laws

MDPI

Article

Pegasus Project: Re-Questioning the Legality of the Cyber-Surveillance Mechanism

Atul Alexander * and Tushar Krishna

Department of Law, West Bengal National University of Juridical Sciences, Kolkata 700098, West Bengal, India
* Correspondence: atulalexander100@nujs.edu

Abstract: States have recently indulged in purchasing surveillance spyware such as Pegasus from big corporations such as the NSO Group to track the activities of its people to curb dissidents. Unfortunately, such incidences are not new in the international domain. Thus, it is imperative to analyze the legality of such spyware used by the states with the assistance of foreign corporates under the international framework. In view of the same, the paper while majorly focusing on the significance of right to privacy, traces the standing limitations in the legal mechanism and tries to propose a shared responsibility regime for states and surveillance companies indulging in human rights violations by drawing parallels with the ICoCA mechanism.

Keywords: Pegasus; surveillance; corporate liability; human rights; spyware

Citation: Alexander, Atul, and Tushar Krishna. 2022. Pegasus Project: Re-Questioning the Legality of the Cyber-Surveillance Mechanism. *Laws* 11: 85. https://doi.org/10.3390/laws11060085

Academic Editors: Esther Salmerón-Manzano and Francisco Manzano Agugliaro

Received: 13 September 2022
Accepted: 18 November 2022
Published: 23 November 2022

1. Introduction

On 18 July 2021, Amnesty International and Forbidden Stories revealed that several thousand political leaders, human rights workers, and journalists are under the widespread surveillance of Niv, Shalev, and Omri Group (NSO Group) using Pegasus spyware in their mobile phones (Khan 2022). As per the report, Pegasus spyware, unlike other spyware, does not require its victim to open any link; rather, the spyware can be inserted into any device with a simple missed call on any individual's mobile number. Amnesty International has also claimed that once inserted, the spyware can automatically operate its victim's mobile microphone or even camera to trace its victim's activities.[1] Nonetheless, the NSO Group has completely denied any illegal usage of its software, claiming that the company provides such spyware "only to Government intelligence and law enforcement agencies" with the objective of curbing terror activities or other serious offences.[2] It is also noteworthy that the terms and conditions for using the spyware are merely contractual, which means that its violation would only make the NSO Group entitled to basic municipal remedies ranging from black listing, liquated damages, or non-continuance of the service, without having any redressal for the shattering effect on individuals' human rights (Saxena 2022). Considering such devastating potential of Pegasus spyware, the UN Human Rights Experts have called for "a global moratorium" on the sale and use of such "life-threatening" spyware until concrete regulatory framework is developed to address the severe impact of such technology on human rights.[3]

1 Forensic Methodology Report: How to catch NSO Group's Pegasus. 2022. Amnesty International. Available online: https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/ (accessed on 30 August 2022).

2 "We license it only to the law enforcement and intelligence agencies of sovereign states. Nor do we have any knowledge of the individuals whom states might be investigating, nor the plots they are trying to disrupt, as is otherwise standard amongst our corporate peers." Transparency and Responsibility Report of 2021 NSO Group. Available online: https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf (accessed on 30 August 2022).

3 Pegasus: Human rights-compliant laws needed to regulate spyware. 2022. *United Nations*. Available online: https://news.un.org/en/story/2021/07/1096142 (accessed on 30 August 2022).

To analyze the abovementioned concerns, the authors have split the article into six parts. **Part I** lays down the background for the subsequent discussions by underlying the current position of international human rights law against cyber-surveillance in order to understand recent developments in the cyber-surveillance industry. **Part II** depicts the limitations of international law, which is primarily state-centric, in holding the liability of the corporates (such as the NSO Group) involved in cyber-surveillance, thereby violating the human rights of its victims. While doing so, the article focuses on two main points: first, the state-centric mechanism under international law, and, second, the inadequacy of the present soft laws. **Part III** draws a parallel between cyber-surveillance companies (such as the NSO Group) and private military and security companies (PMSCs) to understand whether the act of surveillance can be considered an "inherent state function". **Part IV** analyzes the viability of "a shared responsibility regime" for redressing human rights violations based on the multi-stakeholder mechanism of the International Code of Conduct for Private Security Service Providers' Association (ICoCA). **Part V** provides other potential solutions: the first is redefining the concept of privacy in the context of cyber surveillance, and the second is the application of human rights treaties in instances of extraterritorial cyber surveillance. Finally, **Part VI** gives concluding remarks along with some suggestions.

2. Background—Tracing the Violation of Human Rights Owing to Cyber-Surveillance

Many scholars have already validated the argument that the increase in technological enhancement cannot be seen solely from the positive side. The states are using these technologies for their national security and providing a platform for an individual's voice (La Rue 2013; McKune 2019; Chan 2019; Daly 2022). Rather, these technological enhancements have led to enhancement in mass surveillance via the states on their citizens (Karavias 2015). Here, it is necessary to understand that Pegasus is not an unusual case; in other words, there is indeed a larger international market in surveillance technology where international transfer of such technology happens commonly. The United Nations Commission on Human Rights (UNHRC), in its report, has acknowledged that the usage of commercially available cyber-surveillance technologies by authoritarian regimes is a worldwide policy issue (UNCHR 2019). The application of cyber-surveillance technologies for despotic purposes has been discussed since the early 2010s (Schaake 2015). Following the Arab Spring, the private surveillance sector, which had hitherto avoided public scrutiny, was thrust into the limelight for the first time. Numerous western firms' surveillance devices were linked to human rights breaches in nations that employed these technologies for oppressive objectives. Here, one example is an Egyptian case during Mubarak's ouster in which a UK-based firm, Gamma International and FinFisher, which was a subsidiary of Gamma International, provided the application of its spyware FinSpy to the Egyptian government in surveillance, hunting down human rights activists and any dissent (Fuchs 2012; Timm 2012). FinSpy is deployed surreptitiously on target devices and observes conversations, texts, and data transfers. It can even activate the target device's microphone or camera, very much akin to Pegasus. Some other significant instances include (network-based) surveillance systems built by Amesys (used in Libya), Trovicor (used in Bahrain), Blue Coat (used in Syria), and Sandvine (used in Egypt) (Marquis-Boire et al. 2013; Electronic Frontier Foundation 2012; Human Rights Watch 2014; Penney et al. 2018; Privacy International 2016; Silver and Elgin 2011; Coker and Sonne 2011). All these companies are based in Western countries; however, in recent years, the surveillance sector has drawn the attention of companies from other regions as well (most importantly China).[4] The emerging Chinese surveillance enterprises have taken the opportunity to export and promote their surveillance models not just in totalitarian or semi-totalitarian states but also in liberal democracies (Feldstein 2019; Qiang 2019; Rolley 2019). As a result, their presence can be traced in the regions of Africa and Asia with several government clients (Cave et al. 2019; Gwagwa 2018; Mozur and Chan

[4] Many of these countries have also signed onto China's Belt and Road Initiative and its "smart city" projects, including the mass surveillance program. See (Feldstein 2019, pp. 13–15; Shahbaz 2018, pp. 6–9).

2019). Therefore, there is no doubt that Pegasus is not an isolated example, and there is a broader worldwide industry in surveillance technologies, with frequent foreign transfers of such technology.

Jennifer Daskal, one of the eminent jurists in the field of cyberlaw, has suggested that "the data collected using these mass surveillance touches on a bucket of relation rights that privacy protections safeguard" (Daskal 2016). These rights include rights to speech and expression, the right to assemble, and the right to free movement. Among these, one of the most directly affected rights is "the right to privacy", which prompted the authors to concentrate this paper's scope primarily on the right to privacy. It is a well-recognized human right globally that has been incorporated into several national legislatures (either explicitly or implicitly) (Global Internet Liberty Campaign 2022). Article 17 International Covenant on Civil and Political Rights, 1966 (ICCPR), makes the contracting parties ensure the individual's civil and political rights. In other words:

> "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation, and everyone has the right to the protection of the law against such interference or attacks".[5]

This provision can also be seen under Article 12 of the Universal Declaration of Human Rights (another component of the International Bill of Rights), Article 16 of the Convention on the Rights of the Child (1987), and Article 22 of the Convention on the Rights of Persons with Disabilities (2007).[6] Several regional instruments have also recognized privacy as a well-settled fundamental right of individuals.[7] Indeed, in 1988, the scope of the right to privacy was expanded with the adoption of General Comment 16 on ICCPR Article 17 in the beginning of recognizing the concerns of cyber-surveillance. It says, "the gathering and holding of personal information on computers, databanks and other devices by public authorities or private individuals or bodies, must be regulated by law".[8] Even on analyzing the jurisprudence of the Human Rights Committee, the article emphasizes an obligation of the states to take positive steps toward "giving effect to the prohibition of and protection against unlawful or arbitrary interference and attacks against the individual's privacy, whether emanated from state authorities or natural or legal persons".[9] It further recognized the requirement of state legislation to govern the framework of the processing the personal information by both states and private actors.[10] Such an expanded approach can also be traced from the EU's jurisprudence. For example, the European Court of Human Rights (ECtHR), in *MK* v. *France*,[11] observed that "the protection of personal data was of fundamental importance to a person's enjoyment of his or her right to respect for private life".[12] In the recent judgment of *Schrems* v. *Data Protection Commissioner*,[13] it was held that even the legislation enabling government authorities "a generalized basis for the content of electronic communications" must be considered as violating the core component of the

5 Article 17(1). International Covenant on Civil and Political Rights, 1966.

6 Although the language of the provisions of the latter two conventions is not exactly the same as Article 17 of ICCPR, the essence of the provision remains the same.

7 See, for example, Article 7, Charter of Fundamental Rights of the European Union, Art. 7. The American Convention on Human Rights, Art. 11., Article 8, The European Convention of Human Rights, Art. 8. Article 16 and 21, The Arab Charter on Human Rights, Art, 16,21. (Articles 16 and 21).

8 UNHRC. General Comment No. 16. Available online: https://www.refworld.org/docid/453883f922.html (accessed on 30 August 2022). Para. 10.

9 UN Human Rights Committee (HRC). 1988. CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation. Available online: https://www.refworld.org/docid/453883f922.html (accessed on 30 August 2022). Paras. 1, 8, 9, 31.

10 Human Rights Committee. General comment No. 16. Available online: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf (accessed on 30 August 2022) Para. 16, Human Rights Committee. A/HRC/17/27. Para. 58.

11 App No. 19522/09 (2013) ECHR.

12 S & Marper v. the United Kingdom [GC] App. Nos. 21439/04 and 30566/04 (2008) ECHR.

13 Case C—362/14 (6 October 2015), para. 94.

rights to privacy guaranteed under Article 7 of the Charter of Fundamental Rights of the EU. Even in jurisdictions like the United States of America (US), where some government officials claimed that there is no constitutional right to privacy because of the absence of any express right to privacy in the US Constitution, judicial precedents subsequent to the *Griswold* v. *Connecticut* set a favorable jurisprudence toward the right to privacy. For example, *Eisenstadt* v. *Baird* and *Lawrence* v. *Texas* are the most well-known instances in which the American court has expanded the right to privacy.[14] Thus, there is no doubt that an individual's right to privacy is an intrinsic, legal principle under international, as well as national domain.

However, trends in technological advancement have led to the intensification of mass surveillance, which is different from the conventional model of policing (centralized on detecting the crime) both *quantitatively* (the amount of data accessibility) and *qualitatively* (ways of evaluation and processing of data) (Mitsilegas 2016). In 2013, when the former CIA agent Edward Snowden revealed the US National Security Agency's "*Prism Program*"—an unrestricted mass surveillance program carried out on not only US citizens but also all internet users across the globe (Mihr 2014)[15]—several scholars raised concerns about the application of such surveillance in crushing down any democratic movement against the government (UNHRC 2013a, Para. 46; Mendel 2012, p. 43; Gupta 2013). Here, one may argue that the way Pegasus spyware works, targeted at specific individuals and specific devices, is different from the given example of the massive NSA metadata collection effort that Snowden leaked (mass surveillance); however, more than 10,000 numbers in the Moroccan group of the database, as indicated by several media houses (Timberg et al. 2021; George 2021; Chawala 2021), indicate the contrary. Therefore, the personal data collected using Pegasus spyware has raised the vulnerability of using such data to stifle anyone's right to privacy or to identify targets for arbitrary arrests or even torture or death (Daskal 2016). Although this article's scope does not extend to detail the different allegations made against Pegasus, there is no doubt that the mere presence of such spyware without any proper regulatory framework has in itself raised concern about every individual's right to privacy. Such arguments seem to be more forceful in light of the past incidents of torture and detention using cutting-edge surveillance technologies (Sonne and Coker 2022; Coker and Sonne 2011).

3. Limitations under International Law in Tracing Corporate Liability for Violating Human Rights

Under the contemporary international law regime, it is not easy to uphold the obligation of a corporate because international law is centralized on the legal obligations of states with very limited emphasis on non-state actors.[16] Further, the regulating principles such as the UN Guiding Principles of Business and Human rights, Reports of Human Rights Committees, or even UNGA Resolutions, are non-binding[17] and merely serve as guiding instruments (McBeth and NolanAdam McBeth) (McBeth and Nolan 2012; Tully 2012, p. 247). For a better elaboration of these limitations, this part is divided further into the following sub-parts:

3.1. State-Centric Mechanism of International Law

International law looks upon states as the "primary actors" (reflected from the international relations theory's primary approach, in other words, *realism*); thereby, it is evident to

[14] Cornell Law School on Griswold. Privacy. Available online: https://www.law.cornell.edu/wex/privacy#:~:text=%E2%80%8BIn%20Griswold%2C%20the%20Supreme,to%20privacy%20in%20the%20Constitution (accessed 5 July 2022).

[15] Edward Snowden. Leaks That Exposed US Spy Programme. BBC. Available online: http://www.bbc.com/news/world-us-canada-23123964 (accessed 5 January 2022).

[16] The reason to make specific reference to International Humanitarian law is that it is mainly associated with criminal liability which is not often applicable against the legal persons like corporate. (Karavias 2013, p. 19; Vazquez 2005).

[17] UNHR. 2012. The Corporate Responsibility to Respect Human Rights HR/PUB/12/02 (2012), 1.

have obligations and duties only on the part of states or state actors (Karavias 2013, p. 10). There is a certain inclination toward bringing individuals into the picture post-World War II; however, such inclination primarily focuses on the nexus between the state and its nationals (Karavias 2013, p. 19). In the context of international human rights law, the major reason for its emergence is the protection of the individual's rights against the state's arbitrary actions and not against the actions of non-state actors, including private individuals or a corporate body (Karavias 2013, pp. 19–21). It often seems rare to directly address corporate actions under international law, except for cases like jus cogens (Vazquez 2005). Similarly, in the recent past, the concern about the responsibility of international organizations was raised after the adoption of the Articles on Responsibility of International Organisations in 2011; however, "in lack of clear basis of obligation and the threshold of proving international organizations attributability and violation of international legal obligation resting on the organization concerned, it becomes difficult to hold organizations responsible, whether actions or omissions". (Klabbers 2017) Additional hardship is added by the international organizations' special privileges and immunities.[18] Thus, in the standing reality, only informal pressure can be exerted on international organizations by influencing their source of funding or by other similar means absent of any hard enforcement (Pirvan 2021). Moreover, international law in contemporary times appears to be addressing the actions of the corporates in an indirect fashion, which means regulations are mainly brought to make a state enforce certain regulations toward such corporations (Vazquez 2005). Therefore, international law enforcement has a very narrow scope for non-state actors, including corporates. This argument can even be extended to argue that public international law has not matured enough to adopt the realities of the post-globalized world (Ryngaert 2015). Therefore, despite an increase in the adverse implications of the conduct of non-state actors such as big corporates, international law remains centralized toward state obligation. In other words, there is no direct recourse toward the conduct of corporates violating conventional or customary international law, including human rights law, other than municipal laws (Rivera 2015).

3.2. The Inefficiency of the Present Soft Laws

The UN and other international organizations have appeared to frame a voluntaristic obligation mechanism for the corporations, which needs the corporates to voluntarily bind themselves to some guiding principles to safeguard human rights (Layne 2015). The advent of these frameworks can be traced from the early 1970s when at the request of the United Nations Economic and Social Council, the Commission on Transnational Corporations was formulated in 1973 to frame a corporate code of conduct. However, it dissolved in 1994 because of the conflict between developed and developing nations on ratifying a common code (Deva 2012). In 1999, while addressing the World Economic Forum, UN Secretary-General Kofi Annan launched a non-binding principle-based mechanism for businesses known as the UN Global Compact programme (Layne 2015). It asked corporates to voluntarily become its members to ensure human rights protections and conformity with human rights principles (Layne 2015). Although more than 15,000 companies will join the program by 2021(United Nations Global Compact 2022), scholars claim that the sole purpose of the corporates joining such membership is merely to pacify their stakeholders and to have publicity without any real intention of protecting human rights (Layne 2015). Again, in 2003, the UN Sub-Commission on the Promotion and Protection of Human Rights launched a set of norms, non-binding in nature, for the corporates to ensure conformity with the human rights principles (Layne 2015). However, those norms were disapproved by the UN Commission on Human Rights.

To confront the contentious debate over businesses and human rights obligations, the UN Commission on Human Rights urged the appointment of a special representative on the

[18] (UN 1946). Convention on the Privileges and Immunities of the Specialized Agencies of the United Nations of 1947, 33 UNTS 261.

subject (Commission on Human Rights 2005). This ultimately resulted in the appointment of John Ruggie, who established the framework of "Protect, Respect, and Remedy", which underlines the state's obligation to safeguard businesses from human rights violations. Ruggie's efforts culminated in the UN Human Rights Council endorsing the "Guiding Principles of Business and Human Rights (the Guiding Principles)" in 2011 (Ruggie 2011), and it seemed to cease any business conduct violating human rights (Rivera 2019). It is based on three basic principles:

> "First, state duties to protect against third party human rights violations through appropriate policies and regulation; second, corporate responsibility to respect human rights through the exercise of due diligence, including human rights impact assessments, tracking and monitoring and other measures; and third, access by victims of human rights abuses to effective remedies, both judicial and non-judicial". (Ruggie 2007)

However, one of the problems with this guideline is that it merely reiterates the standing legal obligations, which are not that effective in redressing corporate violations of human rights. For example, several principles (for example, Principle 1, Principle 4, and Principle 5) restate the established law as laid down under ARSIWA.

Further, the Guiding Principles are non-binding, solely based on the voluntary acceptance of its principle (Layne 2015). Some scholars argue that these Guiding Principles have brought "Transnational Private Regulations (TPR)," where the corporates engage in self-monitoring (Ryngaert 2015, pp. 99–101). However, such TPR is mostly restricted in states promoting CSR (Ryngaert 2015, p. 108). Further, such TPR is also mostly based on the pressure put on them by the consumers and other stakeholders, thereby "having no genuine desire to change the business policies". (Ryngaert 2015, p. 108) Thus, in a general sense, it is conspicuous that the legal hurdles (apart from the economic hurdles—another major factor) in establishing the case in an international forum have made it almost improbable for the victim to bring her/his claim due to the requirement of, *first*, satisfying jurisdiction in the nation (which generally needs the incorporation of that corporation in that other nation); *second*, tracing the applicable laws in the matter; *third*, the corporate need to have voluntarily undertaken certain guidance to be government, otherwise international law simply becomes a namesake with little meaning or obligation. Therefore, the standing international framework has left the victims of human rights violations with no feasible redressal mechanism against the accused corporations indulging in surveillance.

3.3. Other Hardships in Holding a Corporate Entity Liable for Human Rights Violations

Victims of human rights violations also face hardship in taking action against any particular corporate entity under its national laws (Wallace 2017). One of the best instances would be the *Kiobel case,* in which the US Supreme court "undermined the usage of the Alien Tort Statute (ATS)—the major source of transnational human rights litigation in the US—by putting foreign corporates' violation of human rights out of the scope of ATS" (Karavias 2015).[19] A similar situation can also be traced in other jurisdictions (Baughen 2015). Further, applying legal doctrines like forum non-conveniens (inconvenient forum) makes it more difficult for the victims to seek redressal of their infringement within their nations (Wallace 2017). However, overlooking that cyber torts such as cyber-surveillance can take place from any place globally, the application of forum non-conveniens is highly possible, leading to an accountability gap, which further narrows down the scope of redressal mechanism for victims.

However, considering the nature of these conducts of surveillance, which is highly vulnerable to the human rights of individuals and requires a formal regulation for its usage, it seems important to regard such conduct as inherent state conducts in order to attach more obligations while carrying out cyber-surveillance.

[19] *Kiobel v. Royal Dutch Petroleum Co., 569 US 108 (2013)*, Paras. 115–119. (Karavias 2015).

4. Drawing a Parallel with the PMSC Industry: In Terms of Analyzing Inherent State Activity

Most states engaged in digital surveillance in furtherance of their so-called national security. Thus, it is questionable if such conduct can be deemed an inherent state activity restricted to the state alone (Sullivan 2010). Here, it is imperative to draw a parallel with the private military and security firms (PMSCs), for which the UN Working Group on the Use of Mercenaries has suggested an international framework confirming that the state must retain monopolistic control over industries dealing with inherently state activities (White 2011). There are certain conducts—"direct involvement in hostilities, war or combat operations, the capturing of captives, lawmaking, espionage, spying and the transmission of information with military, security and police application" (United Nations 2010)—which a state cannot outsource or delegate (United Nations 2010). Clearly, the application of digital surveillance systems also attracts the concept of inherent state function. Only state participation gives the act of surveillance some sort of justifiable legitimacy, backed by reasons such as countering terrorist action or other highly criminal actions; otherwise, this cyber-surveillance is in itself prima facie unlawful.[20]

Apart from drawing a parallel from the PMSC industry in terms of the inherent state functions, it also offers the International Code of Conduct for Private Security Service Providers' Association (ICoCA) mechanism to consider in the context of industries indulging in spying activities.[21] The member companies of ICoCA are required to embrace the Montreux principles (which were the precursor to the UN Guiding Principles) and to confirm that they have a responsibility to respect human rights and fulfil humanitarian obligations toward all those affected by their business activities [. . .].[22] Importantly, the ICoCA has equal representation from the state, commerce, and the civil society,[23] which on the other hand, certifies,[24] monitors,[25] and handles the complaints against the corporate entities.[26] Apart from providing the governance and oversight mechanism, it also offers an open-for-all complaint mechanism against any kind of harm caused or violation of the code involving the ICoCA members and affiliated countries.[27] In the last few years, ICoCA implementation seems to be getting more stringent. As per the last annual Report of ICoCA, three companies had their membership cancelled owing to the non-submission of the yearly assessment of the company and the other two companies due to cooperation in bad faith.[28] It can be regarded as the strength of the ICoCA mechanism that prompted major PMSCs to call for more rigorous guidance, particularly for enterprises working in challenging environments. Indeed, big clients of PMSCs have already started referencing the ICoC in their agreements. Indeed, the UN Security Management System's Guidelines on the Use of Armed Security Services from PMSCs (approved by the UN Chief Executives Board for Coordination) mentioned the requirement for the PMSCs to be a member company of the

[20] See, for example, (Convention on Cybercrime 2001). US Computer Fraud and Abuse Act, 18 USC, §1030.

[21] International Code of Conduct for Private Security Service Providers' Association (ICoCA). Available online: https://www.icoca.ch/en (accessed on 8 January 2022).

[22] The International Code of Conduct for Private Security Service Providers (ICoC). Available online: https://www.icoca.ch/en/the_icoc (accessed on 8 January 2022).

[23] ICoCA Articles of Association. Available online: https://www.icoca.ch/sites/default/files/resources/Articles%20of%20Association.pdf (accessed on 8 January 2022).

[24] Principles and Procedures: Certification. ICOCA. Available online: https://www.icoca.ch/sites/default/files/uploads/ICoCA-Procedures-Article-11-Certification.pdf (accessed on 8 January 2022).

[25] Procedures: Reporting, monitoring and assessing performance and compliance (ICoCA). Available online:https://www.icoca.ch/sites/default/files/uploads/ICoCA-Procedures-Article-11-Certification.pdf (accessed on 8 January 2022).

[26] Article 13, ICoCA Principles and Procedures.

[27] ICoCA's complaint mechanism. Available online: https://icoca.ch/registering-a-complaint/ (accessed on 30 August 2022).

[28] The International Code of Conduct for Private Security Service Providers' Association (ICoCA), https://icoca.ch/private-security-companies/ (accessed on 30 August 2022).

ICoC for providing private security services.[29] Moreover, nations are also incorporating the code into their domestic legislation.[30] In 2013, the Swiss Parliament publicly introduced a Draft Federal Act on Private Security Services Provided Abroad, which obligates the PMSCs to undertake the ICoC.[31] The abovementioned discussion made the efficiency of the ICoCA mechanism evident. This mechanism is discussed in greater detail in the subsequent section. Nonetheless, it is clear that today it is time for the cyber-surveillance industry to adopt the mechanism from PMSCs to become self-regulating with the capabilities to address the claims of arbitrary actions in the name of national security. It may be possible that the private corporates engaged in these surveillance industries find it difficult to keep their business profitable by confirming their human rights obligations, but this fact nonetheless confirms the nature of such conduct, which is inherent to state functions.

5. The Feasibility of a Shared Responsibility Regime for Redressing the Human Rights Concerns: In Pursuance of the ICoC and ICoCA Mechanism

The globe has become more interlinked with the enhancement in the collaborative measures between state and non-state stakeholders (focusing on corporates) at a transnational level; however, the standing international law regime seems to overlook this reality (Nollkaempur 2013). It is uncommon to see instances of shared state responsibilities under the institutional frameworks where the state entered into an agreement with a non-state actor (such as the NSO Group) for carrying out certain activities (d'Aspremont et al. 2015). Thus, there is a requirement for a thorough re-examination of the viability of shared responsibility in the international legal framework to fill the accountability gap that remains attached with the emergence of corporates (Schechinger 2014). In this regard, this section will examine how, by expanding the Wassenaar Agreement—the international agreement governing the transfer of weapons, including spyware—a shared responsibility mechanism might be adapted to regulate the commercial usage of cyber-surveillance spyware. Again, a parallel can be drawn from the PMSCs (Jagers 2012) because the nature of the conduct in spyware operating in conflict zones has a close government connection; it also requires significant state involvement. In this regard, the authors find it imperative to look upon *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ("Wassenaar Arrangement")*, which is one of the seminal international agreements concerning arms transfer, including surveillance spyware transfer as all the forty-two participating states have "agreed to meet on a regular interval to maintain that transfers of arms and technologies are handled out responsibly and in pursuit of international and regional peace and security" (Bellal 2014). Additionally, the signatory states chose to keep sharing information pertaining to the transfer of such dual-use goods and to regularly review the list of goods so as to adopt changes as per the technical advancements.[32] At the present time, the Wassenaar Arrangement is the agreement that reaches the international consensus to offer a transnational legal mechanism for limiting the transborder exchange of surveillance devices, software, and know-how.[33] The agreement encompasses a long range of dual-use commodities and technology for which states agreed to enact export control legislation, granting licensing agencies the authority to accept, deny, and examine their transfer. Since

[29] UN Department of Safety and Security, Guidelines on the Use of Armed Security Services from Private Security Companies. 2012. UN Security Management System: Security Management Operations Manual. Available online: http://www.unsceb.org/content/action-safety-and-security (accessed on 30 August 2022).

[30] United Nations Department of Safety. Guidelines on Use of Armed Security Services. Available online: https://www.ohchr.org/sites/default/files/Documents/Issues/Mercenaries/WG/StudyPMSC/GuidelinesOnUseOfArmedSecurityServices.pdf (accessed on 30 August 2022).

[31] United Nations. Switzerland: Clarifying legal rules regarding Private Military and Security Companies (PMSCs). Available online:https://www.un.org/ruleoflaw/blog/portfolio-items/switzerland-clarifying-legal-rules-regarding-private-military-and-security-companies-pmscs/ (accessed on 5 July 2022).

[32] Wassenaar Arrangement. What is the Wassenaar Arrangement? Available online: http://www.wassenaar.org/the-wassenaar-arrangement/ (accessed on 30 August 2022).

[33] List of Dual-Use Goods and Technologies and Munitions List, Wassenaar Arrangement Secretariat. Available online: https://israel-trade.net/wp-content/blogs.dir/49/files/2020/10/WA-DOC-19-PUB-002-Public-Docs-Vol-II-2019-List-of-DU-Goods-and-Technologies.pdf (accessed on 30 August 2022).

its introduction, the incorporation of cyber-surveillance technology in the list has been the most contentious item (although all the member nations unanimously agreed to amend it, recognizing its need in the aftermath of the Libyan incident where the government was found to be indulging in the deployment of surveillance spyware).States commit to "keep effective export restrictions [of weapons and technology] on the agreed list and to make sure that their national policies do not compromise international and regional security".[34] Here, the question may arise whether Pegasus as cyber-surveillance technology falls under dual-use goods. While there is no single definition of "cyber-surveillance technology", it has been addressed by legal scholars, lawmakers, and professionals in works that examine surveillance technologies as dual-use commodities. "Cyber-surveillance technology" refers to "devices, software and skills used by intelligence and law enforcement agencies, as well as network operators operating to secretly monitor, exploit, and analyze data stored, processed, and transferred over ICT".[35] Taken together, this definition and all discussions on Pegasus's usage, there is no doubt that Pegasus can be deemed to be "cyber-surveillance technology". Moreover, the dual-use nature of Pegasus can be justified in view of its capability of assisting states in their law enforcement by carrying out their national security work of tracking out terrorist activities along with other security initiatives and its inherent military capabilities. Here, the commercial aspects come from the fact that since most of the countries lack the technological capability to undertake the surveillance in the way companies as the NSO Group do, which evidently opens a huge commercial opportunity for these companies (including the NSO Group) whereby they assist other nations in realizing their objectives for law enforcement and technologically enabled intelligence. Therefore, the argument of looking at Pegasus spyware under the regime of dual-use goods appears to be justified to a great extent, thereby the proposed regime based on the *Wassenaar Agreement* would be able to regulate Pegasus spyware, which is currently unchecked (the subsequent discussion in this section makes it more evident).

However, we cannot ignore that the *Wassenaar Arrangement* loses its potential due to the sole discretion of the member states in the approval or denial of an export license of such technologies (Bellal 2014, p. 468). Further, some member states are yet to incorporate national legislation in consonance with the objectives of the *Arrangement* (Bellal 2014, p. 471). This led to an inconsistency in effectively controlling the states with doubtful histories of human rights in their ability to acquire dual-use goods (Thomsen and Thomsen 2015). However, the *Wassenaar Arrangement* can be sufficiently used to have scope for the engagement of other stakeholders such as civil organizations and state actors to enter otherwise private transactions. This should be framed based on the ICoCA mechanism to the significance of active participation from other stakeholders; otherwise, only state actors might be held attributable; that is also in case it had control or provided effective directions to the corporate. Therefore, there is a requirement for an instrument similar to ICoC, based on the export-regulating mechanics of *Wassenaar Arrangement*, which includes restricted distribution, transparency through information sharing, and sharing of due notifications on the transferor denial of export licenses, with the sole purpose to safeguard the human rights.

Moreover, the important factor in the creation of a shared responsibility would be the formation of an oversight committee (akin to the ICoCA multi-stakeholder framework) made up of equitable representation from state, non-state organizations (for example, Amnesty International) and a corporate industry involved in providing spyware (for example the NSO Group). This committee would examine the corporate policies and management to observe the conformity with the proposed code (mentioned above) to prevent human rights violations. Non-compliance may lead to actions ranging from

[34] What is the Wassenaar Arrangement? Wassenaar Arrangement. Available online: http://www.wassenaar.org/the-wassenaar-arrangement/ (accessed on 9 January 2022).

[35] The definition cannot be entirely static as new technologies are introduced to the market, and a wider variety of communications devices and networks are involved in actual surveillance operations (Bromley 2017; SIPRI and Ecorys 2015).

penalties, sanctions, or even withdrawal of membership. To begin with, the states and their national legislations are required to correspond to the proposed code (reflecting ICoC regulations on export licensing). This would benefit the common people, state and civil societies, and the corporates involved in the spyware industry by improving the latter's reputation (which is currently facing downfall all across the globe) and enhancing the possibilities of lucrative exports of their technologies.

Although the shared responsibility approach with the involvement of the multi-stakeholder may foster accountability and openness in comparison to the standing position where the states' discretion on accepting or rejecting the usage of dual-use goods, including spyware, the most significant aspect of the shared responsibility approach is the requirement of the active state involvement and the composition of the national legislations with the suggested code. The corporations' participation in the proposed framework and their adherence to the code would give a positive impact on their profile in the cyber-surveillance sector and enhance the commercial opportunity for them (in a similar manner to how the PMSCs' adherence to the ICoCA has positively impacted them). Additionally, under this arrangement, the state authorization and granting of export permits for the dual-use good (spyware) would be contingent on corporate membership and adherence to the proposed framework. The other significant impact of this proposed framework is that even if the proposed oversight committee does not intervene against the corporates that fail to adhere to the proposed obligation under this framework, the aggrieved person could submit the complaint before the committee and a civil action attributable to the state involved. Thus, the proposed framework of shared responsibility would not only mandate that the states keep an eye on corporate behavior to prevent any abuse but also provide the aggrieved persons with a greater opportunity of redressal.

6. Other Required Solutions

One of the evident drawbacks that the standing legal regime faces is the comparatively outdated version of the legal provisions. For example, when General Comment No. 16 was adopted by ICCPR Article 17 in 1988 (UNHRC 1988), there was no way to understand the implications of technological advancement on the right to privacy, as we are observing today. Consequently, the requirement of reframing the legal instruments has been put forward by many eminent scholars like UN Special Rapporteur Frank La Rue,[36] multiple civil societies (UNHRC 2013b), and the UNGA (UNGA 2013). In this regard, the authors find it imperative to mention some of the required alterations toward the understanding of the right to privacy, as discussed below:

6.1. Redefining the Concept of Privacy

Most of the major conventions, declarations, and legislation around the world dealing with the right to privacy (expressly or implicitly) were adopted before the 1980s, when cyber-surveillance technologies like Pegasus did not exist and could not be anticipated, making them inadequate in addressing threats to personal privacy posed by data acquisition and digital technology (UNHRC 2016, Para. 46(a)). Even the major incidents of cyber surveillance (as mentioned on page 2) came after the year 2000. Therefore, it would not be wrong to say that the current body of text on privacy rights (mostly presented in various outdated documents) is restrictive or limited in nature. Further, there is also divergence in a uniform acceptable definition of the right of privacy due to variation in some documents. The lack of any acceptable universal version of the right to privacy, along with the difference in the technological advancement in different demographical locations, is indicative that the principles relating to privacy established almost fifty years

[36] "Legal frameworks must ensure that communications surveillance measures: (a) Are prescribed by law, meeting a standard of clarity and precision that insufficient to ensure that individuals have advance notice of and can foresee their application; (b) Are strictly and demonstrably necessary to achieve a legitimate aim, and adhere to the principle of proportionality and are not employed when less-invasive techniques are available or have not yet been exhausted." (UNHRC 2013a), Para. 6.

ago need to be modified to take into account the highest level of modernization which we have today. Thus, the modernization of the narrow definition of the right to privacy to encompass them as broader, comprehensive, and universal is one of the first steps forward in curbing the recent threats due to the advancement in cyber-surveillance. Here, it is important to understand the expansion in the ambit of the right to privacy is not only with respect to international conventions or declarations but also with the way the concept is understood, articulated, and interpreted by courts and policymakers globally (not only at the international level but also at the national level). The simple reason being the right to privacy is part of not only the significant human rights declarations but also practically most national constitutions (Rengel 2013). To get the real implications, the change should be at all levels, especially because, as we discussed, the enforcement of the international obligation of the right to privacy also primarily involves support from the national domestic law mechanism (as discussed previously). There is a requirement to encompass the concepts of self-determination and autonomy into the definition of privacy, which is also referred to as "information privacy", dealing with the people's interest in holding control over the access of information regarding themselves.[37] This aspect is partially reflected in the standing General Comment to Article 17, which reads as "the accumulation and holding of personal information on databanks, computers and any other devices by private individuals or bodies or public authority, must be under legal regulation (UNHRC 1988)". This practice can also be seen to be followed under the existing jurisprudence of the ECtHR and has been applied by the Human Rights Committee in many of its concluding Observations (UNHRC 2009, Para. 11). The ECtHR has even expressly mentioned on multiple occasions that "safeguarding of personal information is of primary importance to an individual's exercise of respect of her or his personal information and family life"[38] and recognized that personal life cannot be "susceptible to exhaustive definition".[39] The Charter of Fundamental Rights of the EU has recognized the individual's right to protection of personal data (Article 8) separately from the right to privacy (Article 7). Therefore, the international community can take into consideration these ECtHR rulings. Additionally, a historic ruling of the Court of Justice of the EU came in *Schrems* v. *Data Protection Commissioner*,[40] where the complaint was made against Facebook contesting data transfer outside the EU to the US, in light of the PRISM surveillance program.[41] The court determined that the said data transfer is illegal by recognizing that the legal framework allowing the state authorities to "access on a generalized basis to the content of electronic communications must be recognized as a compromise of the essences of the fundamental right to privacy as enshrined under Article 7."[42] Thus, it is suggested that the General Comment should affirm the application of Article 17 to "information privacy", which ensures the individual's right to hold control of the access to their personal data. Further, the expansion of the notion of the right to privacy in the major international declarations will impact the way privacy is treated in its member nations (which may be an indirect side-effect, as the municipal courts of member states which often investigate privacy may refer major declarations as evidence of evolving jurisprudence on privacy). Thus, overall, there is no doubt to have a positive impact of such redefinition. The need for revision is apparent; there has to be an updated understanding of what the fundamentals of the right to privacy entail and what it must safeguard in light of the duties imposed not just on states but also, and perhaps more challengingly, on corporations by international law.

---

37 Information Privacy in the Digital Age. American Civil Liberties Union. Available online: https://www.aclu.org/files/assets/informational_privacy_in_the_digital_age_final.pdf (accessed on 20 January 2022).

38 S and Marper v. the United Kingdom [GC] (App Nos. 30542/04 and 30566/04) (2008) ECHR; MK v. France (App No. 19522/09) (2013) ECHR.

39 Bensaid v. the United Kingdom (App No. 44599/98) (2001) ECHR [47]; Botta v. Italy (App No. 21439/93) (1994) ECHR.

40 Maximilan Schrems v. Data Protection Commissioner, CJEU, C-362/14, (2015).

41 The US National Security Agency's widespread surveillance operation known as PRISM captures digital communications from numerous US-based corporations.

42 Maximilian Schrems v. Data Protection Commissioner, Case C-362/14 (6 October 2015), para. 94.

6.2. Required Application of Human Rights Treaties in Instances of Extraterritorial Cyber Surveillance

The ICCPR's ambit, as defined under Art. 2(1), extends to all the persons who come "within the territory and subject to the jurisdiction" of the signatory states.[43] The issue arises on the determination of state jurisdiction in the matters of cyber surveillance. Here, the major question is whether it covers the persons not living within the state territory. If not, then it would simply mean that states are not obliged with respect to persons who may not reside in the state territory but are, in reality, under "the control of its jurisdiction". Even the national legislations in many developed nations distinguish between their internal and extraterritorial surveillance in terms of the obligation that arises from such conduct.[44] These include the US Foreign Intelligence Surveillance Act 1978,[45] the Australian Intelligence Services Act,[46] and the Regulation of Investigatory Powers Act 2000 (RIPA),[47] among others. In the modern world, where neither state governments nor surveillance companies seem to be respecting territorial borders, it is logically infeasible to rely on the victim's location while protecting its privacy rights. In *Jaloud* v. *the Netherlands*, an Iraqi was shot by mistake by a Dutch soldier in Iraq in 2004 for approaching a checkpoint after the checkpoint was attacked by insurgents.[48] The ECtHR formulated the extraterritorial jurisdiction because state authorities were exercising control over an individual's right without having physical custody of that individual. In other words, the Netherland's jurisdiction was invoked because they exercised control and authority over the victim's right to life at the time of the incident, leading to the extraterritorial jurisdiction without having physical control over the victim. Thus, the question is, if the state could have a human rights obligation to exercise its control and authority over an individual's right to life, then why not exercise the right to privacy, leading to the extraterritorial obligation in the matters of cyber-surveillance? Such an evolution is necessary; the current approach focuses on physical control over the individual or territory, which is prima facie inadequate for the cyber realm (Margulies 2014). In the wake of cyber-surveillance systems like Pegasus, which can exert remote control over the data of any foreign national, the mentioned shift is highly essential. The lower threshold based on physical control will allow the states to continue interference with the individual's right to privacy using the standing gap by easily circumventing their human rights obligation. Therefore, the realities of the existing cyber-surveillance activities cannot be ignored.

In this regard, multiple suggestions are put forward, focusing on the "control of communication" rather than physical control. As per Carly Nyst, when data are intercepted under the territory of a state, it triggers that state's obligation toward that individual whose information is intercepted (Nyst 2013, 2018). This line of argument is in consonance with the argument put forward by Marko Milanovic (2016), who differentiates the state's positive obligation toward securing an individual's human rights (including prevention of human rights violation by third parties) to the state's negative obligation that needs the state to not interfere with individual's right.[49] Both Nyst and Marko's point of argument

[43] States must respect and to ensure' the rights recognised in the treaty to all individuals within its territory and subject to its jurisdiction. International Covenant on Civil and Political Rights. 23 March 1976. 999 UNTS 171. Art. 2(1) and 17.

[44] RIPA places the requirement of providing proof and a warrant, as indicated in section 8, outside the purview of external communications in order to prevent any arbitrary surveillance activity. Privacy International v. GCHQ, IPT/13/92/CH (16 May 2014). Additionally, the US has argued that it is obligated to respond, particularly when the victim is inside its territorial authority. United Nations Human Rights Commission. 24 April 1995. Summary Record. 1405th Meeting, UN Doc., CCPR/C/SR 1405, para. 20.

[45] Foreign Intelligence Surveillance Act, 1978. Sec. 1881a(a) (United States).

[46] Australian Intelligence Services Act, 2001, Sec. 9 (Australia).

[47] Regulation of Investigatory Powers Act, 2000, Sec. 8(4) and Investigatory Powers Act, 2016 (United Kingdom).

[48] Jaloud v. the Netherlands (App No. 47708/08) (2014).

[49] "[I]n cases of surveillance the possible violation of privacy is entirely consummated by the act of surveillance itself, whether it takes place in an area under the state's sovereignty, control, or beyond its control. My own preferred solution to such cases is hence the third model of jurisdiction that distinguishes between positive and negative obligations." (Marko Milanovic 2014).

accents the prohibition against state interference; however, there is a bigger concern which goes beyond the protection toward data storage and interfered communication. The issue of cooperation and transfer of individual data among states and state actors makes it challenging to enforce privacy protection.[50] In this regard, Peter Margulies's virtual control test, among many other suggestions provided with respect to the model of jurisdictions, seems to be applicable to the standing requirements (Margulies 2014). This test will invoke the application of the human rights treaties, including ICCPR, if a state is found to have exercised "virtual control" over people's personal data or communications no matter where that person is located at that time or whether the state has any physical control over that person or its location (Margulies 2014). Here, virtual control implies the ability of the state to store, intercept, use, or analyze personal information or communication. This approach seems to align with the recent perspective of human rights courts and bodies (Georgieva 2015). This approach incorporates the jurisdictional challenges of human rights obligations in surveillance cases, as the organizations involved in the surveillance can even control individuals' lives and personal information with a single click. Further, one of the biggest advantages of this particular model is that it promotes equality in the sense that any individual's human rights are equally protected no matter what is his/her nationality or demographical location. More importantly, the state's tie-up for circumvention can fall within their obligation—which means that in the present situation of Pegasus, in which the governments are tying up with the NSO Group for the application of this cyber-surveillance, would make the states fall under human rights obligations.

In fact, these approaches are also reflected in recent years, as UNGA, while adopting Resolution 68/167, has supported the application of ICCPR in cases of extraterritorial surveillance (UNGA 2013).

> "General Assembly is reaffirming the human rights and fundamental freedoms enshrined in the [. . .] relevant international human rights treaties, including the ICCPR [. . .] [d]eeply concerned at the negative impact that surveillance and/or interception of communications [. . . and] [c]alls upon all states to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law". (UNGA 2013).

Further, Emmerson, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, has observed that "state jurisdiction is also invoked in the matters where it exercises a regulatory authority over the internet or telecommunication service provider that can physically control the information or data (UNHRC 2014, Para. 41)". The UN Office of High Commissioner has also noted that in the situation where the state is exercising the regulatory jurisdiction over the third party which physically exercises control over the individual's personal data, that the state would have an obligation under that agreement (UNGA 2014, Para. 34).

Resultantly, it is evident that a virtual control test is necessary since the components of an effective control test are in appropriate in the modern digital era. Since the digital data transit through a multitude of jurisdictions before reaching the intended recipient, it would be arduous to determine where the conventional territorial control is established and how the conventional physical control (which is narrowly defined and leaves a significant gap to exploit) is accomplished. Therefore, the conundrum of the applicability of the virtual control test, irrespective of the victim's jurisdiction and nationality, has become crucial.

7. Conclusions

With the enhancement in technology, there has been a spike in the use of spyware for mass surveillance, leading to human rights abuse ranging from the violation of the right to

[50] Parliamentary Assembly of the Council of Europe. 2015. Mass Surveillance. Doc. 13734, para. 30–33.

privacy, unlawful detention, torture, or even death (Gupta 2013). The recent incident of the Pegasus project is one of the biggest examples of such a negative aspect of technological development. However, the state-centric approach and "the voluntaryism mechanism" in international law, particularly international human rights law, have kept these corporates detached from any strong obligation to protect individuals from their surveillance actions. In the existing framework, liability can only emerge if it can be connected to the state action, which is difficult to prove in most cases. Thus, it is high time for international institutions to formulate a shared responsibility framework based on the ICoCA mechanism—to sufficiently govern the conduct of the corporates involved in the cyber-surveillance business. While doing so, it is also imperative to not let these mechanisms become state-centric; rather, it must ensure the active participation of all the stakeholders, including civil societies, state actors, and corporate bodies. Alternatively, redefining the contours of the right to privacy under Article 17 ICCPR, addressing how the human rights obligations of states can be ensured in cyber-surveillance, including third-party collusion, can be seen as a step forward to solving the existing problems, thereby ensuring that the international legal framework stays abreast with the increasing need of a technologically advanced society. In addition, there are other crucial recommendations, most of which stem from the preceding debate. *First*, states must guarantee that cyber-surveillance mechanisms, like Pegasus, are only deployed where the legitimate objective is exemplified while adhering to the principles of necessity and proportionality (a reference can be made from the right to self-defense under the PIL). For the effective implementation of the former point, there is a requirement to establish an autonomous body (or an oversight committee, as suggested above, akin to the ICoCA multi-stakeholder framework) to screen states and their data privacy practices, inspect complaints from victims and different organizations, and impose effective sanctions in case of unlawful infringement on the privacy of the others (here, the role of international organizations becomes imperative). *Second*, states and corporate entities must take robust measures to foster greater transparency and accountability while having involvement in utilizing the cyber-surveillance mechanism. *Third*, adequate remedies must be made available to all the victims for the infringement of privacy by the states without distinguishing between national and non-national because of the evident involvement of the transboundary concerns (here, the extraterritorial jurisdiction can also be brought up, as suggested in the above discussion). *Fourth*, the corporate entities must endeavor to gratify their obligation to uphold individuals' human rights, including the right to privacy. This can be done by effective implementation of the Guiding Principles of Business and Human Rights, which entails the obligation of undertaking due diligence in relation to the right to privacy, followed by adequate measures to ameliorate any adverse implications (even if such implications are merely suspicions in nature). *Fifth*, in case the conduct of the corporate entities has led to detrimental repercussions of an individual's privacy, they must engage in restoration through authorized channels, encompassing the effective redressal mechanisms. For ascertaining the effectiveness of these mechanisms, there is a need to ensure that they are consistent, accessible, transparent, fair, and coherent. Although these recommendations seem to be rigorous, they are merely illustrative in nature, considering the pace of technological advancement in recent years in the field of the cyber-surveillance.

Author Contributions: Conceptualization, A.A.; Methodology, A.A.; Software, T.K.; Validation, A.A.; Data curation, T.K.; Writing—original draft, T.K.; Supervision, A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank Anjana Raghunath for proofreading this work. The authors would also like to profusely thank the West Bengal National University of Juridical Sciences (WBNUJS) for providing the time and space to undertake this research.

Conflicts of Interest: The authors declare no conflict of interest.

References

Baughen, Simon. 2015. *Human Rights And Corporate Wrongs Closing: The Governance gap*, rev. ed. Cheltenham: Edward Elgar Publishing, p. 172.

Bellal, Annyssa. 2014. Arms Transfers and International Human Rights Law. In *Weapons under International Human Rights Law*. Cambridge: Cambridge University Press.

Bromley, Mark. 2017. *Export Controls, Human Security and Cyber-Surveillance Technology: Examining the Proposed Changes to the EU Dual-Use Regulation*. Solna: Stockholm International Peace Research Institute, pp. 6–10.

Cave, Danielle, Fergus Ryan, and Vicky Xiuzhong Xu. 2019. Mapping More of China's Technology Giants: AI and Surveillance. Available online: https://www.aspi.org.au/report/mapping-more-chinas-tech-giants (accessed on 30 August 2022).

Chan, Anna W. 2019. The Need for a Shared Responsibility Regime between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware. *Brooklyn Journal of International Law* 44: 795.

Chawala, Ajay. 2021. Pegasus Spyware—"A Privacy Killer". Available online: https://ssrn.com/abstract=3890657 (accessed on 30 August 2022).

Coker, Margaret, and Paul Sonne. 2011. Life Under the Gaze of Gadhafi's Spies. *Wall Street Journal*. Available online: https://www.wsj.com/articles/SB10001424052970203764804577056230832805896 (accessed on 5 January 2022).

Commission on Human Rights. 2005. Promotion and Protection of Human Rights. Available online: https://www.ohchr.org/sites/default/files/Documents/HRBodies/SP/AMeetings/20thsession/UNODCGuidance_Item6.pdf (accessed on 30 August 2022).

Convention on Cybercrime. 2001. Council of Europe. Available online: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (accessed on 7 January 2022).

Timberg, Craig, Michael Birnbaum, Drew Harwell, and Dan Sabbagh. 2021. On the list: Ten prime ministers, three presidents and a king. *The Washington Post*. Available online: https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/ (accessed on 30 August 2022).

d'Aspremont, Jean, André Nollkaemper, Ilias Plakokefalos, and Cedric Ryngaert. 2015. Sharing Responsibility Between Non-State Actors and States in International Law: Introduction. *Netherland International Law Review* 62: 49–67. [CrossRef]

Daly, Emma. 2022. Why Tech is a Double-Edged Sword for Human Rights. Human Rights Watch. Available online: https://www.hrw.org/news/2014/01/06/whytech-double-edged-sword-human-rights (accessed on 2 February 2022).

Daskal, Jennifer. 2016. Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues. *Journal of National Security and Law* 8: 475–82.

Deva, Surya. 2012. Guiding Principles on Business and Human Rights: Implications for Companies. *EU Company Law* 9: 101–9. [CrossRef]

Electronic Frontier Foundation. 2012. Swedish Telcom Giant Teliasonera Caught Helping Authoritarian Regimes Spy on Their Citizens. Available online: https://www.eff.org/deeplinks/2012/05/swedish-telcom-giant-teliasonera-caught-helping-authoritarian-regimes-spy-its (accessed on 30 August 2022).

Feldstein, Steven. 2019. The Global Expansion of AI Surveillance. *Carnegie Endowment for International Peace*, September 17.

Fuchs, Christian. 2012. *Implications of Deep Packet Inspection Internet Surveillance for Society: The Privacy & Security Research Paper Series*. Issue 1. Uppsala: Department of Informatics and Meida, Uppsala University Kyrkogardsgatan.

George, P. J. 2021. Explained: Pegasus and the laws of surveillance in India. *The Hindu*. Available online: https://www.thehindu.com/news/national/explained-pegasus-and-the-laws-on-surveillance-in-india/article61437972.ece (accessed on 30 August 2022).

Georgieva, Ilina. 2015. The Right to Privacy under Fire-Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Article 17 ICCPR and Article 8 ECHR. *Utrecht Journal of International and European Law* 31: 104. [CrossRef]

Global Internet Liberty Campaign. 2022. Privacy And Human Rights: An International Survey of Privacy Laws and Practice. Available online: http://gilc.org/privacy/survey/intro.html (accessed on 2 January 2022).

Gupta, Rishi R. 2013. Germany's Support of Assad: Corporate Complicity in the Creation of the Syrian Surveillance State Under the European Convention on Human Rights. *American University International Law Review* 28: 1359–60.

Gwagwa, Arthur. 2018. Exporting Repression? China's Artificial Intelligence Push into Africa. *Net Politics*. Available online: https://www.cfr.org/blog/exporting-repression-chinas-artificial-intelligence-push-africa (accessed on 5 June 2022).

Human Rights Watch. 2014. *They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia*. New York: Human Rights Watch.

Jagers, Nicola. 2012. Regulating the Private Security Industry: Connecting the Public and the Private through Transnational Private Regulation. *Human Rights & International Legal Discourse* 6: 88.

Karavias, Markos. 2013. *Corporate Obligations Under International Law*, rev. ed. Oxford: Oxford University Press, p. 10.

Karavias, Markos. 2015. Shared Responsibility and Multinational Enterprises. *Netherlands International Law Review* 62: 106. [CrossRef]

Khan, Irene. 2022. Spyware Scandal: UN Experts Call for Moratorium on Sale of 'Life Threatening' Surveillance Tech, UNHR. Available online: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27379&LangID=E (accessed on 30 August 2022).
Klabbers, Jan. 2017. Reflections on Role Responsibility: The Responsibility of International Organizations for Failing to Act. *European Journal of International Law* 28: 1133–61. [CrossRef]
La Rue, Frank. 2013. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. UNGA. Available online: https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (accessed on 30 August 2022).
Layne, Stephen R. 2015. Corporate Responsibility for Human Rights Violations: Redressability Avenues in the United States and Abroad. *Gonzaga Journal of International Law* 18: 7–8.
Margulies, Peter. 2014. The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism. *Fordham Law Review* 82: 2139.
Marquis-Boire, Morgan, Collin Anderson, Jakub Dalek, Sarah McKune, and John Scott-Railton. 2013. *Some Devices Wander By Mistake: Planet Blue Coat Redux*. Toronto: University of Toronto (Canada Centre for Global Security Studies).
McBeth, Adam, and Justine Nolan. 2012. The International Protection and Human Rights and Fundamental Freedoms. In *International Corporate Legal Responsibility*, 1st ed. Alphen aan den Rijn: Kluwer Law International.
McKune, Sarah. 2019. Submission to the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. March 2. Available online: https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Surveillance/SARAH_MCKUNE.pdf (accessed on 30 August 2022).
Mendel, Toby. 2012. *Global Survey on Internet Privacy and Freedom of Expression*. Paris: UNESCO, p. 43.
Mihr, Anja. 2014. Good Cyber Governance: The Human Rights and Multi-Stakeholder Approach. *Georgetown Journal of International Affairs* 15: 28.
Marko Milanovic. 2014. *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*. Harvard: Harvard University, p. 126.
Milanovic, Marko. 2016. UK Investigatory Powers Tribunal Rules that Non-UK Residents Have No Right to Privacy under the ECHR. EJIL: Talk! Available online: https://www.ejiltalk.org/uk-investigatory-powers-tribunal-rules-that-non-uk-residents-have-no-right-to-privacy-under-the-echr/ (accessed on 17 January 2022).
Mitsilegas, Valsamis. 2016. Surveillance and Digital Privacy in the Transatlantic 'War on Terror:' The Case for a Global Privacy Regime. *Columbia Human Rights Law Review* 2: 47.
Mozur, P. J. M. Kessel, and M. Chan. 2019. Made in China, Exported to the World: The Surveillance State. *The New York Times*. Available online: https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html (accessed on 5 June 2022).
Nollkaempur, Andrew. 2013. Shared Responsibility in International Law: A Conceptual Framework. *Michigan Journal of International Law* 42: 436. [CrossRef]
Nyst, Carly. 2013. Interface Based Jurisdiction Over Violations of the Right to Privacy. EJIL:Talk! Available online: http://www.ejiltalk.org/interference-based-jurisdiction-over-violations-of-the-right-toprivacy/ (accessed on 22 January 2022).
Nyst, Carly. 2018. Secrets and Lies: The Proliferation of State Surveillance Capabilities and the Legislative Secrecy which Fortifies them—An Activist's Account. *State Crime Journal* 7: 10–12.
Penney, Jonathon, Sarah McKune, Lex Gill, and Ronald J. Deibert. 2018. Advancing Human Rights-By-Design In the Dual-Use Technology. Available online: https://jia.sipa.columbia.edu/advancing-human-rights-design-dual-use-technology-industry (accessed on 30 August 2022).
Pirvan, Petruta. 2021. EU GDPR applicability to international organizations. *International Association of Privacy Professionals*. Available online: https://iapp.org/news/a/eu-gdpr-applicability-to-international-organizations/ (accessed on 5 January 2022).
Privacy International. 2016. *Open Season: Building Syria's Surveillance State*. London: Privacy International.
Qiang, Xiao. 2019. The Road to Digital Unfreedom: President Xi's Surveillance State. *Journal of Democracy* 30: 53–67. [CrossRef]
Rengel, Alexandra. 2013. *Privacy in the 21st Century*. Leiden: Martinus Nijhof Publishers.
Rivera, Humberto F. C. 2015. Business and Human Rights: From a "Responsibility to Respect' to Legal Obligations and Enforcement. In *Human rights And Business: Direct Corporate Accountability For Human Rights*. Edited by Jernej LetnarCernic and Tara Van Ho. Chicago: Wolf Legal Publishers, p. 322.
Rivera, Cantú. 2019. National Action Plans on Business and Human Rights: Progress or Mirage? *Business and Human Rights Journal* 4: 213–37. [CrossRef]
Rolley, Chip. 2019. Is Chinese-Style Surveillance Coming to the West? *Guardian*. Available online: https://www.theguardian.com/commentisfree/2019/may/07/chinese-style-surveillance-exported-west (accessed on 30 August 2022).
Ruggie, John. 2007. Business and Human Rights: Mapping International Standards of Responsibility and Accountability for Corporate Acts. UN Document A/HRC/4/035. February 19.
Ruggie, John. 2011. Presentation of Report to United Nations Human Rights Council. Available online: https://www.ohchr.org/en/statements-and-speeches/2022/10/presentation-annual-report-united-nations-high-commissioner-human (accessed on 30 August 2022).

Ryngaert, Cedric. 2015. Transnational Private Regulation and Human Rights: The Limitations of Stateless Law and the Re-Entry of the State. In *Human rights and Business: Direct Corporate Accountability For Human Rights*. Edited by Jernej LetnarCernic and Tara Van Ho. Chicago: Wolf Legal Publishers, p. 99.

Saxena, Nipun. 2022. Pegasus is merely contractual, and while the consequences of breach may have a permanent devastating effect on human rights, the redressal under any municipal contractual remedy. *Leaflet*. Available online: https://www.theleaflet.in/is-it-the-last-flight-for-pegasus-part-i/ (accessed on 30 August 2022).

Schaake, Marietje. 2015. Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries. Available online: https://www.accessnow.org/cms/assets/uploads/archive/Access%20input%20on%20HR%20and%20techonlogy%20draft%20report.pdf (accessed on 30 August 2022).

Schechinger, Jessica. 2014. *Principles of Shared Responsibility in International Law: An Appraisal of the State of the Art*. Edited by Andrew Nollkaemper and I. Plakokefalos. Cambridge: Cambridge University Press.

Shahbaz, Adrian. 2018. Freedom on the Net 2018: The Rise of Digital Authoritarianism. *Freedom House*, October 31.

Silver, Vernon, and Ben Elgin. 2011. *Torture in Bahrain Becomes Routine with Help of Nokia Siemens*. New York: Bloomberg.

SIPRI and Ecorys. 2015. Submission, European Commission for Impact Assessment. In *Data and Information Collection for EU Dual-Use Export Control Policy Review*. Stockholm: SIPRI, Rotterdam: Ecorys, p. 143.

Sonne, Paul, and Margaret Coker. 2022. Firms Aided Libyan Spies First Look Inside Security Unit Shows How Citizens Were Tracked. *Wall Street Journal*. Available online: http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html (accessed on 30 August 2022).

Sullivan, Scott M. 2010. Private Force/Public Goods. *Connecticut Law Review* 42: 853.

Thomsen, Roszel, and Philip Thomsen. 2015. Export Controls on Intrusion and Surveillance Items: Noble Sentiments Meet the Law of Unintended Consequences. *Journal of Internet Law*, 23–25.

Timm, Trevor. 2012. Spy Tech Companies & Their Authoritarian Customers: Part I: FinFisher and Amesys Electronic Frontier Foundation. Available online: https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-i-finfisher-and-amesys (accessed on 30 August 2022).

UN. 1946. Convention on the Privileges and Immunities of the United Nations. Available online: https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=III-1&chapter=3&clang=_en (accessed on 30 August 2022).

UNCHR. 2019. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Surveillance and Human Rights. Available online: https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression (accessed on 30 August 2022).

UNGA. 2013. Res 68/167. Available online: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/449/47/PDF/N1344947.pdf?OpenElement (accessed on 30 August 2022).

UNGA. 2014. Report of the Office of the United Nations High Commissioner for Human Rights the Right to Privacy in the Digital Age. Available online: https://www.ohchr.org/en/calls-for-input/report-right-privacy-digital-age (accessed on 30 August 2022).

UNHRC. 1988. The Right to Respect of Privacy, Family, Home and Correspondence and Protection of Honour and Reputation. Available online: https://www.refworld.org/docid/453883f922.html (accessed on 30 August 2022).

UNHRC. 2009. Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, Spain. Available online: https://www.refworld.org/docid/49ae42152.html (accessed on 30 August 2022).

UNHRC. 2013a. Report by the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. Available online: https://digitallibrary.un.org/record/1304394?ln=en (accessed on 30 August 2022).

UNHRC. 2013b. Written Statement by Reporters without Borders International, a Non-Governmental Organisation in Special Consultative Status. Available online: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/17/NGO/8 (accessed on 30 August 2022).

UNHRC. 2014. Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Ben Emmerson QC. Available online: https://www.ohchr.org/en/special-procedures/sr-terrorism (accessed on 30 August 2022).

UNHRC. 2016. Report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci. Available online: https://www.ohchr.org/en/special-procedures/sr-privacy (accessed on 30 August 2022).

United Nations. 2010. *Report of the Working Group on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination*. New York: United Nations.

United Nations Global Compact. 2022. Our Participants. Available online: https://www.unglobalcompact.org/what-is-gc/participants (accessed on 10 January 2022).

Vazquez, Carlos Manuel. 2005. Direct vs. Indirect Obligations of Corporations Under International Law. *Columbia Journal of Transnational Law* 43: 927.

Wallace, Stuart. 2017. Private Security Companies and Human Rights: Are Non-Judicial Remedies Effective. *Boston University International Law Journal* 35: 72.

White, Nigel D. 2011. The Privatization of Military and Security Functions and Human Rights: Comments on the UN Working Group's Draft Convention. *Human Rights Law Review* 11: 137–40. [CrossRef]