6. Governing the Global Proliferation of Digital Surveillance Technologies: Lessons from the EU

Machiko Kanetake

Abstract: The chapter engages with the EU's legal discourse surrounding the regulation of digital surveillance technologies or so-called spyware. It does so by focusing on the EU's attempt to regulate the international sale of digital surveillance technologies. The urgent need for rule-based control of the global surveillance technologies market has been on the agenda of the UN, EU, governments, NGOs, and research institutions. Within the EU, a particular legal instrument, known as dual-use export control, has come under the spotlight as a tool to mitigate human rights risks associated with the sale and transfer of spyware. While the field of law has developed to mitigate military risks within the EU's security and defense policies, it has not yet sufficiently evolved to address the multifaceted human rights risks that the sale of surveillance technologies may pose to the destination countries.

Keywords: spyware, export control, dual-use technologies, cyber surveillance, human rights, due diligence

Introduction

Digital surveillance technologies are sold and transferred from one country to another, bringing both significant benefits and risks transnationally. Consider, for instance, a company's sale of advanced remote monitoring software to another state's intelligence services. While the intrusion technology may assist the intelligence services in their criminal investigations,

Van Dijck, José, Karin van Es, Anne Helmond, and Fernando van der Vlist, eds. *Governing the Digital Society: Platforms, Artificial Intelligence, and Public Values*. Amsterdam: Amsterdam University Press, 2025
DOI 10.5117/9789048562718_CH06

the same technology could also be a medium with which to monitor and suppress journalists and dissidents, bringing enormous human rights risks to the destination country (Feldstein 2019; Wagner 2012). In the case of the German-based company FinFisher, for example, its surveillance technology was deployed against Bahrain's pro-democracy activists, Ethiopia's opposition members, and Egyptian human rights defenders, to name a few (Amnesty International 2020; Marczak et al. 2015, 12). The global sale of FinFisher products has led to a series of non-judicial complaints and juridical proceedings in the UK and Germany (as will be discussed in section 5). Despite the multifaceted risks and competing interests, there is still little transparency and accountability in global surveillance trade (UN Human Rights Council 2019, para. 5).[1]

The call for rule-based control of the global transfer of surveillance technologies has been on the agenda of the UN, the EU, governments, NGOs, and research institutions for several years (e.g., Privacy International 2016; UN Human Rights Council 2019). In 2015, the EU's Action Plan on Human Rights and Democracy 2015–19 called for the mitigation of risks associated with the "uncontrolled export of ICT products" (Council of the EU 2015, 40). In 2019, the UN's Special Rapporteur on freedom of opinion and expression called for an "immediate moratorium on the global sale and transfer of the tools of the private surveillance industry" until necessary safeguards are put in place (UN Human Rights Council 2019, paras. 2, 66). In 2021, the UN's call for a moratorium was reiterated and endorsed by as many as 156 civil society organizations across the globe, following the Pegasus Project revelations (Access Now et al. 2021). In 2022, the Pegasus Project led the European Parliament to launch an inquiry committee (PEGA Committee) on the use of Pegasus and other spyware. In June 2023, the European Parliament adopted a series of recommendations based on the findings of the Committee (PEGA Committee 2023a; 2023b). Having referred to the UN Special Rapporteur's call for an immediate moratorium, the Parliament took the position that "the trade in and use of spyware needs to be regulated strictly" (European Parliament 2023, recital AQ and para. 28). On this basis, the European Parliament listed the conditions that EU member states must fulfill. Included therein was to repeal "all export licences that are not fully in line with the Dual-Use Regulations" (ibid., para. 29(d)).

1 This chapter builds upon the research project that the author has conducted in 2023 for the Center for Democracy and Technology (CDT) on the EU's Dual-Use Regulation.

The "Dual-Use Regulation" mentioned by the European Parliament is one of the legal instruments which can be applied to prevent some of the problematic consequences of the global sale of surveillance technologies. The instrument in question is the EU's Dual-Use Export Control Regulation (EU) 2021/821 to control the international transfer of items which serve both civilian and military purposes. Despite the rather technical nature of the regulation, this legal instrument came under the spotlight as a legal tool to prevent the uncontrolled proliferation of surveillance technologies (Kanetake 2019a).

Against this background, the present chapter examines the EU's attempt between 2013 and 2023 to use the Dual-Use Regulation to control the trade of digital surveillance technologies. The central argument of this chapter is that the EU's Dual-Use Export Control Regulation has not developed sufficiently to address multifaceted human rights risks associated with the sale of digital surveillance technologies. This is primarily because the field of law has evolved based on the duality and dichotomy of "civil and military" purposes, within the broader regional and international policies on security and defense (Kanetake 2018). While the EU has strengthened rights-based control regarding cyber surveillance technologies, such control sits oddly with the traditional civil–military dichotomy which, more importantly, leaves rights-based risk assessment effectively marginalized.

The chapter will start with explaining the relevance of dual-use export control for the regulation of digital surveillance technologies (section 2). Then the chapter provides the interpretation of the EU's export control provision over cyber surveillance items (section 3). This will be followed by the analysis of some reported cases of the misuse of spyware, which may illustrate key regulatory gaps in the EU's dual-use export control (section 4). The chapter will end with articulating a set of lessons learnt from the EU's experience in regulating the transfer of digital surveillance technologies (section 5 and conclusion).

Digital surveillance

The market for digital surveillance tools is "shrouded in secrecy," as the UN's Special Rapporteur on freedom of opinion and expression acknowledged (UN Human Rights Council 2019, para. 1). Such secrecy is connected to the secrecy of the governmental use of surveillance technologies, which limits the possibilities for external scrutiny (Van der Vlist 2017, 137–38).

Surveillance technologies are also increasingly "entangled" with ordinary consumer electronics and services (Van der Vlist 2017, 139).

While it is difficult to have an overview of the global market of surveillance, according to the data collected by Steven Feldstein and Brian Kot, there are "at least seventy-four governments" between 2021 and 2023 that have contracted with companies for their spyware or digital forensics technology (Feldstein and Kot 2023, 9). This is combined with a number of reported cases regarding the misuse of exported cyber surveillance items (Wagner 2012; Feldstein 2019). Such reported cases could still be the tip of the iceberg, as Dunja Mijatović, the Council of Europe's commissioner for human rights, pointed out (Mijatović 2023).

Debates have taken place within the EU since 2013 concerning how to strengthen its export control of information and communications technologies (ICTs). This was in response to controversies in the aftermath of the Arab Spring that EU companies sold and provided technical assistance to those governments that had experienced popular uprisings. One of the most contentious issues during the EU's legislative process to "modernize" its dual-use export controls was how to address the human rights risks associated with the export of "cyber surveillance items" (Kanetake 2019a; 2019b). After years of debate, in May 2021, the EU adopted the renewed Regulation (EU) 2021/821, also called the Dual-Use Regulation. Included therein are controls of non-listed "cyber surveillance items" under Article 5, as will be further explained in section 3 below.

Before articulating the provisions relating to surveillance, it is necessary to provide some ideas about dual-use export controls, in part because it is considered as a highly technical field of law and by no means a popularly known legal instrument. "Dual-use" items are understood as those which can be used for both "civil and military purposes" (Regulation 2021/821, Article 2(1)). Among a wide range of "military purposes," dual-use export controls put an emphasis on the non-proliferation of weapons of mass destruction (i.e., nuclear, chemical, and biological weapons), although the control of conventional weapons is also included in regulatory objectives. By imposing authorization requirements on the international transfer of items, export controls aim to mitigate the misuse of items for purposes which may pose security threats. Among a variety of security threats, the field of law is essentially shaped by the mitigation of military risks, as demonstrated by the very definition of "dual-use" items. This point is critical for the sake of understanding the potentials and limits of the use of export controls for regulating digital surveillance technologies. In essence, the field of law, due to its central rationale, traditionally marginalized the mitigation of

non-military risks, such as risks that the sale of ICT products poses to the rights of individuals abroad.

Under the EU's export controls, there are two modes of export controls: namely, "list-based" control and so-called "catch-all" control. An authorization shall be foremost required for the export of dual-use items listed in Annex I of the EU's Dual-Use Regulation (Regulation 2021/821, Article 3(1)). Certain surveillance technologies have already been listed as controlled items. For example, mobile telecommunications interception equipment (or IMSI catchers) (Wassenaar Arrangement 2012, Category 5.A.1.f), IP network communications surveillance systems, and intrusion software (Pyetranker 2015, 162–64; Wassenaar Arrangement 2013, Categories 4.A.5 and 5.A.1.j) have been added to the list within the Wassenaar Arrangement and subsequently to the EU's control list. Regulation 2021/821's Annex I contains, for example, controls relating to: telecommunication interception systems (5A001.f), internet surveillance systems (5A001.j), intrusion software (4A005), and law enforcement monitoring software (5D001.e). While such a list-based control is at the heart of export controls, the "catch-all" control is a residual mechanism that allows authorities to exert export control over items which are not specifically listed in Annex I of the EU's Dual-Use Regulation. The catch-all clauses require unique vigilance on the part of the exporter, in that an exporter cannot simply rely on the list provided in Annex I, but instead must check an item against one of the broadly formulated criteria under Articles 4–10 of Regulation (EU) 2021/821.

While Regulation 2021/821 has direct effect across the EU, it does not mean that the EU itself receives and processes license requests from exporters. It is in the hands of the competent authority of each EU member state—such as the Federal Office for Economic Affairs and Export Control (BAFA) in Germany—that is responsible for implementing the EU's export controls, assessing export license requests, and deciding whether to grant a license. EU member states may also impose additional license requirements. While Regulation 2021/821 has strengthened EU-wide information exchange and cooperation regarding implementation and enforcement, it would be good to bear in mind that licensing decisions are taken by each member state, based on their own procedures and experiences, and within the resources (e.g., personnel, facilities) that each state is willing to allocate for export controls. Member states also vary in terms of the resilience of the rule of law and their relationships with the industry, including the ICT sectors. In short, the functioning of the EU's export control mechanisms is intertwined with the legal and political contexts of each member state.

The EU's export control over cyber surveillance

As mentioned above, the export control of "cyber surveillance items" became one of the most contested issues during the legislative process leading to the adoption of Regulation 2021/821.

Article 5(2) of Regulation 2021/821
Under Article 5, Regulation 2021/821 introduced export controls over such items as part of "catch-all" clauses. At the heart of legislative debates was Article 5(2), which provides:

> Where an exporter is *aware*, according to its *due diligence findings*, that cyber-surveillance items which the exporter proposes to export, not listed in Annex I, are *intended*, in their entirety or in part, for any of the uses referred to in paragraph 1 of this Article [i.e., for use in connection with *internal repression* and/or the *commission of serious violations of human rights and international humanitarian law*], the exporter shall *notify* the competent authority. (Emphasis added)

According to Article 5(2), an exporter's awareness of the intended uses of dual-use items for the serious violations of human rights and international humanitarian law gives rise to an obligation to notify a relevant EU member state authority. In accordance with Article 5(2), once the authority is notified by the exporter, that competent authority shall decide whether to make the export concerned subject to authorization.

Definition of "cyber surveillance items"
To understand the meaning of Article 5(2), we must examine the meaning of "cyber surveillance items" in the first place. According to Article 2(2) of the regulation, they are defined as follows:

> Article 2(20): "Cyber-surveillance items" means dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems.

Among a number of interpretive elements, the following four merit further explanation in particular: (1) the concept of "dual-use" items; (2) the meaning of "covert surveillance"; (3) the interpretation of the analysis of data "from" IT systems; and (4) the understanding of the phrase "specially designed."

First of all, cyber surveillance items should be part of "dual-use" items. This means that surveillance items subject to control need to have a potential to be used for military purposes. At the same time, this duality does not constitute a major obstacle, simply due to the prevalent use of surveillance technologies in military contexts.

Second, the term "covert surveillance" was one of the contested points during the legislative processes. Surveillance can be broadly defined as "a broad range of activities related to the gathering and processing of information on individuals" (Van Daalen et al. 2021, 17)—regardless of whether it is done by private or public entities, or regardless of whether it constitutes a violation of human rights. While Regulation 2021/821 assumes that surveillance can be "covert" or overt, the regulation does not define the meaning of "covert surveillance." According to Van Daalen et al., surveillance should be understood as covert with regard to a person "if that person does not know *whether* and *how* information on her is being used to target her specifically" (2021, 18, emphasis in original). This means that, for example, surveillance is "covert" even if a journalist knows a particular technology is monitoring her activities, provided that the journalist does not know that the data is used to track her contact with a political dissident. According to the European Commission's guidelines on Article 5, published in October 2024 after a public consultation, surveillance can be covert if the "gathered data can be diverted, evaluated or processed for other *purposes* than the ones the affected natural person is made aware of." The guidelines provide that the surveillance can be covert "when a natural person cannot objectively expect to be under surveillance" (Commission Recommendation (EU) 2024/2659, 6, Section 1.2.2; European Commission 2023, 4, Section II.2.2).

Third, the definition refers to items that monitor, extract, collect, or analyze data "from" information and telecommunication systems. As data must be monitored, etc. from ICT systems, this definition seems to exclude technologies that monitor or collect "offline" data (Van Daalen et al. 2021, 19). For example, microphones and security cameras that collect a person's biometric data would not fall under the definition of cyber surveillance items under Regulation 2021/821, even if this is counterintuitive (BAFA 2021, 5).

Finally, the interpretation of "specially designed" can vary depending on EU member states. This is the term customarily used in export controls to assess whether certain technical specifications are linked to particular functions and purposes. As Van Daalen et al. summarize it, items that are specially designed to enable the covert surveillance of natural persons are "items whose design includes 'particular features to achieve' such surveillance" (2021, 20). As the BAFA's document regarding the interpretation of

Article 5 pointed out, it does not require an item to be exclusively designed for the covert surveillance of natural persons (BAFA 2021, 5). This is also articulated in the European Commission's guidelines of 2024. According to the guidelines, the product's "*technical features* are suitable for and objectively enable covert surveillance of natural persons" (Commission Recommendation (EU) 2024/2659, 5, Section 1.2.1, emphasis added). At the same time, the technical features do not always dictate the problematic uses of technologies. In that sense, the Commission's guidelines are in line with BAFA's position that the term "specially designed" "does *not* require that the item can *solely* be used for the covert surveillance of natural persons" (Commission Recommendation (EU) 2024/2659, 5).

In short, despite many interpretive uncertainties, it becomes clear that a variety of technologies fall under the definition of cyber surveillance items. Regulation 2021/821 is applicable, for example, to the export of the algorithm and user interface components of facial and emotion recognition technologies, location tracking technologies, and open-source intelligence software (Van Daalen et al. 2021, 54–57). The European Parliament stressed that "the definition of cyber-surveillance items in the recast Dual-Use Regulation *cannot be given a restrictive interpretation* but should include *all technologies in this area*" including "Unmanned Aerial Vehicles capable of conducting surveillance" (European Parliament 2023, para. 65, emphasis added). How exactly EU member states define the concept of "cyber surveillance items" should be monitored by relevant stakeholders, as the definition is the entry point for exercising export controls.

Serious violations of human rights and humanitarian law

As mentioned above, the drafting of Article 5 was one of the most contested questions during the legislative process. This is especially because of its novelty, where the export control of surveillance is explicitly linked to consideration to "internal repression and/or the commission of serious violations of human rights and international humanitarian law" as a standard with which to determine the imposition of authorization requirements. "Internal repression" is understood as "major violations of human rights" (Council Common Position 2008/944/CFSP 2008, Article 2(2)(b) criterion 2) and it can overlap with "serious" violations of human rights.

While Regulation 2021/821 does not define what constitutes "serious" violations of human rights and international humanitarian law, these are the terms often used in the context of arms trade controls. With regard to the latter (humanitarian law), serious violations of international humanitarian law are generally understood as "war crimes" (ICRC 2012). Regarding

the former (human rights), whether or not human rights violations are regarded as serious depends on the "combination of various aggravating elements," such as the "irreparable impact on victims, together with the value protected by the human rights rule and the degree of vulnerability of a situation presents for the victims" (Siatitsa 2022, 63). While determining what constitutes "serious" violations requires case-specific assessment, exported cyber surveillance items can indeed be used in violations of human rights that have an irreparable impact on victims (e.g., the right to be free from torture, the right to life).

While Regulation 2021/821 introduces the novel aspect of explicitly referring to these serious violations, it is important to note that the assessment of such violations is not identical to determining whether the use of a specific cyber surveillance item constitutes a serious violation of human rights or amounts to a war crime. This assessment is carried out within the context of determining whether to regulate and approve exports. Thus, the analysis includes the technical capabilities of cyber surveillance items in question, the assessment of the past and present situations in the countries to which items would be sold, and the examination of the past and present conduct of end users in using cyber surveillance technologies. Despite the complexity arising out of the application of Article 5(2), it appeared that limited attention was given during the EU's legislative processes to address, for instance, the types of human rights that exporters must consider, and which reports and databases that exporters should consult in assessing the destination countries and end users therein.

Concept of "due diligence"

According to Article 5(2) quoted above, an exporter is expected to conduct "due diligence." "Due diligence" under Article 5(2) is understood as a type of business risk analysis, although its meaning has uniquely developed through export control practices (e.g., item classification) (Kanetake and Ryngaert 2023, Section 1.1). The preamble of Regulation 821/2021 refers to "due diligence" as a type of transaction screening as part of an internal compliance program (ICP) (Regulation 2021/821, recital 7). Under Regulation 2021/821, an ICP to facilitate compliance includes "due diligence measures assessing risks related to the export of the items to end-users and end-uses" (Regulation 2021/821, Article 2(21)).

While the term "due diligence" is a familiar term for export control professionals, the EU's Dual-Use Regulation 2021/821 is still significant in that it effectively obliges dual-use exporters—and not only governmental authorities—to undertake such a risk analysis within the frameworks

of international human rights and humanitarian law. The Commission's guidelines also made it clear that, under Article 5(2), exporters are "*required* to carry out due diligence" through transaction-screening measures (Commission Recommendation (EU) 2024/2659, 10, emphasis added). The guidelines expect exporters to "draw up plans to prevent and mitigate potential future adverse impacts" on the basis of due diligence findings (Commission Recommendation (EU) 2024/2659, 12). This means that exporters' due diligence is by no means static; it has to evolve on the basis of past practices. To reiterate, the concept of due diligence is nothing new in the field of export controls. Yet Article 5(2) of Regulation 2021/821 is novel in terms of its explicit reference to human rights and international humanitarian law, which serve as the yardsticks for conducting risk assessment by exporters.

Awareness of the intended use

Finally, under Article 5(2) of Regulation 2021/821, an exporter's obligation to inform arises when the exporter is "aware" of the intended use of cyber surveillance items for the serious violations of human rights and humanitarian law. The question is how to interpret the exporter's "awareness." According to the BAFA's interpretation, awareness here means "positive knowledge" or, in the terminology of criminal law, "direct intent" (BAFA 2021, 10). The fact that such uses "deem possible" is not sufficient, according to the BAFA (2021, 10). The Commission's guidelines seem to follow the BAFA's description, in that the guidelines also require an exporter's "positive knowledge of the intended misuse." The Commission made it clear that the "mere possibility of such a risk is not sufficient to establish awareness" (Commission Recommendation (EU) 2024/2659, 7, Section 1.2.6; European Commission 2023, 6 (II.2.6)).

At the same time, the European Commission's guidelines note that awareness here "cannot be assimilated to passivity" because such awareness "requires that the exporter has taken steps to obtain sufficient and adequate knowledge for assessing risks." What the guidelines do not state is whether awareness is deemed to have existed when the exporter had sufficient sources of knowledge but still failed to take steps to analyze such sources. In the field of export controls, knowledge is generally understood as "positive" knowledge. Nonetheless, Article 5(2) seems to lose its normative significance if it cannot be invoked against an exporter (who did not conduct a substantial risk assessment and therefore was not positively aware) as a ground for arguing that the exporter should have been aware of the intended misuse of technologies.

Predator spyware's sale despite Regulation 2021/821

While it remains to be seen how Article 5(2) is implemented in practice, the greater awareness about cyber surveillance exports fell short of preventing the spread of a spyware called Predator through some of the EU member states. Predator is a spyware developed by the company called Cytrox and "has become a favored option for many governments" (Feldstein and Kot 2023, 5) after the revelation of the Pegasus Project and the NSO Group started receiving extensive international scrutiny. In December 2021, the Citizen Lab's researchers found the likely presence of Predator customers in Armenia, Egypt, Greece, Indonesia, Madagascar, Oman, Saudi Arabia, and Serbia (Marczak et al. 2021).

For the sake of the EU's Dual-Use Export Control Regulation, most relevant is the sale of Predator by Intellexa, a company based in several jurisdictions, including Greece. It has been reported that Intellexa based in Greece sold Predator to Madagascar and Sudan and that the sale was apparently authorized by the Greek government after the entry came into force with Regulation 2021/821. According to the *New York Times* in December 2022, the Greek government admitted that it had granted licenses for the export of Predator to Madagascar (*New York Times* 2022). The Greek official also admitted in April 2023 that "Intellexa's Predator spyware was exported from Greece to Sudan" (*Athens News* 2023). In November 2022, the deputy minister of foreign affairs for economic diplomacy in Greece ordered an internal investigation to ascertain possible violations of export control regulations (*Athens News* 2023). As summarized in table 6.1, the investigations concerning the sale of Predator involve the following five export approvals, granted between November 15, 2021, and the end of March 2022 (Telloglou and Triantafillou 2023)—namely, after the entry into force of Regulation 2021/821.

Table 6.1. Export Approvals by Greek Authorities (November 2021 to March 2022)

Exporter	Item	Date	Value	End users
Intellexa	"system designed for mobile data extraction and data collection management"	Approved on November 15, 2021	€2.7 million	Recipient: Signum Intelligence Ltd (UK company) End user: National Anti-Fraud Agency in Madagascar
Intellexa	"a WiFi tracking and interception system designed to extract and analyze data from mobile devices using WiFi"	Approved on November 15, 2021	Presumably €0.2 million	Recipient: Signum Intelligence Ltd (UK company) End user: National Anti-Fraud Agency in Madagascar

Exporter	Item	Date	Value	End users
Krikel	"mobile data extraction and data collection management"	Application submitted on February 22, 2022	€70,000	End user: Ministry of Defense of Sudan Intermediate recipients: Toru Technologies (UAE) and Octopus Information Technology Services LLC (UAE)
Krikel	"wifi tracking and interception system designed for deployment and data analysis of mobile devices using wifi"	Application submitted on February 22, 2022	€5,000	End user: Ministry of Defense of Sudan Intermediate recipients: Toru Technologies (UAE) and Octopus Information Technology Services LLC (UAE)
Krikel	"data extraction from mobile devices and data collection management"	Application submitted on March 24, 2022 Approved on March 31, 2022	€70,000	End user: Ministry of Digital Transformation of Ukraine (eventually not exported)

Source: Based upon Telloglou and Triantafillou (2023).

As noted by the European Parliament, "the Greek government *admitted it has granted export licences* to Intellexa for the sale of the Predator spyware to repressive governments, such as Madagascar and Sudan" (European Parliament 2023, recital Q, emphasis added). As pointed out by the PEGA Committee, "the Greek government disclosed that it had provided Intellexa with two export licenses on November 15, 2021" (PEGA Committee 2023b, para. 155). Namely, the export licenses were given after the entry into force of Regulation 2021/821. With regard to the sale to Madagascar, the PEGA Committee's report observes that the "licence was granted despite the country's poor human rights record" and "*potentially being in conflict with the EU Dual-Use Regulation*" (PEGA Committee 2023b, para. 155, emphasis added). The PEGA Committee's report notes that Greece and Cyprus were "involved in the *illegal export* of Predator spyware to the Sudanese Rapid Support Forces (RSF) militias" and that "Greece has issued an export licence" (PEGA Committee 2023b, para. 242, emphasis added). On this basis, the European Parliament called on Greece to "urgently repeal all export licences that are not fully in line with the Dual-Use Regulation and investigate the allegations of illegal exports, among others to Sudan" (European Parliament 2023, para. 20(b)). To be sure, Greece is by no means the only country that has received extensive attention in the PEGA Committee's investigation following the Pegasus Project. The present chapter pays particular attention to the case of Greece, precisely because of its

reported connection to the EU's export controls over cyber surveillance technologies.

While the case of Predator illustrates the bitter reality that the EU's Regulation 2021/821 failed to prevent the problematic transfer of technologies to non-EU destinations, the Dual-Use Regulation has served as a basis for domestic and EU-level calls for accountability. Significantly, the European Public Prosecutor's Office (EPPO) has reportedly opened an investigation into illegal Predator software exports by the Greek government in breach of the EU's Dual-Use Regulation 2021/821 (Michalopoulos 2023). However, as of October 2023, the EPPO's official website has not made any information about the investigation available to the public. According to EURACTIV, it has been reported that EPPO received evidence providing that the Greek government "facilitated the proliferation of Intellexa's Predator spyware to countries such as Saudi Arabia, Sudan, Madagascar, and Bangladesh" by "granting export licences through the country's foreign ministry" (Michalopoulos 2023).

Strengthening connection to broader legal frameworks on human rights due diligence, including access to remedies

As demonstrated in section 3, Regulation 2021/821 on cyber surveillance items explicitly uses the term "due diligence." Given its explicit link to the risks of human rights and humanitarian law violations, Article 5(2) should be regarded as a step forward in integrating and strengthening human rights-based risk assessment in the process of controlling the export of cyber surveillance and its global proliferation. At the same time, as explained in section 3 above, the concept of due diligence under Article 5(2) is close to a risk analysis for businesses. This is arguably much narrower than the concept of "due diligence" developed as a part of the UN Guiding Principles on Business and Human Rights (UNGPs) (UN 2011).

Under the UNGPs, all business enterprises have "responsibility"—if not a strict legal obligation—to "exercise human rights due diligence." Due diligence here is understood to be "a comprehensive, proactive attempt to uncover human rights risks, actual and potential, over the entire life cycle of a project or business activity" for the sake of "avoiding and mitigating those risks" (UN Human Rights Council 2009, para. 71). Such a concept of due diligence is much broader than the notion of due diligence under Article 5(2) of the EU's Dual-Use Regulation. If judged against the yardsticks in UNGPs, the surveillance industry's due diligence practices are hardly encouraging. According to the UN's Special Rapporteur on freedom of

opinion and expression, companies in the surveillance industry "appear to fail to meet even [the UNGPs'] minimum baselines" (UN Human Rights Council 2019, para. 31).

An important question then is whether the concept of "due diligence" for cyber surveillance controls can evolve by incorporating the thicker version of "due diligence" developed under the UNGPs. Should the former (i.e., due diligence for export controls) be read in the light of the latter (i.e., due diligence under the UNGPs), exporters would be obliged to take a set of comprehensive processes to identify and mitigate human rights risks. While it is difficult to predict how the meaning of due diligence evolves in a specific industry, it is reasonable to expect some kind of normative approximation of "due diligence" under Article 5 of Regulation 2021/821 with "due diligence" under the UNGPs. This is because of the standard-setting and lawmaking efforts in the field of business and human rights. The European Commission has the ICT sector-specific guide to assist the implementation of the UNGPs (European Commission 2013). This and other instruments relating to the UNGPs should incrementally affect the interpretation of due diligence in cyber surveillance export controls.

The normative approximation is particularly relevant when we think about the dimension of access to effective remedy. To ensure access to remedy for business-related human rights abuses is one of the important elements of due diligence under the UNGPs and related guidance (UN 2011, 27–35). While the provision of remedy should be foremost done by states, it is also integral to the responsibility of business enterprises. The UNGPs expect business enterprises to "establish or participate in effective operational-level grievance mechanisms for individuals and communities who may be adversely impacted" (UN 2011, 31, principle 29).

In the context of spyware, access to effective remedy is one of the core problems that affected victims encounter. Consider the significant detrimental impacts that Pegasus and other spyware have had on human rights of journalists, human rights activists, and political opponents and dissidents. It is crucial to analyze what judicial and non-judicial avenues are available at the national and international levels for those who are affected by the export and eventual use of cyber surveillance items to raise complaints and seek remedies.

At the national level, there may be some possibilities to resort to judicial mechanisms to hold the companies or the governments accountable in connection to the export of cyber surveillance items. At the international level, there is a possibility to make use of the OECD's National Contact Point (NCP) as a (formally non-judicial) venue for resolving issues that arise from the

alleged non-observance of the OECD Guidelines for Multinational Enterprises. In fact, the international sale of Finfisher—mentioned at the beginning of this chapter—has led the UK NCP to find the UK-based company (Gamma International UK, part of Gamma Group to which FinFisher belonged) to be in violation of human rights standards under the guidelines (UK National Contact Point 2014). At the same time, the processes before the OECD NCPs have some fundamental limitations. As the UK NCP reiterated in *Privacy International v. Gamma International UK LTD* (2014), the NCP has "no powers to require any part to provide information to it, nor any special status permitting it to obtain confidential information" that is legally protected (UK National Contact Point 2014, para. 27). Ultimately, the findings of the NCPs consist of recommendations, and their effectiveness relies on both companies' willingness to act upon them and the NCPs' follow-up mechanisms.

It is therefore necessary to provide judicial venues in holding the companies or the governments accountable in connection to the export of cyber surveillance items. In thinking about the ways to resort to judicial proceedings, a series of court cases concerning the sale of FinFisher products provide some concrete examples. In the UK, there have been a series of judicial proceedings against (1) the licensing authorities,[2] (2) the companies involved,[3] and (3) a foreign government[4] that used FinFisher products. Yet perhaps most significantly, in Germany, the public prosecutor's office in Munich has filed, in May 2023, criminal charges against the executives of FinFisher (Staatsanwaltschaft München I 2023). The executives were charged on the basis of their allegedly intentional breach of obligations under the Foreign Trade and Payments Act to seek export authorization for the export of the surveillance software. While the ultimate outcomes

2 Privacy International filed for judicial review of the UK government's decision to refuse to provide any details regarding investigation to Gamma's export practices. In May 2014, the UK's High Court (Administrative Court) declared that the UK authorities acted unlawfully in issuing blanket refusals into the status of any investigation into the export of surveillance technologies: *R* (*on the application of Privacy International*) *v. The Commissioner for HM Revenue & Customs* [2014] EWHC 1475 (Admin) (UK).

3 A group of four pro-democracy activists and politicians launched judicial proceedings in 2018 against Gamma Group. The claimants argued that the companies involved had sold the spyware to the Government of Bahrain despite the well-documented record of human rights violations (Leigh Day 2018).

4 Two Bahrani activists have also brought proceedings against the government of Bahrain, on the basis that it hacked or infected their computers with FinSpy while the activists and their computers were in the UK. In February 2023, the High Court dismissed Bahrain's claim of jurisdictional immunity, allowing the case to proceed further: *Dr Saeed Shehabi and Moosa Mohammed v. The Kingdom of Bahrain* [2023] EWHC 89 (KB) (High Court of Justice, Queen's Bench Division, February 8, 2023) (UK).

of the criminal proceedings remain to be seen, these administrative, civil, and criminal proceedings in the UK and Germany concerning FinFisher products provide a test case for examining the availability of procedural avenues and substantive bases for seeking accountability in the global market of digital surveillance.

Finally, transparency is central to all the initiatives for improving the regulation of cyber surveillance exports. Amnesty International's report on the NSO Group articulated that transparency is required with regard to corporate structure, company's decision-making policies and processes, and the records of sales and exports (Amnesty International et al. 2021, 62–63). As the PEGA Committee's report articulated, "secrecy" is a "major obstacle in detecting and investigating the illegitimate use of spyware" (PEGA Committee 2023b, 144). National security grounds are often used by authorities to deny or restrict the scope of information to be made available to affected individuals and entities (PEGA Committee 2023b, 144). That is why the European Parliament also emphasized the need for obliging, through the future amendment of the Dual-Use Regulation, the authorities in member states to provide specific details of the approval and denial of export licenses for dual-use items, without broad exceptions that justify the withholding of information (European Parliament 2023, paras. 63–64). Without any transparency, it is not feasible for external observers, including civil society organizations, to engage with the industry to assess whether exporters have duly taken into account risks of the serious violations of human rights and international humanitarian law. Without any transparency, the affected victims, including dissidents and journalists whose digital footprints are monitored, would be left with no or little information necessary to seek remedies.

Conclusion

In the aftermath of the Arab Spring, the EU's Dual-Use Regulation was given a political significance, perhaps rather unexpectedly, partly to respond to a series of reports that EU companies sold surveillance tools to those governments which had experienced popular uprising. As noted at the beginning of the chapter, the EU's dual-use export control is merely one of the tools available for the EU to mitigate the problematic consequences of transferring cyber surveillance technologies to non-EU destinations. This has to be combined with broader efforts to promote domestic compliance with human rights law, including the protection of journalists, both by EU member states themselves and their trading partners.

At least at the level of the EU, there has been a regulatory change towards the integration of human rights norms into the framework aimed at regulating the proliferation of sensitive items. Yet what was also highlighted by the EU's legislative debates and the wording of the relevant provisions was the marginalized presence of human rights and international humanitarian law as a yardstick for controlling the risks associated with dual-use items, including cyber surveillance items. Article 5(2) does not explicitly state that an exporter would be in breach of the provision for the failure to take steps to obtain information and assess the risks of serious violations of human rights. One could only assume that such a normative consequence is implicit in Article 5(2) and may be ensured at the national level. During the legislative processes, little attention was given to the specific types of human rights, tensions among different human rights, and the difficulty in relying on technical features as a source for assessing normative risks. Within the field developed for the mitigation of military risks, human rights norms are invoked, but they tend not to be given substantial presence—unless the implementation of rights-based risk assessment continues to be monitored by governments, civil society organizations, and researchers.

Overall, Article 5(2) of Regulation 2021/821 is an important step forward when seen from the traditional military-based perspective about the field of law. Whether or not this represents a significant advancement in mitigating human rights risks associated with the sale of cyber surveillance depends on how practices of due diligence engage with other instruments in the field of business and human rights. Due to the explicit engagement with human rights and international humanitarian law, Article 5(2) created an important deliberative bridge between the community of export control professionals, on the one hand, and the broader community of business and human rights, on the other hand. In this sense, the "modernization" of the Dual-Use Regulation created the opportunity for shared endeavors for governments, industry, researchers, and civil society organizations in their efforts to detect and respond to the uncontrolled proliferation of surveillance technologies in the digital age.

References

Access Now et al. 2021. "Joint Open Letter by Civil Society Organizations and Independent Experts Calling on States to Implement an Immediate Moratorium on the Sale, Transfer and Use of Surveillance Technology." Amnesty, July 27. https://www.amnesty.org/en/documents/doc10/4516/2021/en/.

Amnesty International. 2020. "Germany-Made FinSpy Spyware Found in Egypt, and Mac and Linux Versions Revealed." Amnesty, September 25. https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/.

Amnesty International, Privacy International, and Centre for Research on Multinational Corporations (SOMO). 2021. "Operating from the Shadows: Inside NSO Group's Corporate Structure." SOMO, 31 May. https://www.somo.nl/operating-from-the-shadows/.

Athens News. 2023. "Greek Deputy Foreign Minister Claims 'Export of Predator Spyware to Sudan.'" April 20. https://en.rua.gr/2023/04/20/greek-deputy-foreign-minister-claims-export-of-predator-spyware-to-sudan/.

BAFA. 2021. "Leaflet on Art. 5 of the EU Dual-Use Regulation (Regulation (EU) 2021/821)." October. German Federal Office for Economic Affairs and Export Control. https://www.bafa.de/SharedDocs/Downloads/EN/Foreign_Trade/ec_leaflet_art-5_eu-dual-use-regulation.html.

Commission Recommendation (EU) 2024/2659. 2024. "Guidelines on the Export of Cyber-Surveillance Items under Article 5 of Regulation (EU) 2021/821 of the European Parliament and of the Council." October 11. http://data.europa.eu/eli/reco/2024/2659/oj.

Council Common Position 2008/944/CFSP. 2008. "Defining Common Rules Governing Control of Exports of Military Technology and Equipment." *Official Journal of the European Union*, L 335/99. http://data.europa.eu/eli/compos/2008/944/oj.

Council of the EU. 2015. "Council Conclusions on the Action Plan on Human Rights and Democracy 2015–2019." July 20. https://op.europa.eu/publication-detail/-/publication/045bdbed-a943-11e5-b528-01aa75ed71a1.

European Commission. 2013. "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights." https://op.europa.eu/publication-detail/-/publication/ab151420-d60a-40a7-b264-adce304e138b.

European Commission. 2023. "Public Consultation: Guidelines on the Export of Cyber-surveillance Items under Article 5 of Regulation (EU) No 2021/821." March 31. https://policy.trade.ec.europa.eu/consultations/guidelines-export-cyber-surveillance-items-under-article-5-regulation-eu-no-2021821_en.

European Parliament. 2023. "Recommendation of 15 June 2023 to the Council and the Commission Following the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware (2023/2500(RSP))." P9_TA(2023)0244. http://data.europa.eu/eli/C/2024/494/oj.

Feldstein, Steven. 2019. "The Global Expansion of AI Surveillance." Carnegie Endowment for International Peace, September. https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance.

Feldstein, Steven, and Brian Kot. 2023. "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses." Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses.

ICRC. 2012. "What Are 'Serious Violations of International Humanitarian Law'? Explanatory Note." International Committee of the Red Cross. https://www.icrc.org/en/doc/assets/files/2012/att-what-are-serious-violations-of-ihl-icrc.pdf.

Kanetake, Machiko. 2018. "Balancing Innovation, Development, and Security: Dual-Use Concepts in Export Control Laws." In *Global Environmental Change and Innovation in International Law*, edited by N. Craik et al., 180–200. Cambridge: Cambridge University Press.

Kanetake, Machiko. 2019a. "The EU's Dual-Use Export Control and Human Rights Risks: The Case of Cyber Surveillance Technology." *Europe and the World: A Law Review* 3(1). https://doi.org/10.14324/111.444.ewlj.2019.14.

Kanetake, Machiko. 2019b. "The EU's Export Control of Cyber Surveillance Technology: Human Rights Approaches." *Business and Human Rights Journal* 4: 155–62. https://doi.org/10.1017/bhj.2018.18.

Kanetake, Machiko, and Ryngaert, Cedric. 2023. "Due Diligence and Corporate Liability of the Defence Industry: Arms Exports, End Use and Corporate Responsibility." Flemish Peace Institute. https://vlaamsvredesinstituut.eu/wp-content/uploads/2023/05/VVI-Rapport-Due-Dilligence-WEB-new.pdf.

Leigh Day. 2018. "Pro-Democracy Activists Launch Legal Action against British Spyware Companies." October 11. https://www.leighday.co.uk/News/News-2018/October-2018/Pro-democracy-activists-launch-legal-action-agains.

Marczak, Bill, et al. 2015. "Pay No Attention to the Server behind the Proxy: Mapping FinFisher's Continuing Proliferation." Citizen Lab Research Report no. 64, University of Toronto, October. https://hdl.handle.net/1807/97784.

Marczak, Bill, et al. 2021. "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware." Citizen Lab, December 16. https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

Michalopoulos, Sarantis. 2023. "Exclusive: EU Prosecutor Probes Greek 'Predatorgate.'" *EURACTIV,* April 4. https://www.euractiv.com/section/politics/news/exclusive-eu-prosecutor-probes-greek-predatorgate/.

Mijatović, Dunja. 2023. "Highly Intrusive Spyware Threatens the Essence of Human Rights." Council of Europe, January 27. https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights.

New York Times. 2022. "How the Global Spyware Industry Spiraled Out of Control." December 8. https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html.

PEGA Committee. 2023a. "European Parliament Draft Recommendation to the Council and the Commission." Rapporteur Sophie in 't Veld, B9-0260/2023, May 22. https://www.europarl.europa.eu/doceo/document/B-9-2023-0260_EN.html.

PEGA Committee. 2023b. "Report of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware (2022/2077(INI))." Rapporteur Sophie in 't Veld, A9-0189/2023, May 22. https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html.

Privacy International. 2016. "Open Season: Building Syria's Surveillance State." December. https://privacyinternational.org/report/1016/open-season-building-syrias-surveillance-state.

Pyetranker, Innokenty. 2015. "An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement." *Northwestern Journal of Technology and Intellectual Property* 13: 153–80. https://scholarlycommons.law.northwestern.edu/njtip/vol13/iss2/3.

Regulation (EU) 2021/821. 2021. "Setting up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit, and Transfer of Dual-Use Items (Recast)." *Official Journal of the European Union*, L 206/1, May 20. http://data.europa.eu/eli/reg/2021/821/oj.

Siatitsa, Ilia. 2022. *Serious Violations of Human Rights: On the Emergence of a New Special Regime.* Oxford: Oxford University Press.

Staatsanwaltschaft München I. 2023. "Anklageerhebung Wegen Gewerbsmäßigen Verstoßes Gegen das Außenwirtschaftsgesetz Durch den Nicht Genehmigten Verkauf von Überwachungssoftware an Nicht-EU-Länder." May 22. https://www.justiz.bayern.de/gerichte-und-behoerden/staatsanwaltschaft/muenchen-1/presse/2023/4.php.

Telloglou, Tassus, and Eliza Triantafillou. 2023. "Greek Ministry of Foreign Affairs Secret Investigation Reveals Spyware Export Licenses." *Inside Story*, May 7. https://insidestory.gr/article/greek-ministry-foreign-affairs-secret-investigation-reveals-predator-spyware-export-licenses.

UK National Contact Point. 2014. "Privacy International & Gamma International UK LTD, Final Statement After Examination of Complaint." UK National Contact Point for the OECD Guidelines for Multinational Enterprises, December. https://assets.publishing.service.gov.uk/media/5dd415444ofob6o6eab6423c/UK-NCP-Final-statement-complaint-Privacy-International-Gamma-International-UK-Ltd.pdf.

UN. 2011. "Guiding Principles on Business and Human Rights: Implementing the UN 'Protect, Respect and Remedy' Framework." HR/PUB/11/04. https://www.ohchr.org/en/publications/reference-publications/guiding-principles-business-and-human-rights.

UN Human Rights Council. 2009. "Business and Human Rights: Towards Operationalizing the 'Protect, Respect and Remedy' Framework." Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises. UN Doc. A/HRC/11/13, April 22. https://documents.un.org/doc/undoc/gen/g09/128/88/pdf/g0912888.pdf.

UN Human Rights Council. 2019. "Surveillance and Human Rights." Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. UN Doc. A/HRC/41/35, May 28. https://documents.un.org/doc/undoc/gen/g19/148/76/pdf/g1914876.pdf.

Van Daalen, Ot, et al. 2021. "The New Rules for Export Control of Cyber-Surveillance Items in the EU." Institute for Information Law (IViR), University of Amsterdam. June. https://www.ivir.nl/publicaties/download/Report-on-cybersurveillance-items.pdf.

Van der Vlist, Fernando N. 2017. "Counter-Mapping Surveillance: A Critical Cartography of Mass Surveillance Technology after Snowden." *Surveillance & Society* 15(1): 137–57. https://doi.org/10.24908/ss.v15i1.5307.

Wagner, Ben. 2012. *Exporting Censorship and Surveillance Technology.* Humanist Institute for Co-operation with Developing Countries (Hivos).

Wassenaar Arrangement. 2012. "List of Dual-Use Goods and Technologies and Munitions List." *WA-LIST* 12(1), December 12. https://www.wassenaar.org/app/uploads/2019/consolidated/WA-LIST%20%2812%29%201.pdf.

Wassenaar Arrangement. 2013. "List of Dual-Use Goods and Technologies and Munitions List." *WA-LIST* 13(1), December 4. https://www.wassenaar.org/app/uploads/2019/consolidated/WA-LIST%20%2813%29%201.pdf.

About the Author

Machiko Kanetake is associate professor of public international law at Utrecht University, and the director of the master's program in Public International Law.