Student Occasional Paper Series No. 5 | December 2023

The Efficacy of European Union Spyware Regulations

By Riley Phillips | Edited By Aaron Brantly

Abstract:

Supranational organizations like the European Union (EU) have struggled to enforce successful legal frameworks that adequately regulate and enforce the export and misuse of malware technologies. Considering the Pegasus Project and the newly released Predator Files, EU systems of regulation fall short at addressing the broader malware market abuse, production, and proliferation. Despite numerous export regulations EU states membership in the acclaimed organization has provided a false sense of security and accountability for the upholding of human rights. Pegasus Project and Predator files reveal the mass proliferation of spyware throughout the EU by leveraging its vague export controls and state centered accountability methods. The 2022 EU directive and legislation efficacy fails to uphold export arrangements and by extension United Nations (UN) and EU human rights standards through terminological loopholes and proliferative export regulations.

Spyware Market Within the EU

As it currently exists, the spyware economy thrives under the guise of supranational export controls implemented under national jurisdiction. From 2011 to 2020 Steven Feldstein identified 65 countries as commercial spyware clients.[1] As of 2023, that number rose to seventy-four states.[2] Private spyware companies like NSO Group, Intellexa, and Candiru remain largely unregulated despite public backlash due to the high demand of spyware technology.[3] Enabling this demand, democratic nations send mixed messaging on their stance towards spyware through obscure export regulations.[4] The Wassner Arrangement (WA) and the EU's Dual Use Regulations (EUDUR) serve to regulate export controls of dual use items through control lists. This is one way the EU establishes itself as an export control regime with little to no efficacy. Recent publications by spyware investigations like the EU Parliament's PEGA Committee characterize export controls under the WA and EUDUR as being "'deliberately'" lax when it comes to national implementation.[5] As a result, loopholes within export controls facilitate the proliferation of

spyware resulting in deleterious effects on journalists, politicians, activists, and more. The EU Directive following PEGA committee investigations identified the spying of "journalists, prosecutors, civil society actors," and politicians in Poland, Hungary, Greece, Spain, Luxembourg, Cyprus, and Austria.[6] Claiming that it is "safe to assume that all Member States have purchased or used one or more spyware systems."[7] PEGA Committee findings were further affirmed through the publication of Predator files by Amnesty International in 2023. Revealing EU's failure to regulate spyware and by extension uphold international human rights standards.

Dual Use Export Controls

Export controls function as a means of regulating goods and services within the global market. The term dual use refers to technologies that are "'applicable both for military purposes and for...civilian ends.'"[8] In other words, dual use is used to ensure that the application of potentially dangerous goods like weapons of mass destruction are only used for peaceful ends.[9] Dual use controls, however, only apply to a nation's purpose of trade leaving the application of dual use goods like spyware unregulated. The EU's multilateral control regime facilitating spyware-related technologies is the recast EUDUR which deems dual use through a "'military'" versus "'civil'" lens.[10] Through this lens spyware's application is determined by how the technology would be used by their end-use and user giving national government full jurisdiction of dual use technologies applications.[11] Spyware firms utilize dual use legislation as a way of legitimizing malware as a product on the market for crime prevention and counterterrorism efforts and not a weapon or software affiliated with violence. The intention behind export regulations is to limit military misuse by states. To uphold the intention of export regulations, agreements require companies like NSO Group to stop selling their spyware to human rights offenders or to implement due diligence requirements.[12] Under the current export regime model, obscurity of diction and lack national accountability results in the failure of the EU to uphold international and intra-European standards of export and human rights by enabling the proliferation of spyware.

How Spyware is Proliferated under EU Legislation

Spyware's distribution leverages export regulations and agreements to supply the demand within its market. Cybersecurity companies utilize "regulatory fragmentation" in EU member states where the implementation of dual use controls and other regulatory protections have a history of being weak.[13] EU states that have been documented failing to uphold regulation standards include Cyprus, Bulgaria, and Greece.[14] By leveraging loopholes within EUDUR, spyware is distributed throughout but not restricted to the European Union. This was directly acknowledged in the EU Directive in May of 2023 identifying "Pegasus and equivalent software" abuse of human rights through the surveillance of "journalists, politicians, law enforcement officials, diplomats, lawyers, businesspeople, civil society actors, and other actors."[15] It is also worth noting that this demand is widespread with twenty-two end-users in fourteen EU member states acquiring Pegasus.[16] EU legislation like the EUDUR doesn't assess the efficacy of states' legal frameworks. For example, if "the end use of the technology by the end use is lawful in the importing jurisdiction."[17] This means that if the technology isn't endangering the exporting country in its application, then the export is not subject to export control.[18] Furthermore, the EU has no legislative power to enforce regulation at the national level since there are no accountability checks on national compliance. As a result, companies like Intellexa establish subsidiaries in states that overlook spyware activities as a way of bypassing controls.[19] NSO group established

subsidiaries in Bulgaria and Cyprus both states that have a history of spyware activity and overlooking export controls.[20] Subsidiary companies take advantage of end-use and end-user differentiation, obscure legislation, and export country oversight to bypass EU export regulations. Not only does this violate EU regulations but also violates UN Human Rights. The situation is only further complicated when subsidiaries and trojan computers are internationally located ensuring oversight on the proliferation of spyware by the EU.

EU proliferation is not limited to the EU but spreads spyware globally through different canals of oversight. States' status as EU members is seen as a sufficient guarantee of human rights exempting countries from due diligence measures. For example, Israel's export authority doesn't require EU member states to submit human rights assessment despite it usually being a requirement for receiving an export license.[21] In some instances, Allocations form the EU's Emergency Trust Fund for Africa gave Niger's government mobile interception technology without carrying out risk assessment.[22] Predator files illuminated and echoed the effects of EU legislation and lack of risk evaluation. Specifically, the Predator Files identified Irish-based Intellexa Alliance products as being circulated widely. Intellexa Alliance technologies were found present in twenty-five countries across four continents.[23] Like other spyware companies Intellexa functions through subsidiary entities in "France, Germany, Greece, Ireland, Czech Republic, Cyprus, Hungary, Switzerland, Israel, North Macedonia, and the United Arab Emirates (UAE)."[24] Lack of government oversight and indiscriminate distribution of malware technology promotes human rights abuses despite export regulation regardless of regime.

Dual Use Export Controls

Export controls function as a means of regulating goods and services within the global market. The term dual use refers to technologies that are "'applicable both for military purposes and for...civilian ends.'"[25] In other words, dual use is used to ensure that the application of potentially dangerous goods like weapons of mass destruction are only used for peaceful ends.[26] Dual use controls, however, only apply to a nation's purpose of trade leaving the application of dual use goods like spyware unregulated. The EU's multilateral control regime facilitating spyware-related technologies is the recast EUDUR which deems dual use through a "'military'" versus "'civil'" lens.[27] Through this lens spyware's application is determined by how the technology would be used by their end-use and user giving national government full jurisdiction of dual use technologies applications.[28] Spyware firms utilize dual use legislation as a way of legitimizing malware as a product on the market for crime prevention and counterterrorism efforts and not a weapon or software affiliated with violence. The intention behind export regulations is to limit military misuse by states. To uphold the intention of export regulations, agreements require companies like NSO Group to stop selling their spyware to human rights offenders or to implement due diligence requirements.[29] Under the current export regime model, obscurity of diction and lack national accountability results in the failure of the EU to uphold international and intra-European standards of export and human rights by enabling the proliferation of spyware.

How Spyware is Proliferated under EU Legislation

Spyware's distribution leverages export regulations and agreements to supply the demand within its market. Cybersecurity companies utilize "regulatory fragmentation" in EU member states where the implementation of dual use controls and other regulatory protections have a

history of being weak.[30] EU states that have been documented failing to uphold regulation standards include Cyprus, Bulgaria, and Greece.[31] By leveraging loopholes within EUDUR, spyware is distributed throughout but not restricted to the European Union. This was directly acknowledged in the EU Directive in May of 2023 identifying "Pegasus and equivalent software" abuse of human rights through the surveillance of "journalists, politicians, law enforcement officials, diplomats, lawyers, businesspeople, civil society actors, and other actors."[32] It is also worth noting that this demand is widespread with twenty-two end-users in fourteen EU member states acquiring Pegasus.[33] EU legislation like the EUDUR doesn't assess the efficacy of states' legal frameworks. For example, if "the end use of the technology by the end use is lawful in the importing jurisdiction."[34] This means that if the technology isn't endangering the exporting country in its application, then the export is not subject to export control.[35] Furthermore, the EU has no legislative power to enforce regulation at the national level since there are no accountability checks on national compliance. As a result, companies like Intellexa establish subsidiaries in states that overlook spyware activities as a way of bypassing controls.[36] NSO group established subsidiaries in Bulgaria and Cyprus both states that have a history of spyware activity and overlooking export controls.[37] Subsidiary companies take advantage of end-use and end-user differentiation, obscure legislation, and export country oversight to bypass EU export regulations. Not only does this violate EU regulations but also violates UN Human Rights. The situation is only further complicated when subsidiaries and trojan computers are internationally located ensuring oversight on the proliferation of spyware by the EU.

EU proliferation is not limited to the EU but spreads spyware globally through different canals of oversight. States status as EU members is seen as sufficient guarantee of human rights exempting countries from due diligence measures.[38] For example, Israel's export authority doesn't require EU member states to submit human rights assessment despite it usually being a requirement for receiving an export license.[39] In some instances, Allocations form the EU's Emergency Trust Fund for Africa gave Niger's government mobile interception technology without carrying out risk assessment.[40] Predator files illuminated and echoed the effects of EU legislation and lack of risk evaluation. Specifically, the Predator Files identified Irish-based Intellexa Alliance products as being circulated widely. Intellexa Alliance technologies were found present in twenty-five countries across four continents.[41] Like other spyware companies Intellexa functions through subsidiary entities in "France, Germany, Greece, Ireland, Czech Republic, Cyprus, Hungary, Switzerland, Israel, North Macedonia, and the United Arab Emirates (UAE)."[42] Lack of government oversight and indiscriminate distribution of malware technology promotes human rights abuses despite export regulation regardless of regime.

Implications looking forward

The spyware market remains formidable and vibrant despite recent public revelations through publications like PEGA committee directive and Predator Files. Under current export and legislative oversight, the spyware market within the EU and by extension globally continues to grow. Loopholes that facilities state oversight of risk calculation and human rights reports result in abuse of government surveillance as evident through the PEGA committee research and Predator Files report. Long term approaches to curb the proliferation and abuse of spyware technologies require an analysis of market demand. In the meantime, supranational organizations have the potential to curb the human rights abuses caused by malware misuse. Firstly, the status of spyware as a dual use service through analysis of its application displaying its continuous abuse of human rights rings inaccurate and harmful to populations of democratic and nondemocratic states

alike. Due to spyware's weapon-like application, it could be argued that spyware software should be under controls similar to that of arms. Beyond spyware's regulatory classification, the lack of accountability that supranational organizations continue to uphold within their legislative bodies facilitates state oversight. In response, Accountability measures and repercussions are necessary to communicate intolerance of abuse and dedication to upholding human rights. Without efficacious regulations, the spyware market will continue to thrive. Looking forward, litigate action must be taken in response to recent reports alongside an evolution within regulations regarding spyware in the hopes of maintaining human rights.

Bibliography

"Armenia/Azerbaijan: Pegasus Spyware Targeted Armenian Public Figures amid Conflict," May 25, 2023. https://www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict/.

Bauer, Sibylle, and Mark Bromley. "Challenges and Good Practices in Detecting,Investigating and Prosecuting Export Control Violations." *Stockholm International Peace Research Institute*, December 1, 2019, 7–22. https://www.jstor.org/stable/resrep20061.8.

"BLASTPASS NSO Group IPHone Zero-Click, Zero-Day Exploit Captured Int He Wild," September 7, 2023. https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/.

Feldstein. "Commercial Spyware Global Inventory." *Mendeley Data* V2 (December 7, 2020). https://doi.org/10.17632/csvhpkt8tm.2.

Feldstein, Steven. "Distinguishing Between Legitimate and Unlawful Surveillance." *The Global Expansion of AI Surveillance*, September 1, 2019. https://www.jstor.org/stable/resrep20995.6.

Feldstein, Steven, and Brian Kot. "Explaining the Resilience of the Global Spyware and Digital Forensics Industry." *Carnegie Endowment for International Peace* 137, no. 3476 (March 1, 2023): 980–980. https://doi.org/10.1038/137980d0.

Fittarelli, Alberto, and Lokman Tsui. "Beautiful Bauhinia," July 13, 2023, 61.

"Global: 'Predator Files' Spyware Scandal Reveals Brazen Targeting of Civil Society, Politicians and Officials," October 9, 2023. https://www.amnesty.org/en/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting-of-civil-society-politicians-and-officials/.

Riecke, Lena. "Unmasking the Term 'Dual Use' in EU Spyware Export Control." *European Journal of International Law*, 2023, chad039. https://doi.org/10.1093/ejil/chad039.

Scott-Railton, John, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, and and Ron Deibert. "CatalanGate Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru," n.d. https://joan.domenechmilan.com/wp-content/uploads/2022/04/citizenlab.ca-CatalanGate-Extensive-Mercenary-Spyware-Operation-against-Catalans-Using-Pegasus-and-Candiru.pdf.

Veld, Sophie in 't. "EUROPEAN PARLIAMENT DRAFT RECOMMENDATION 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," May 22, 2023. https://www.europarl.europa.eu/doceo/document/B-9-2023-0260_EN.html.

Whang, Cindy. "Trade and Emerging Technologies." *Security and Human Rights* 31, no. 1–4 (2021): 11–34. https://doi.org/10.1163/18750230-31010007.

Endnotes

[1] John Scott-Railton et al., "CatalanGate Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru," n.d., https://joan.domenechmilan.com/wp-content/uploads/2022/04/citizenlab.ca-CatalanGate-Extensive-Mercenary-Spyware-Operation-against-Catalans-Using-Pegasus-and-Candiru.pdf.

[2] Feldstein, "Commercial Spyware Global Inventory," *Mendeley Data* V2 (December 7, 2020), https://doi.org/10.17632/csvhpkt8tm.2.

[3] Steven Feldstein, "Distinguishing Between Legitimate and Unlawful Surveillance," *The Global Expansion of AI Surveillance*, September 1, 2019, https://www.jstor.org/stable/resrep20995.6.Feldstein.

[4] Feldstein, S. (2019). Distinguishing Between Legitimate and Unlawful Surveillance. *The Global Expansion of AI Surveillance*. https://www.jstor.org/stable/resrep20995.6

[5] Sophie in 't Veld, "EUROPEAN PARLIAMENT DRAFT RECOMMENDATION 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," May 22, 2023, https://www.europarl.europa.eu/doceo/document/B-9-2023-0260_EN.html.

[6] Veld.

[7] Veld.

[8] Lena Riecke, "Unmasking the Term 'Dual Use' in EU Spyware Export Control," *European Journal of International Law*, 2023, chad039, https://doi.org/10.1093/ejil/chad039.

[9] Veld, "EUROPEAN PARLIAMENT DRAFT RECOMMENDATION 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."

[10] "Armenia/Azerbaijan: Pegasus Spyware Targeted Armenian Public Figures amid Conflict," May 25, 2023, https://www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict/.

[11] Cindy Whang, "Trade and Emerging Technologies," *Security and Human Rights* 31, no. 1–4 (2021): 11–34, https://doi.org/10.1163/18750230-31010007.Whang.

[12] Steven Feldstein and Brian Kot, "Explaining the Resilience of the Global Spyware and Digital Forensics Industry," *Carnegie Endowment for International Peace* 137, no. 3476 (March 1, 2023): 980–980, https://doi.org/10.1038/137980d0.

[13] Feldstein and Kot.

[14] Veld, "EUROPEAN PARLIAMENT DRAFT RECOMMENDATION 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."

[15] Feldstein, "Commercial Spyware Global Inventory."

[16] Feldstein and Kot, "Explaining the Resilience of the Global Spyware and Digital Forensics Industry."

[17] Feldstein and Kot.

[18] Whang, "Trade and Emerging Technologies."

[19] Feldstein and Kot, "Explaining the Resilience of the Global Spyware and Digital Forensics Industry."

[20] Feldstein, "Distinguishing Between Legitimate and Unlawful Surveillance."

[21] Feldstein and Kot, "Explaining the Resilience of the Global Spyware and Digital Forensics Industry."

[22] Feldstein and Kot.

[23] "Global: 'Predator Files' Spyware Scandal Reveals Brazen Targeting of Civil Society, Politicians and Officials," October 9, 2023, https://www.amnesty.org/en/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting-of-civil-society-politicians-and-officials/.

[24] "Global: 'Predator Files' Spyware Scandal Reveals Brazen Targeting of Civil Society, Politicians and Officials."

[25] Riecke, "Unmasking the Term 'Dual Use' in EU Spyware Export Control."

[26] Alberto Fittarelli and Lokman Tsui, "Beautiful Bauhinia," July 13, 2023, 61.

[27] "BLASTPASS NSO Group iPhone Zero-Click, Zero-Day Exploit Captured Int He Wild," September 7, 2023, https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/.

[28] Whang, "Trade and Emerging Technologies."

[29] Feldstein and Kot, "Explaining the Resilience of the Global Spyware and Digital Forensics Industry."

[30] Feldstein and Kot.

[31] Veld, "EUROPEAN PARLIAMENT DRAFT RECOMMENDATION 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."

[32] Sibylle Bauer and Mark Bromley, "Challenges and Good Practices in Detecting,Investigating and Prosecuting Export Control Violations," *Stockholm International Peace Research Institute*, December 1, 2019, 7–22, https://www.jstor.org/stable/resrep20061.8.

[33] Feldstein and Kot, "Explaining the Resilience of the Global Spyware and Digital Forensics Industry."

[34] Bauer and Bromley, "Challenges and Good Practices in Detecting,Investigating and Prosecuting Export Control Violations."

[35] Whang, “Trade and Emerging Technologies.”

[36] Feldstein and Kot, “Explaining the Resilience of the Global Spyware and Digital Forensics Industry.”

[37] Feldstein, “Distinguishing Between Legitimate and Unlawful Surveillance.”

[38] Feldstein and Kot, “Explaining the Resilience of the Global Spyware and Digital Forensics Industry.”

[39] Feldstein, “Commercial Spyware Global Inventory.”

[40] Feldstein and Kot, “Explaining the Resilience of the Global Spyware and Digital Forensics Industry.”

[41] “Global: ‘Predator Files’ Spyware Scandal Reveals Brazen Targeting of Civil Society, Politicians and Officials.”

[42] “Global: ‘Predator Files’ Spyware Scandal Reveals Brazen Targeting of Civil Society, Politicians and Officials.”