

A RIGHT TO PRIVACY UNDER MASS SURVEILLANCE?

Samuel I. Horowitz*

INTRODUCTION	332
II. THE RIGHT TO PRIVACY	332
A. <i>The Right to Privacy in the Digital Age</i>	336
B. <i>The Right to Privacy as it Relates to Other Human Rights</i>	337
C. <i>States' Duty to Protect Privacy</i>	337
III. STATE COUNTER-TERRORISM PRACTICES.....	339
A. <i>Mass Surveillance around the World</i>	340
IV. BALANCING THE RIGHT TO PRIVACY AND THE OBLIGATION TO COUNTER TERRORISM.....	343
V. CONCLUSION	344

* J.D., 2020, University of Minnesota Law School; B.A., 2017, University of Wisconsin-Madison; A.A., 2014, Defense Language Institute. The author is a practicing attorney with experience and an educational background in international relations, international organizations, human rights law, humanitarian law, criminal law, and environmental law.

INTRODUCTION

A multitude of human rights are implicated by state counterterrorism practices—not least of which is the right to privacy. The right to privacy is a necessary prerequisite to the exercise or enjoyment of other fundamental human rights such as the right to family, freedom of peaceful assembly, freedom of association, and freedom of opinion and expression.¹ Mass surveillance has given governments unprecedented access to private information.² As use of the internet and digital communication technologies have become necessities for most humans, and will likely only increase in importance, it is crucial that individuals' right to privacy in this area be sufficiently protected from governmental and private interference. Section I of this paper provides an overview of the right to privacy, the impact of digital technologies on that right, and states' duties to protect that right. Section II provides examples of mass surveillance programs around the world. Section III presents the challenge of balancing security and privacy in a world where states may be held responsible both for failing to prevent acts of terrorism as well as for violating human rights, including the right to privacy.

II. THE RIGHT TO PRIVACY

Privacy itself has been defined as “the presumption that individuals should have an area of personal autonomous development, interaction and liberty free from State intervention and excessive unsolicited intrusion by other uninvited individuals.”³ In other words, privacy is the right to be left alone.

1. High Comm'r for Hum. Rts., *Right to Privacy in the Digital Age*, ¶ 14, U.N. Doc. A/HRC/27/37 (June 30, 2014) [hereinafter *Right to Privacy in the Digital Age*].

2. See Fergal Davis et al., *Mapping the Terrain*, in *SURVEILLANCE, COUNTER-TERRORISM AND COMPARATIVE CONSTITUTIONALISM* 3, 4, 9 (Fergal Davis et al. eds., 2014); David Cole, *Preserving Privacy in a Digital Age: Lessons of Comparative Constitutionalism*, in *SURVEILLANCE, COUNTER-TERRORISM AND COMPARATIVE CONSTITUTIONALISM* 95, 96–97 (Fergal Davis et al. eds., 2014).

3. U.N. Secretary-General, *Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, ¶ 28, U.N. Doc. A/69/397, (Sept. 23, 2014).

The right to privacy is enshrined in Article 12 of the Universal Declaration of Human Rights (UDHR),⁴ Article 17 of the International Covenant on Civil and Political Rights (ICCPR),⁵ Article 16 of the Convention on the Rights of the Child (CRC),⁶ Article 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (ICMW),⁷ Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR),⁸ and Article 11 of the American Convention on Human Rights (ACHR).⁹ It is also found in a number of other regional human rights treaties and in individual States' constitutions.¹⁰

Article 12 of the UDHR states that “[n]o 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.”¹¹ Article 17 of the ICCPR contains nearly identical language to Article 12 of the UDHR, but prohibits “unlawful” interference and attacks as well.¹²

Both the UDHR and ICCPR would appear, on their faces, to prohibit states from engaging in mass surveillance. Mass surveillance is inherently indiscriminate in that it is not aimed at a particular individual reasonably suspected of having engaged

4. G.A. Res. 217 (III) A, Universal Declaration of Human Rights, at art. 12 (Dec. 10, 1948) [hereinafter UDHR].

5. International Covenant on Civil and Political Rights art. 17(1), Dec. 16, 1966, S. Treaty Doc. No. 95-20, 999 U.N.T.S. 171 [hereinafter ICCPR].

6. Convention on the Rights of the Child art. 16, Sept. 2, 1990, 1577 U.N.T.S. 3.

7. International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families art. 14, Dec. 18, 1990, 2220 U.N.T.S. 3.

8. Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221, E.T.S. 5 [hereinafter ECHR].

9. American Convention on Human Rights art. 11, Nov. 22, 1969, O.A.S.T.S. No. 36, 1144 U.N.T.S. 144.

10. See Office of the High Comm’r for Human Rights, *International Standards Special Rapporteur on the Right to Privacy*, HUMAN RIGHTS TOPICS, <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx> (last visited Feb. 8, 2024); *Legal Issues Concerning Transit Agency Use of Electronic Customer Data*, NAT’L ACADS. OF SCIS. ENG’G & MED., Mar. 2017, at 36.

11. UDHR, *supra* note 4, at art. 12.

12. ICCPR, *supra* note 5, art. 17(1)–(2).

in unlawful conduct.¹³ Contrary to state practice, these privacy articles additionally seem to require states to enact legislation prohibiting, as opposed to authorizing, mass surveillance. Legislation like the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act,¹⁴ the Philippine Human Security Act (HSA),¹⁵ the Indian Prevention of Terrorism Act (POTA),¹⁶ and the Canadian Anti-Terrorism Act (ATA),¹⁷ would seem to violate the second part of these articles in an effort to make mass surveillance lawful and therefore compliant with the lawfulness prong of the first part.

The right to privacy in Article 8 of the ECHR differs from that found in the UDHR and ICCPR. Article 8 provides that “[e]veryone has the *right to respect* for his private and family life,

13. See Gerald Staberock, *Intelligence and Counter-Terrorism: Towards a Human Rights and Accountability Framework?*, in COUNTER-TERRORISM: INT’L L. & PRAC. 351, 366 (Ana María Salinas de Frías et al. eds. 2012) (“[M]odern interception techniques of signal intelligence are typically not individualized as was the case with more traditional forms of wiretapping; instead, they are often based on the automatic searches of specified criteria.”); William C. Banks, *The United States a Decade after 9/11*, in GLOB. ANTI-TERRORISM L. & POL’Y 449, 470, 474–75 (Victor V. Ramraj et al. eds., 2d ed. 2012) (asserting that the USA PATRIOT Act allowed the FBI to request information from parties without having to show the suspect’s involvement in terrorism or espionage and that it is possible for officials to use databases and algorithms to search through millions of emails and phone calls for suspicious activities). *Contra* Sudha N. Setty, *The United States*, in COMPAR. COUNTER-TERRORISM L. 49, 56–57 (Kent Roach ed., 2015) (stating that FISA requires law enforcement to show probable cause and “undertake a minimization process” to exclude individuals and communications that are not under investigation).

14. 21313 See Cole, *supra* note 2, at 103; Banks, *supra* note 13, at 471–73; Setty, *supra* note 13, at 49–52, 58–59; Kent Roach, *Thematic Conclusions and Future Challenges*, in COMPAR. COUNTER-TERRORISM L. 683, 722 (Kent Roach ed., 2015); DORLE HELLMUTH, COUNTERTERRORISM AND THE STATE: WESTERN RESPONSES TO 9/11 34 (2016).

15. See H. Harry L. Roque, Jr., *The Human Security Act and the IHL Law of the Philippines: of Security and Insecurity*, in GLOBAL ANTI-TERRORISM L. & POL’Y 310, 323–25 (Victor V. Ramraj et al. eds., 2012); see also Human Rights Committee, *Concluding Observations on the Fourth Periodic Report of the Philippines*, ¶ 15, U.N. Doc. CCPR/C/PHL/CO/4 (Nov. 13, 2012) (addressing reports that human rights defenders have been subjected to surveillance by law enforcement and recommending that the state take measures to ensure compliance of its surveillance programs with Article 17).

16. See Ujjwal Kumar Singh, *Mapping Anti-Terror Legal Regimes in India*, in GLOB. ANTI-TERRORISM L. & POL’Y 420, 428–36 (Victor V. Ramraj et al. eds., 2d ed. 2012).

17. See Robert Diab, *Canada*, in COMPAR. COUNTER-TERRORISM L. 78, 88–90 (Kent Roach, ed., 2015) (“Yet the act still contemplates a form of mass warrantless surveillance similar to what is permitted in the United States”).

his home and his correspondence.”¹⁸ Instead of an outright prohibition on arbitrary or unlawful interference with privacy, Article 8 is written as a right to respect for private life. However, in practice, the European Court of Human Rights has held that the purpose of Article 8 is “to protect the individual against arbitrary action by the public authorities.”¹⁹ The largest distinction between the right to privacy in the ECHR and the UDHR and ICCPR is that Article 8 includes an explicit limitation clause. The limitation clause states:

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.²⁰

The European Court of Human Rights has—in line with other jurisprudence on limitations—required that interference with privacy be “in accordance with the law, in pursuit of a legitimate aim, and necessary in a democratic society.”²¹

Despite its importance, the right to privacy is not an absolute right.²² It may be the subject of derogation and, though lacking an explicit limitation clause, would seemingly be subject to

18. ECHR, *supra* note 8, art. 8(1) (emphasis added).

19. *Kroon and Others v. The Netherlands*, App. No 18535/91 ¶ 31 (27/10/1994), <https://www.refworld.org/jurisprudence/caselaw/echr/1994/en/114141>.

20. ECHR, *supra* note 8, art. 8(2).

21. EUROPEAN COURT OF HUMAN RIGHTS, GUIDE ON ARTICLE 8 OF THE CONVENTION—RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE 8 [hereinafter Guide on Article 8].

22. See Merris Amos, *The Impact of Human Rights Law on Measures of Mass Surveillance in the United Kingdom*, in SURVEILLANCE, COUNTER-TERRORISM AND COMPARATIVE CONSTITUTIONALISM 152, 167 (Fergal Davis et al. eds., 2014) (“Private life, as protected by art 8 of the ECHR, is not an absolute right.”).

limitation provided that any interference with the right is “neither arbitrary nor unlawful.”²³

A. *The Right to Privacy in the Digital Age*

The use of digital communications technology has made it possible to connect all of humanity almost instantaneously. It serves as a vehicle through which people can share their opinions and experiences with an ever-widening audience. It allows people to work more efficiently and productively from anywhere in the world. In the case of migratory workers, it allows them to stay in touch with the families they have left behind and to send remittances so that their families can support themselves. From the mundane task of finding the nearest coffee shop or grocery store, to the ability of world leaders on opposite sides of the globe to meet and communicate in real-time, this technology provides humanity with unprecedented problem-solving powers.²⁴

However, this same technology that provides unprecedented benefits also creates unprecedented vulnerabilities. These vulnerabilities are not limited to the states and private actors that rely on digital networks to govern and run their businesses. They apply—definitely more intimately—to the individual whose every movement in her community or around the world is tracked by the GPS device in her phone, whose financial and health information exists digitally, whose relatives and associates communicate with her on her phone, and whose musings, political views, and activities of the past decade are recorded on her social media profiles.²⁵

Just as these tools can be powerfully used to “amplify [...] the voices of human rights defenders” and “offer the promise of improved enjoyment of human rights[,]” they can also be used by those opposed to those goals to locate dissenters, expropriate or freeze assets, and silence political opponents.²⁶

23. Right to Privacy in the Digital Age, *supra* note 1, ¶ 21.

24. *See id.* ¶ 1.

25. *See* Davis, *supra* note 2 *see also* Right to Privacy in the Digital Age, *supra* note 1, ¶ 1.

26. Right to Privacy in the Digital Age, *supra* note 1, ¶¶ 1–3.

B. *The Right to Privacy as it Relates to Other Human Rights*

The right to privacy is a fundamental human right,²⁷ and a number of other rights rely on it for their enjoyment and full realization.²⁸ When state practice threatens or violates the right to privacy, these other rights are also implicated and individuals may be unable to exercise them fully. At its most extreme, mass surveillance can be used to identify individuals suspected of engaging in terrorist acts. Once located, those individuals may be detained or even targeted by the state, resulting in a potential violation of the right to life. Evidence gathered through mass surveillance may be used against an individual in a criminal trial resulting in a due process violation if they are unable to access the evidence due to national security exemptions. An individual's dignity may be violated if mass surveillance results in the capture of embarrassing private information. Privileges between attorneys and their clients or doctors and their patients may also be violated when their communications are swept up in mass surveillance programs.

C. *States' Duty to Protect Privacy*

As discussed in Section II above, various human rights treaties—in particular the ICCPR and the ECHR—protect an individual's right to privacy from unlawful or arbitrary interference. These treaties impose both negative and positive obligations on states parties. A state's negative obligations require it and its agents to refrain from interfering with privacy rights. Its positive obligations require it to prevent interference

27. Jens Kremer, *On the End of Freedom in Public Places: Legal Challenges of Wide-Area and Multiple-Sensor Surveillance Systems*, in *SURVEILLANCE, COUNTER-TERRORISM AND COMPARATIVE CONSTITUTIONALISM* 117, 124 (Fergal Davis et al., eds. 2019).

28. 1222See Right to Privacy in the Digital Age, *supra* note 1, ¶ 14 at 5; see also Cole, *supra* note 2, at 104 (stating that after information has been gathered in violation of the right to privacy, it may implicate other rights including freedom from discrimination, due process, and other similar rights); Amos, *supra* note 22, at 154 (listing freedom of association and expression and loss of status as a person by being transformed into a mere "collection of data" as harms resulting from privacy violations through surveillance); Priv. Int'l, *Privacy and Human Rights: An International Survey of Privacy Laws and Practice*, GLOBAL INTERNET LIBERTY CAMPAIGN, (last visited May 13, 2019), <http://gilc.org/privacy/survey/intro.html>.

with privacy rights by non-state or private actors and pass legislation protecting privacy rights and prohibiting interference with the same.²⁹ Specifically, as it relates to mass surveillance, the Human Rights Committee (HRC) stated that

Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.³⁰

The privacy rights in the ICCPR and ECHR differ in that Article 17 of the ICCPR contains no explicit limitation clause, while Article 8 of the ECHR does. However, the terms “arbitrary” and “unlawful” in Article 17 have been interpreted as authorizing some interference with privacy rights.³¹ Thus, in practice, interference with privacy rights under both bodies is governed by the “principles of legality, necessity[,] and proportionality.”³² It does not appear that it is possible for a state to engage in mass surveillance as such within these parameters.³³

Privacy rights under both bodies are also subject to derogation, provided the requirements imposed by Article 4 of the ICCPR and Article 15 of the ECHR are met. Both provisions

29. Human Rights Committee, General Comment No. 16 ¶¶ 1–2 (Apr. 8, 1988) [hereinafter General Comment 16]; Guide on Article 8, *supra* note 21.

30. General Comment 16, *supra* note 29, ¶ 8.

31. See General Comment 16, *supra* note 29, ¶¶ 3–4; Right to Privacy in the Digital Age, *supra* note 1, ¶¶ 21–23.

32. Right to Privacy in the Digital Age, *supra* note 1, ¶ 23.

33. See *id.* ¶ 20 at 6; see also Human Rights Committee, Concluding Observations on the Sixth Periodic Report of Hungary, ¶¶ 43–44, U.N. Doc. CCPR/C/HUN/CO/6 (May 9, 2018); Human Rights Committee, Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, ¶ 24, U.N. Doc. CCPR/C/GBR/CO/7 (Aug. 17, 2015); *Szabó & Vissy v. Hungary*, App. No. 37138/14, 52, ¶ 11. (Jan. 12, 2016), <https://hudoc.echr.coe.int/eng?i=001-160020>.

require the existence of a public emergency that threatens the life of the nation, that the state party officially proclaim a state of emergency, that the measures taken be limited “to the extent strictly required by the exigencies of the situation,” and that the measures taken are not inconsistent with the state’s other obligations under international law.³⁴ States taking advantage of the derogation clause must also notify the relevant treaty bodies of the provisions from which they are derogating and the reasons for those derogations.³⁵ Though courts and treaty bodies have recognized a “margin of appreciation” as an acknowledgement of a potential state of emergency, the other requirements—especially notice requirements³⁶—are more strictly enforced. Given the requirements that notice must be provided and that such notice must provide “a sufficiently detailed account of the relevant facts,”³⁷ it is unlikely that a state’s mass surveillance program could be a valid derogation from its responsibilities under Article 17. This is especially true considering that such programs have become the norm,³⁸ as opposed to exceptional measures.³⁹

III. STATE COUNTER-TERRORISM PRACTICES

States have a very clear obligation to ensure the safety of civilians within their jurisdiction and—especially following post-9/11 Security Council resolutions—to criminalize, prevent, and punish acts of terrorism.⁴⁰ This obligation requires states “to carry out protection by ‘due diligence,’ which means that *all reasonable measures* under the circumstances must be taken to

34. ICCPR, *supra* note 5, art. 4(1); ECHR, *supra* note 8, art. 15(1).

35. ICCPR, *supra* note 5, art. 4(3); ECHR, *supra* note 8, art. 15(3).

36. See Human Rights Committee, General Comment 29 ¶ 17 (July 24, 2001); see also *Silva v. Uruguay*, Communication No. 34/1978 (1981).

37. *Silva v. Uruguay*, Communication No. 34/1978 (1981).

38. See *Right to Privacy in the Digital Age*, *supra* note 1, ¶ 3; Davis et al., *supra* note 2, at 4.

39. See PHILIP ALSTON & RYAN GOODMAN, INTERNATIONAL HUMAN RIGHTS 394 (2013).

40. VINCENT-JOËL PROULX, TRANSNATIONAL TERRORISM AND STATE ACCOUNTABILITY: A NEW THEORY OF PREVENTION 30–32 (2012); TAL BECKER, TERRORISM AND THE STATE: RETHINKING THE RULES OF STATE RESPONSIBILITY 131 (2006).

prevent terrorist acts.”⁴¹ The exercise of due diligence requires “where possible, the use of modern technologies to monitor [terrorist] activity.”⁴² Due diligence has also been defined as “as a duty on the State to use all the administrative, legal and security measures at its disposal to prevent and suppress terrorist and related activity as effectively as possible.”⁴³ As a method of prevention, states have employed mass surveillance to identify individuals who are engaged in, or who are likely to engage in, terrorist acts and to monitor, detain, prosecute or eliminate them.

A. Mass Surveillance around the World

It is not surprising that the United States, having been the target of the attacks on 9/11, has led the world in the adoption and application of mass surveillance counterterrorism measures.⁴⁴ Following the passage of the USA PATRIOT Act, the executive branch—and the NSA and FBI in particular—were given *carte blanche* to engage in mass surveillance without the safeguards of judicial oversight.⁴⁵ In its Concluding Observations on the Fourth Periodic Review of the United States in 2014, the HRC expressed its continuing concern at the scale and scope of the U.S. surveillance programs and the continuing lack of sufficient oversight.⁴⁶ The mass surveillance counterterrorism

41. PROULX, *supra* note 40, at 31 (emphasis added) (quoting JA McCredie, *The Responsibility of States for Private Acts of International Terrorism*, 1 TEMPLE INT'L & COMP. L. J. 69, 86); see also BECKER, *supra* note 40, at 132 (“[A] standard of due diligence is entailed, requiring the State to use all means at its disposal to prevent and suppress terrorist activity.”).

42. *Id.* at 135.

43. 40*Id.* at 142.

44. See HELLMUTH, *supra* note 14, at 34; DAVID J. WHITTAKER, COUNTER-TERRORISM AND HUMAN RIGHTS 109 (2009); see also Cole, *supra* note 2, at 96 (stating that U.S. phone companies responded to 1.3 million law enforcement data requests in 2001 alone while British companies responded to 2.7 million from 2005 to 2010).

45. See Human Rights Committee, Concluding Observations of the Human Rights Committee, ¶ 21, U.N. Doc. CCPR/C/USA/CO/3/Rev.1, (Dec. 18, 2006) [hereinafter 2006 US Concluding Observations]; Setty, *supra* note 13, at 58–59.

46. See Human Rights Committee, Concluding Observations on the Fourth Periodic Report of the United States of America, ¶ 22, U.N. Doc. CCPR/C/USA/CO/4, (Apr. 23, 2014).

practices of the United States are especially problematic because other countries may follow suit when they procure the ability to do so.⁴⁷ Other nations have indeed already followed suit and established mass surveillance programs or passed legislation expanding the government's authority to engage in surveillance.

Canada's ATA allows law enforcement to obtain wiretaps that last for a year, avoid notice requirements for individuals subjected to surveillance for up to three years, and intercept communications of individuals in Canada as long as "the interceptions are 'directed at foreign entities located outside Canada.'"⁴⁸ It may also be possible for information gathered by Canada's intelligence services to be used in administrative or criminal proceedings.⁴⁹ Despite the similarities between Canada's surveillance program and that of the United States, Canada's has not been abused to the same extent.⁵⁰

In Colombia, "prosecutors may authorize electronic surveillance [on the internet and 'other computer-based systems'] of suspects based on preliminary evidence" under Article 54 of Law 1453 of 2011.⁵¹

Mass surveillance is especially problematic in Singapore because its "Constitution does not provide for a constitutional right to privacy."⁵² Additionally, Singapore has "no laws . . . that explicitly prohibit the use of wiretaps and other forms of surveillance, including electronic ones."⁵³ There is also little, if any, oversight and there are no laws prohibiting the admission of

47. See Setty, *supra* note 13, at 77.

48. Diab, *supra* note 17, at 88, 90.

49. *Id.* at 89.

50. *Id.* at 109; but see *id.*, at 90 (explaining that although the Canadian ATA anticipates the privacy concerns of Canadians by requiring that "satisfactory measures are in place to protect the privacy of Canadians and to ensure the private communications will only be used or retained if they are essential to international affairs, defense or security. . .", the act still "contemplates a form of mass warrantless surveillance similar to what is permitted in the United States...").

51. Luz E. Nagle, *Columbia*, in COMPAR. COUNTER-TERRORISM L. 115, 137 (Kent Roach, ed., 2015).

52. Eugene K. B. Tan, *Singapore*, in COMPAR. COUNTER-TERRORISM L. 610, 628 (Kent Roach, ed., 2015).

53. *Id.* at 627.

evidence obtained through surveillance in preventive detention procedures or criminal prosecutions.⁵⁴

In India, the POTA introduced “provisions pertaining to the interception of electronic communication and their admissibility as evidence in court”⁵⁵ Though repealed in 2004, POTA’s surveillance provisions were imported into the Unlawful Activities Prevention Act (UAPA).⁵⁶

Indonesia’s Anti-Terrorism Law allows “an investigator [to] use any intelligence report as preliminary evidence” in a criminal procedure.⁵⁷ Investigators can also “request information from banks and other financial institutions regarding the assets of any person who is known or strongly suspected of having committed a criminal act of terrorism.”⁵⁸ Investigators are also able to “open, examine and confiscate mail and packages by post or other means of delivery and ‘[...] intercept any conversation by telephone or other means of communication suspected of being used to prepare, plan and commit a criminal act of terrorism.’”⁵⁹

In the Philippines, the HSA “grants law enforcement agencies the power to intercept any communication described in it”⁶⁰ The law allows for the interception of personal communications and does not provide for exemptions, which has led to the law being challenged by a priest.⁶¹ The law does not establish guidelines or provide limitations for the means and methods that law enforcement may use to intercept communications.⁶² Unlike the USA PATRIOT Act, the HSA does not include a “sunset” provision for communications surveillance.⁶³

These examples—spanning the globe—show how readily states have adopted mass surveillance as a counterterrorism tool. The glaring lack of oversight and specificity in these programs

54. *Id.*

55. Singh, *supra* note 16, at 430.

56. *Id.* at 420, 439.

57. Hikmahanto Juwana, *Anti-Terrorism Efforts in Indonesia*, 11 *INDON. J. INT’L L.* 151, 156 (2014).

58. *Id.* at 156–57.

59. *Id.* at 157.

60. Roque, *supra* note 15, at 323.

61. *Id.* at 314.

62. *Id.* at 324.

63. *Id.*

and those like them presents a severe threat to the right to privacy world-wide.

IV. BALANCING THE RIGHT TO PRIVACY AND THE OBLIGATION TO COUNTER TERRORISM

Perhaps nowhere is the balance between security and liberty in the counterterrorism field more implicated than with regard to mass surveillance and the right to privacy. A state's obligation to prevent terrorism and the concomitant duty to exercise due diligence creates a Catch-22 in its human rights obligations, especially those dealing with to privacy. A state, provided it either has or should have requested international assistance in building its counterterrorism capacities, can be held responsible for not preventing a terrorist attack if it knew or should have known of the attack. If a state has the means to engage in mass surveillance and does so, it may be assumed that the state had constructive knowledge of the attack and can therefore be held responsible.⁶⁴ However, if a state does engage in mass surveillance, it opens itself up to liability for violating the right to privacy and the host of other rights implicated by it.⁶⁵

Though beyond the scope of this paper, this dilemma is further complicated by the links between terrorism and the denial of civil liberties in general. Krueger and others have identified "civil liberties [as] an important determinant of terrorism."⁶⁶ The relationship also flows both ways as "terrorism *can* lead to a lack of civil liberties [because of a state's counterterrorism efforts], and vice versa."⁶⁷

64. BECKER, *supra* note 40, at 140 ("Assuming actual or constructive knowledge of terrorist activity, the State will violate its obligations if it *in fact* failed to reasonably harness the powers at its disposal to prevent the activity.").

65. See Right to Privacy in the Digital Age, *supra* note 1.

66. ALAN B. KRUEGER, WHAT MAKES A TERRORIST: ECONOMICS AND THE ROOTS OF TERRORISM 89 (2007); see also TODD SANDLER, TERRORISM: WHAT EVERYONE NEEDS TO KNOW 29 (2018) ("[L]ack of basic civil freedoms, and not poverty, appears to influence transnational terrorism.") (citing Claude Berrebi, *Evidence about the Link between Education, Poverty and Terrorism among Palestinians*, 13 PEACE ECON., PEACE SCI., & PUB. POL'Y 1, 1–36 (2007)).

67. KRUEGER, *supra* note 66, at 148.

Despite the dangers of mass surveillance to privacy, many civilians seem to acquiesce to living in a surveillance state out of fear.⁶⁸

V. CONCLUSION

Mass surveillance may indeed be a very effective way to detect and prevent acts of terrorism.⁶⁹ However, by its very nature, it is applied indiscriminately and implicates the privacy rights of entire populations, as opposed to only those reasonably suspected of engaging in terrorist activities.⁷⁰ States should be permitted to only engage in surveillance against those who are reasonably suspected of engaging in terrorism. There must also be sufficient oversight of surveillance practices, either from the legislative or judicial branches of government. It is difficult for individuals who have had their privacy violated to hold state actors accountable because they may never know or be able to prove they were subjected to surveillance that violated their privacy.⁷¹ As the executive branch of the government is the one to which extensive surveillance powers are given, it falls to the legislature, judiciary, and civil society to impose limits on such power.⁷² As privacy is “a

68. See SANDLER, *supra* note 66, at 40–41 (“[i]n such dire times, the electorate will tolerate the loss of some civil liberties. Following 9/11[...] [t]he USA PATRIOT Act suspended certain liberties by, among other things, allowing for greater surveillance.”); WHITTAKER, *supra* note 44, at 114 (“[M]ost Americans, frightened by the media bogey of Terror, seem ready to let go of privacy concerns as soon as their safety is in danger.”).

69. Amos, *supra* note 22, at 154 (“[T]here is convincing evidence that mass surveillance has, for example, averted enormous loss of life from planned terrorist attacks, led to the apprehension and conviction of a notorious serial child killer or regenerated a previously unsafe area of a city with resulting benefits to businesses and local residents.”).

70. 13See Staberock, *supra* note 13, at 366.

71. See *id.* at 367 (“[T]hose affected by intelligence surveillance will not—unlike their counterparts in law enforcement and criminal justice surveillance—learn about the measures unless, exceptionally, they are notified accordingly.”); Cian C. Murphy, *Transatlantic Perspectives on Counter-Terrorism Surveillance: Surveillance, Borders and the Culture of Legality*, in SURVEILLANCE, COUNTER-TERRORISM & COMPAR. CONSTITUTIONALISM 175, 186 (Fergal Davis et al., eds. 2014) (“The inability to ascertain precisely what data are being held makes it more difficult to challenge unlawful use of those data.”); see also 2006 US Concluding Observations, *supra* note 45 (“In particular, the Committee is concerned about the restricted possibilities for the affected persons to be informed about such measures and for them and recipients to effectively challenge them.”).

72. See Right to Privacy in the Digital Age, *supra* note 1, ¶¶ 37–38.

civil right whose scope is in part dependent on social context and therefore whose erosion is not always easily identifiable[,]”⁷³ it is crucial that the descent into a surveillance or police state “be subject to contest and justification”⁷⁴ at every opportunity.

73. Murphy, *supra* note 71, at 186.

74. *Id.* at 187.

