international treaty regulating the activities of intelligence agencies.[176]

Any international code of conduct that creates safeguards and charts the boundaries of a specific system of action is useful as long as there is a robust institutional framework to enforce the code.[177] Periodic reviews or limits on data retention work well when there is an independent and autonomous judicial or administrative body to enforce these standards. Further, the code of procedural safeguards usually stems from a recognition of the fact that the act in question has the potential to cause harm in the absence of that code, even though the specific, subjective contours of that harm is rarely incorporated into the code itself.

Deeks justifies the utility of this framework by putting forward three arguments. First, she argues that political pressure in the aftermath of the Snowden leaks produced

---

[166] Julie Cohen, *What Privacy is For*, 126 HARVARD LAW REVIEW 1905 (2013).
[167] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4(5) HARVARD LAW REVIEW 193 (1890).
[168] Ashley Deeks, *An International Legal Framework for Surveillance*, 55(2) VIRGINIA JOURNAL OF INTERNATIONAL LAW 296 (2015).
[169] *Id*., 351.
[170] *Id*., 354.
[171] *Id*., 354, 357.
[172] *Id*., 359.
[173] *Id*.
[174] *Id*., 359-360.
[175] *Id*., 361-362.
[176] Watt, *supra* note 63, 784.
[177] For example, the World Trade Organisation mechanism that enforces economic sanction might present a credible threat.

significant pressure from foreign States on the US government to alter its activities.[178] The reason political pressure is unlikely to work lies in the definite gains from defection by the more powerful States and the strategically flexible nature of the pressure itself. Notably, the most problematic component of US law, §702 was re-authorised by the Congress in 2018. Further, despite opposing US policy at the United Nations, Germany itself wanted to be a part of the 'Five Eyes' group of allies that conducts surveillance on the rest of the world as that would strategically benefit Germany.[179]

Deeks' second justification lies in the envisioning of a universal environment that ensures the enforcement of fundamental rights through international tribunals or domestic courts.[180] Research suggests that there is a limited correlation between the pressures exerted by international human rights bodies and State behaviour.[181] Domestic courts naturally have more teeth but are less likely to be responsive to the claims of foreigners in a manner that alters foreign policy. In the United States context, the case of *United States* v. *Verdugo-Urquidez* clearly stated that non US-citizens located extraterritorially and lacking a 'substantial connection' to the United States should have no Fourth Amendment Protections.[182] Similarly, recent cases in the United Kingdom on mass surveillance have only declared it illegal when conducted on citizens and does not expand this scope to non-citizens yet.[183] Therefore, judging from existing jurisprudential trends, it is unlikely that domestic institutions in the States conducting surveillance will act as enforcement mechanisms for the rights of the victims.

Instead, incorporating procedural safeguards in an international code may allow States to evade the reputational costs of conducting surveillance as well. By demonstrating supposed procedural compliance with the standards in the code, States can avoid discussion on the substantive, moral and socio-psychological ramifications of surveillance.[184] Any form of surveillance comes with costs, even if done in a manner that complies with procedural safeguards. Even if there was a hypothetical robust international institution that could enforce rights-based claims, the deviation of focus from the protection of rights to mere procedural compliance is a possible harm of devising an international code in the manner Deeks contemplates.

Deeks' final justification lies in economic pressures from the NSA's corporate partners, whose overseas business may be threatened if non-citizens are made aware of the prospects of continuous surveillance.[185] This aspect is worth considering. Microsoft, for example, has attempted to protect the data of its customers in the European Union by setting up a

[178] Deeks, *supra* note 168, 328.
[179] Peter Spiegel, *Angela Merkel eyes place for Germany in US Five Eyes Club*, THE FINANCIAL TIMES, October 25, 2013, available at https://www.ft.com/content/e2492a3a-3d7a-11e3-9928-00144feab7de (Last visited on June 24, 2019).
[180] Deeks, *supra* note 168, 333.
[181] Daniel W. Hill Jr., *Estimating the effects of Human Rights Treaties on State Behaviour*, 72(4) THE JOURNAL OF POLITICS 1161,1163 (2010).
[182] United States v. Verdugo-Urquidez, 494 U.S. 259.
[183] Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, (2016) UKIPTrib 15_11-CH; Secretary of State for the Home Department v Watson, (2018) EWCA Civ 70.
[184] *See* Chase Madar, *Samantha Power and the weaponization of human rights*, COUNTER PUNCH, September 10, 2009, available at www.counterpunch.org/2009/09/10/samantha-power-and-the-weaponization-of-human-rights/ (Last visited on June 25, 2019).
[185] Deeks, *supra* note 168, 338.

'data trustee' model through which a local German telecom provider Deutsche Telekom acts as a trustee of the data of European citizens and protects it from unwarranted intrusion by foreign surveillance agencies.[186] However, this pressure does not come due to the existence of an international agreement but from discursive political dialogue by customers. In fact, as Schulhofer validly points out, an international legal treaty may have damaging consequences for political dialogue.[187]

An international legal framework would bring to the table security service providers who seek to negotiate more permissive thresholds of privacy violation. Economic pressure on service providers driven by political dialogue is likely to focus on the lived experiences of the rights and require responses that cater to some of these subjective elements. Claims made in this manner are more likely to cause service providers to compete among themselves to deliver solutions that appeal to the lived experiences and expectations of the most number of customers. An international treaty made up of procedural safeguards would allow service providers to contest claims by customers and justify their more relaxed policies on the supposed grounds of legality.

The reliance on international human rights as a workable body of law that fosters compliance needs to be reconsidered. Through future research, alternate approaches to conceptualising human rights and galvanising consensus among relevant stakeholders—private sector, government, civil society, and most important citizens will be essential for international human rights to retain any value. Failure to do so will result in continued irrelevance further damaged by false reverence.

V. CONCLUSION

The policy problems in today's rapidly evolving world are inherently multi-faceted and multi-dimensional. Internet governance, climate change and the refugee crisis are all problems which cannot be defined through one research question but require several inter-disciplinary approaches to be resolved adequately. Human rights law continues to be an essential construct for safeguarding human liberties and dignity in today's world but arguably lacks teeth as international institutions are threatened by inward-looking States whose populations have become increasingly averse to the 'outsiders', who are perceived to take up jobs, fuel religious fundamentalism and threaten the edifice of national security.

With this construct in mind, this paper attempted to engage with the complex contours of the problem of extraterritorial algorithmic surveillance. Each element of the policy problem amplifies the vulnerability of the non-citizen whose data is targeted without consent and aggregated by a non-sentient machine to create an algorithmic profile that may not capture all facets of his personality but still converts him into the subject of a process he has no say in crafting. In an ideal world, where the doctrinal constructs of international law could be enforced against all actors, perhaps refining the law to account for the modern ramifications of technological advancement would be enough to safeguard the vulnerable.

---

[186] Data Trustee Principle, MICROSOFT AZURE, July 4, 201, available at https://docs.microsoft.com/en-us/azure/germany/germany-overview-data-trustee (Last visited on June 25, 2019).

[187] Stephen Schulhofer, *An International Right to Privacy? Be careful what you wish for*, 14 (1) INTERNATIONAL JOURNAL OF CONSTITUTIONAL LAW 218,257 (2016).

Yet, technological change has only amplified the power imbalance between States, which means that the countries which possess the greatest capability to conduct mass surveillance also have the least incentive to comply with human rights law due to the lack of a credible threat of punishment. The United States and its Five Eyes partners control a disproportionate extent of internet infrastructure and continue to conduct mass surveillance on foreigners. Other States are unable to prevent these violations, either through threats of punishment or through international institutions that can compel these States to comply. Procedural safeguards can subsequently be weaponised by those with greater weight in global institutions and geo-political processes to evade reputational costs rather than actively seeking to protect the vulnerable, and the powerless.

A new agenda for conceptualising human rights, given the imbalances in global technological advancements is the need of the hour. Ongoing research that I am undertaking looks at understanding human rights through bottom up processes of social interaction, among individual rather than a top down process of normative development. The conception of human rights as a solely normative endeavour is under constant pressure. The future of human rights lies in lawyers, activists and private sector actors getting back to the drawing board and arriving at ways in which it can be used as a tool to facilitate human interaction and collaboration, rather than a normative framework that enables its weaponisation by the powerful.