THE PREDATOR FILES: CAUGHT IN THE NET

THE GLOBAL THREAT FROM "EU REGULATED" SPYWARE

EXECUTIVE SUMMARY

AMNESTY INTERNATIONAL

Amnesty International is a movement of 10 million people which mobilizes the humanity in everyone and campaigns for change so we can all enjoy our human rights. Our vision is of a world where those in power keep their promises, respect international law and are held to account. We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and individual donations. We believe that acting in solidarity and compassion with people everywhere can change our societies for the better.

First published in 2023
by Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

Index: ACT 10/7246/2023
Original language: English

amnesty.org

Cover illustration: *© Colin Foo 2023*

AMNESTY INTERNATIONAL

EXECUTIVE SUMMARY

Over the past decade, civil society organizations, researchers, and journalists have exposed how governments around the world have been unlawfully targeting activists, journalists, and politicians using tools developed by private cyber-surveillance companies. Amnesty International and numerous civil society organizations have repeatedly warned that states' opaque trade and deployment of privately manufactured surveillance technologies, particularly spyware, have wrought a digital surveillance crisis, which has severely and detrimentally impacted human rights, media freedoms, and social movements across the world. The 2021 Pegasus Project disclosures — which exposed the global scale and breadth of unlawful surveillance facilitated by NSO Group's Pegasus spyware — and subsequent civil society research have forced governments around the world to take note of the massive scale and breadth of spyware abuse, spurring the beginnings of action to rein in some of the most notorious spyware vendors. However, fresh disclosures by Amnesty International, and the findings of the new Predator Files investigation coordinated by European Investigative Collaborations (EIC) media network, have laid bare how government action has been inadequate and ineffective in ending spyware abuse. This report details these findings.

First, as part of the Predator Files investigation, Amnesty International's Security Lab collaborated with EIC, a partnership of European media organizations, as a technical partner. Amnesty International analysed documents accessed by EIC to ascertain the technical specifications of a suite of surveillance products developed, operated, and marketed by the Intellexa alliance — which is an alliance of surveillance technology companies — between 2007 and 2022. Amnesty International found that this includes a host of targeted and mass surveillance technologies.

Targeted surveillance technologies include highly invasive mobile spyware like Predator, which can be delivered to devices using either 1-click attacks or 0-click attacks. The Intellexa alliance also offers various techniques to install the spyware through "tactical attacks", which enable the targeting of devices in close physical proximity. In addition, strategic infection methods have also been developed, operated, and marketed by the Intellexa alliance. These methods allow a state actor to deliver silent infection attempts to users of cooperating internet service providers, or across a whole country if the spyware operator has direct access to internet traffic. Strategic infection systems resemble mass surveillance tools as they require access to large-scale internet traffic to target and infect individuals. The mass and "massive" surveillance products offered by the Intellexa alliance suggest an evolution of earlier surveillance technologies from lawful interception systems that allowed traffic monitoring in a targeted, individualised manner — that potentially allowed for more checks and limitations —to more overbroad and indiscriminate methods.

Amnesty International believes that both types of technologies — highly invasive spyware and indiscriminate mass surveillance tools — are fundamentally incompatible with human rights. The Predator spyware, and its rebranded variants, are highly invasive spyware that can access unlimited amounts of data on the device and cannot, at present, be independently audited. As such, Amnesty International's assessment is that no deployment of Predator and other such forms of highly invasive spyware can be human rights compliant, and they should be permanently banned.

Second, in this report, Amnesty International has revealed a previously undisclosed targeted surveillance operation by a customer of Intellexa's Predator spyware with connections to Viet Nam. The customer appears to be aligned with government interests in Viet Nam, and between February and June 2023, it targeted at least 50 social media accounts belonging to 27 individuals and 23 institutions, using spyware tools developed and sold by the Intellexa alliance. The targeting was done using 1-click attacks sent to the

social media accounts of individuals and institutions from an X (formerly known as Twitter) account called @Joseph_Gordon16. Those targeted as part of this spyware operation include a Berlin-based independent news website, political figures in the European Parliament, the European Commission, academic researchers, and think-tanks. In addition to these, other attempted targets include United Nations officials, the President of Taiwan, United States senators and representatives, and other diplomatic authorities.

Google's Threat Analysis Group confirmed to Amnesty International that Google's own research had identified that the domains and URLs that Amnesty International discovered as part of the spyware operation were linked to the Intellexa alliance's Predator spyware system. Together with evidence from EIC partners, our findings show evidence of sales of Intellexa alliance's surveillance products to the Vietnamese Ministry of Public Security and suggest that agents of the Vietnamese authorities, or persons acting on their behalf, may be behind the spyware campaign. In addition, Google confirmed to EIC partners that they "associate" the Intellexa Predator campaign and indicators described in this report to "a government actor in Vietnam".

These disclosures are based on ongoing technical research by Amnesty International's Security Lab to monitor the development and deployment of surveillance technologies offered by mercenary spyware companies, including those offered by the Intellexa alliance. As part of these efforts, Amnesty International's analysis of recent technical infrastructure linked to the Predator spyware system also indicates likely active customers or targeting of individuals in Sudan, Madagascar, Kazakhstan, Mongolia, Egypt, Indonesia, Viet Nam, and Angola.

The findings in this report are also based on an interview with a targeted journalist from Viet Nam, shipment records, trade data, and other EIC research and reporting into the Intellexa alliance's sales of surveillance and infection solutions. Amnesty International also reviewed reports, statements, laws, and studies by UN bodies and experts, regional and various national level authorities, investigative and policy reports by civil society organizations, as well as media reports.

Third, this report discusses the human rights implications of the Predator Files disclosures, which show how a suite of highly invasive surveillance technologies supplied by the Intellexa alliance is being sold and transferred around the world with impunity. The Intellexa alliance is comprised of various surveillance vendors with a corporate presence in European Union (EU) member states, as well as other countries around the world. The disclosures show the global scale and breadth of sales of surveillance technologies of just one alliance of surveillance vendors, which has been supplying its wares to Egypt, Libya, Madagascar, Saudi Arabia, Viet Nam, and France among many others between 2007 and 2022. These transfers pose a high likelihood of human rights violations due to past instances of unlawful surveillance in these countries and/or an absence of domestic surveillance safeguards that could prevent these technologies from being unlawfully unleashed on civil society, journalists, or opposition politicians.

Fourth, this report details a history of human rights abuses that have been linked to the Intellexa alliance in Greece, Libya, and Egypt. Intellexa advertises itself as an "EU based and regulated company". The Intellexa alliance reportedly comprises of Nexa Technologies and Advanced Middle East Systems (comprising the Nexa group), as well as WiSpear, Cytrox and Senpai Technologies (comprising the Intellexa group). The Nexa and Intellexa groups of companies control multiple corporate entities, some of which have been renamed. The entities span various jurisdictions, both within and outside the EU. The exact nature of links between these companies is shrouded in secrecy, as corporate entities and the structures between them are constantly morphing, renaming, rebranding, and evolving. These opaque and complex corporate structures appear to make it easier for companies to evade accountability, transparency, and government regulation, including regional and national export controls and corporate due diligence mechanisms. In the case of the Intellexa alliance, the picture is even more complex, due to corporate structures of not only one primary company, but its allied surveillance product vendors, its parent companies, and their investors. The convoluted nature of this corporate entity could make accountability and transparency for unlawful targeting using tools of this surveillance alliance even harder.

As laid out in the UN Guiding Principles on Business and Human Rights (UN Guiding Principles), companies have a responsibility to respect human rights wherever they operate in the world. In order to meet that responsibility, companies must carry out human rights due diligence. The companies in the Intellexa alliance have themselves not proactively disclosed any information about their human rights due diligence practices. Any assessments, if they exist, about the human rights impacts of their surveillance technologies remain shrouded in secrecy. Nation states also have binding obligations under international human rights law to protect human rights from abuse by third parties. This includes the obligation to regulate the conduct of companies who are domiciled in their territory or are under their effective control in order to prevent them from causing or contributing to human rights abuses even if they occur in other countries. The failure of states to put a meaningful check on the Intellexa alliance, – for example, states where the alliance's

corporate entities are based, which includes Greece, Ireland, France, Germany, Czech Republic, Cyprus, Hungary, Switzerland, Israel, North Macedonia, and the UAE – has led to human rights violations. Taken together, the above-mentioned findings show that civil society and journalists continue to face the devastating consequences of unlawful and unchecked use of surveillance technologies, which continue to threaten the rights to privacy, freedom of expression, association, and peaceful assembly of those targeted. In addition, as detailed in this report, the targeting of regional, national, and international official authorities, shows once again that commercial spyware has severe implications both for human rights and the security of the digital ecosystem. Unregulated, these surveillance technologies can and have been turned back on third governments and authorities.

These findings are just the tip of the iceberg. As surveillance companies and their state clients continue to hide behind the rhetoric of national security and confidentiality to evade transparency and accountability, the actual scale and breadth of unlawful targeting using tools supplied by the Intellexa alliance is likely to be much higher. Warnings by civil society and lessons from the Pegasus Project mean that for each of the countries where disclosures reveal that the Intellexa alliance has sold its technologies, civil society could be facing wholesale clandestine surveillance. These new disclosures make clear, yet again, that the unchecked sale and transfer of surveillance technologies could continue to facilitate human rights abuse on a massive global scale, as companies are still being allowed to freely sell and transfer their wares in utmost secrecy. Our findings demonstrate once more that any claims by companies that unlawful targeting is anomalous are decidedly false. Human rights abuse is a feature of the industry, not a bug.

In the aftermath of the Pegasus Project disclosures, states have taken some steps in the right direction to regulate the industry and state-use of these technologies. Some are significant and welcome steps in the right direction. However, public declarations, recommendations, and voluntary commitments have not always translated into action, and those unlawfully targeted with spyware around the world have not yet obtained meaningful accountability or remedies. While some states have initiated voluntary efforts, others have stone-walled investigations and failed to provide meaningful transparency. There need to be more concerted efforts by states to put in place binding and enforceable human rights safeguards at a national, regional and international level. In 2019, the former UN Special Rapporteur on Freedom of Opinion and Expression noted “It is insufficient to say that a comprehensive system for control and use of targeted surveillance technologies is broken. It hardly exists.” Amnesty International believes that despite initial progress, this is still the case.

In particular, the latest disclosures paint a dismal picture of failures of the EU and its member states to rein in unaccountable companies and errant member states, which continue to take advantage of the conspicuously large cracks in the regulatory systems at regional and national levels. The brazen surveillance campaign detailed in this report using the Intellexa alliance's tools shows the very direct risks from the uncontrolled proliferation and transfer of cyber-surveillance tools from countries within the EU. Not only do they lead to human rights abuses abroad, but they are also a threat to security and human rights within the EU.

Exports of spyware from the EU are subject to licensing under the Dual-Use Export Regulation, which should, in theory, take account of human rights risks posed by such exports. The “Predator Files” disclosures, however, demonstrate that export licences for surveillance technologies were granted by member states when there was a substantial risk of human rights violations by the end users. Disclosures also show that EU export control regulations were circumvented through opaque corporate structures and entities in third countries. It is clear that the EU Dual-Use Export Regulation has significant shortcomings. Two years after the publication of the Recast Dual Use regulation, it has not been robustly and transparently implemented. The European Parliament’s Pegasus and other Equivalent Spyware Investigation Committee (PEGA Committee) also pointed to the lack of political will of the EU and member states. While ongoing legislative efforts like the Corporate Sustainability Due Diligence Directive (CSDDD) offer a timely opportunity to begin to address the harms of the targeted surveillance sector, the loopholes in the proposals put forward by the EU co-legislators could mean the CSDDD is not properly applied to surveillance technology companies.

KEY RECOMMENDATIONS TO STATES

In light of the ineffectiveness of the current regulation, as well as the intrinsically abusive nature of Predator, all states should:

- (Particularly states that have granted export licences) Immediately revoke all marketing and export licences issued to the Intellexa alliance and conduct an independent, impartial, transparent investigation to determine the extent of unlawful targeting, to culminate in public statement on results of efforts and steps to prevent future harm.
- Enforce a ban on the use of highly invasive spyware. Such spyware cannot, at present, be independently audited or limited in its functionality to only those functions that are necessary and proportionate to a specific use and target.
- Implement a human rights regulatory framework that governs surveillance and that is in line with international human rights standards. Until such a framework is implemented, a moratorium on the purchase, sale, transfer, and use of all spyware should be enforced.
- Implement domestic legislation that imposes safeguards against human rights violations and abuses through digital surveillance and establish accountability mechanisms designed to provide victims of surveillance abuses a pathway to remedy.
- Legally require surveillance companies to conduct human rights due diligence in relation to their global operations, including on the use of their products and services.

KEY RECOMMENDATIONS TO THE EUROPEAN UNION AND ITS MEMBER STATES

- EU member states and the European Commission should ensure the robust implementation of the 2021 EU Export Control Rules. This includes taking immediate action towards underscoring the human rights due diligence obligations that follow from the Dual-Use Regulation and creating a transparent market in cybersurveillance technologies that is bound by effective human rights safeguards.
- EU member states must adopt and enforce legislation that requires all corporate actors to respect human rights and implement human rights due diligence measures in line with the UN Guiding Principles. As part of the ongoing deliberations on the Corporate Sustainability Due Diligence Directive (CSDDD), the EU should require companies to conduct human rights due diligence with respect to the full value chain including the purchase, sale, transfer, export and use of products. Companies operating in all sectors should implement the requirements on the CSDDD including those producing spyware, as well as financial institutions.

KEY RECOMMENDATIONS TO GOVERNMENT OF VIET NAM

The Government of Viet Nam should conduct an independent, impartial, and transparent investigation into the unlawful targeted surveillance mentioned in this report, including investigating whether there are links between this spyware campaign and any specific government agencies.

KEY RECOMMENDATIONS TO THE INTELLEXA ALLIANCE

The Intellexa alliance should cease the production and sale of Predator, or any other similar highly invasive spyware that does not include technical safeguards allowing for its lawful use under a human right respecting regulatory framework. It should also provide adequate compensation or other forms of effective redress to victims of unlawful surveillance.

AMNESTY INTERNATIONAL IS A GLOBAL MOVEMENT FOR HUMAN RIGHTS. WHEN INJUSTICE HAPPENS TO ONE PERSON, IT MATTERS TO US ALL.

CONTACT US


info@amnesty.org


+44 (0)20 7413 5500

JOIN THE CONVERSATION


www.facebook.com/AmnestyGlobal


@Amnesty