EDPS meeting with NSO Group on Pegasus spyware

21 June 2022, 09:30 - 10:30, MTS30, 6th floor meeting room

Purpose of event

A meeting of the European Data Protection Supervisor with representatives of NSO Group, who will be in Brussels to meet with the European Parliament's PEGA Commission of Inquiry on the same day, 21 June 2022, 15.00-18.30. The meeting has been requested by NSO Group with a letter dated 28 February 2022 and subsequently by an email dated 13 June 2022.

Participants:

NSO Group:

- [redacted] | Legal & Compliance Department, NSO Group
- [redacted] external Legal Counsel, [redacted]

EDPS:

- Mr Wojciech WIEWIÓROWSKI, Supervisor, European Data Protection Supervisor (*possible participation*)
- [redacted] European Data Protection Supervisor
- Ms Anna BUCHTA, Head of Unit, Policy and Consultation Unit, European Data Protection Supervisor
- [redacted] Policy and Consultation Unit, European Data Protection Supervisor
- [redacted] Policy and Consultation Unit, European Data Protection Supervisor

- [redacted] Technology and Privacy unit, European Data Protection Supervisor

Main messages:

- Highly advanced military-grade spyware like Pegasus has the potential to cause unprecedented risks and damages not only to the fundamental rights and freedoms of the individuals but also to democracy and the rule of law.

- Spyware like Pegasus constitutes a paradigm shift in terms of access to private communications and devices, which is able to affect the very essence of our fundamental rights, in particular the right to privacy. This fact makes its use incompatible with our democratic values.

- The EDPS believes a ban on the development and the deployment of spyware with the capability of Pegasus in the EU would be the most effective option to protect our fundamental rights and freedoms, until appropriate international standards and regulatory frameworks are in place.

- If such tools are nevertheless applied in exceptional situations, e.g. to prevent a very serious imminent threat, the EDPS has proposed a number of non-exhaustive list of steps and measures as a guarantee against unlawful use (*see the EDPS Preliminary Remarks*).

Defensives

Q 1. In the EDPS Preliminary Remarks ('report') page 4, section 2, the report states "one cannot exclude the possibility of using Pegasus beyond mere interception capabilities". Pegasus software is an intelligence gathering tool solely, and cannot be used for any other purposes based on contracts, technological capabilities provided with the system, and the End User Certificate issued to the customer by the Israeli Ministry of Defense.

Q 2. On the report's page 4, section 2, the report states that it (Pegasus?) could impersonate the victim" – Pegasus is unable to manipulate data on a target's phone (like sending messages on their behalf). Pegasus is designed with surveillance and data gathering capabilities and it is incapable of impersonating a victim.

EDPS: (*both to Q1 and Q2*) The EDPS Preliminary Remarks, issued on 15 February 2022, aim to contribute to the ongoing debate in the European Union and globally on the possible impact of modern spyware tools like Pegasus on fundamental rights, and particularly on the rights to privacy and data protection. The EDPS report is a **policy document**, not a forensic analysis, therefore it includes elements of **foresight about the possible future developments**. The EDPS intention was to highlight the technical possibility of modern spyware tools in general and their potential impact on privacy and data protection, not referring specifically to what is technically achievable in the case of Pegasus[1].

Q *3. On page 5, section 2, the report states that "all traces of the software vanishes" - while turning down the phone, and that "the attack infrastructure is in the cloud". While Pegasus is indeed hard to detect on a target's phone, it has a built-in investigative capability, in case a misuse is suspected, that making it impossible to erase and/or manipulate. Those capabilities cannot be completely vanished, and an "audit trail log" exists permanently, with the ability to retroactively check whether or not a certain phone number was hacked. NSO has been granted access by its customers to performed this type of investigation many times in the past, when an allegation of misuse arose, leading to shut down of systems and termination of seven contracts to date. Without this consent we are not privy to the phone numbers that are the subject of our customers' investigations.*

Q 4. On page 6, section 2, the report states that Pegasus creates "permanent and strong risk of massive security breaches…, comparable in a way to encryption backdoors". This

[1] The EDPS is not aware of any independent review of what is technically achievable with Pegasus.

statement is incorrect : the data collected by the customers is NOT stored in the cloud, any cloud, and there are no backdoors to the system. There is no shared data base of NSO's customers, contrary to some media reports, and the logs securely exists only on the servers of the customers, for the sole purpose of investigation of improper use. The Pegasus system allows for targeted surveillance only, with customers receiving license for a limited number of concurrent targets and is therefore inherently less intrusive then a backdoor. In this light we refer you to the recent interview of the Belgian Minister of Digitalisation and Privacy Mr. Mathieu. On that occasion Minister Mathieu stated he did "not agree with lowering the level of security and privacy of all Belgians' messages in order to conduct investigations from time to time. It's as if, because the police and the justice system do searches from time to time, everyone should leave their back door open". In this context Minister Mathieu further argued that "today we have technological means to access tapping other than by degrading the level of security of all Belgians. Look at the Pegasus software".

EDPS: (*both to Q3 and Q4*) As already stated, the EDPS report's intention is to highlight the technical possibility of modern spyware tools in general and itstheir potential impact on privacy and data protection, not referring specifically to what is technically achievable in the case of Pegasus.

The EDPS Preliminary Remarks have been based on the available media and civil society reports and investigations. The EDPS is also looking forward to the results of the ongoing official investigations, including judicial proceedings, reported in the media, which should provide additional information and details about technology.

In any event, the overarching objective of the EDPS is to ensure a strong and effective protection of the fundamental rights and freedoms of the individuals, including the rights to privacy and data protection, while taking into due consideration the general interest recognised by the European Union, such as the fight against terrorism and serious crimes.

EDPS understands that the technical possibilities of moderny spyware tools are based on cybersecurity vulnerabilities of smartphones. In practice, the exploitation of such vulnerabilities has the same result as the encryption backdoors: end to end encryptin is circumvented and access to data at rest and data in use is possible, despite end to end encryption.

Q 5. On page 6, section 3, the report states that you are basing your claims for misuse of our products on "worldwide media investigations." As stated earlier in this submission, these "worldwide media investigations" contain a number of assumptions and premises

that are wrong. Most recently, the Israeli news outlet Calcalist published a story dubbed "The Pegasus Affair" claiming that the Israeli police used Pegasus to infiltrate phones without a warrant, essentially conducting mass-surveillance of high-profile politicians, opposition leaders and activists, without the proper legal authority. The Deputy Attorney General along with representatives of the Mossad and the Shin Bet announced the findings of their investigation into the allegations. Their report found no evidence of wrongdoing. Shortly thereafter, Calcalist announced an investigation into their reporting to determine what went wrong. Unfortunately this scenario has repeated itself throughout the past several years. We have patiently responded to hundreds of media inquiries, walking reporters through our due diligence program, pointing to the release of our Transparency and Responsibility Report and stating that while we are restricted in what we can say due to confidentiality and national security issues, many of these allegations are wrong and, in some cases, they were contractually and technologically impossible. For example, the allegation which claimed that our products were misused on President Emmanuel Macron, Jeff Bezos, and Jamal Kashoggi is not true; they were never targeted by NSO's products.

EDPS: It is a well-known fact that the development and us of surveillance and interception technologies and tools is very much opaque and protected by secrecy and confidentiality rules. Therefore, as already mentioned before, we would welcome more official investigations and studies by competent authorities, given the seriousness of some of the allegations.

Furthermore, in the NSO letter to the EDPS of 28 February 2022 the company claims that: "*We deeply abhor any alleged or actual misuse of our products [...] we are especially troubled by credible allegations that our products may have been, or actually were, used in a manner that could have enabled improper or otherwise abusive surveillance of journalists, human rights advocates, and others. [...] we are undertaking several investigations to assess the reality of certain allegations*."

Could you share with us the outcomes of these investigations (if any)?

Background information

EP PEGA Committee

On 10 March 2022, the European Parliament decided to set up a **Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA Committee)** to investigate alleged infringement or maladministration in application of EU law in relation to the use of Pegasus and equivalent spyware surveillance software. In particular, the PEGA Committee is asked to gather information on the extent to which Member States or third countries are using intrusive surveillance to the extent that it

violates the rights and freedoms enshrined in the Charter of Fundamental Rights of the EU.

The PEGA Committee was established in accordance with Article 226 TFEU[2] with a twelve-month mandate.

The Committee has 38 Members and 38 substitute Members and is led by:

Chair: Jeroen Lenaers (EPP, NL)

First Vice-Chair: Sándor Rónai (S&D, HU)

Second Vice-Chair: Diana Riba i Giner (Greens/EFA, ES)

Third Vice-Chair: Moritz Körner (Renew, DE)

The PEGA Committe will make use of various methods to investigate the alleged violations: it will hold hearings with experts, victims and other persons, request studies and briefings and undertake fact-finding missions when needed. The investigations shall be concluded with the submission of a final report.

There are two dimensions to the investigation. The **internal** one is about the use or misuse by EU member states of Pegasus and other equivalent spyware. The committee is not only focusing on the spyware from the NSO Group. The **external** dimension relates to third countries and whether their use of spyware had an impact on fundamental rights ensured under EU law. The committee will also look into the role of the government of Israel and of other third countries in supplying Pegasus and equivalent surveillance spyware to member states.

The PEGA Committee has held so far the following public hearings:

- 14 June: Hearing on Big Tech and spyware

- 13 June: Hearing on Use, Supervision and Safeguards (**with the participation of Mr Wojciech Wiewiórowski, EDPS**)

[2] Article 226
In the course of its duties, the European Parliament may, at the request of a quarter of its component Members, set up a temporary Committee of Inquiry to investigate, without prejudice to the powers conferred by the Treaties on other institutions or bodies, alleged contraventions or maladministration in the implementation of Union law, except where the alleged facts are being examined before a court and while the case is still subject to legal proceedings.
The temporary Committee of Inquiry shall cease to exist on the submission of its report.
The detailed provisions governing the exercise of the right of inquiry shall be determined by the European Parliament, acting by means of regulations on its own initiative in accordance with a special legislative procedure, after obtaining the consent of the Council and the Commission.

- 9 June: Exchanges of views with UN representatives, including Dr. Ana Brian Nougrères, UN Special Rapporteur for Privacy

- 10 May: Hearing on Functioning of Pegasus and equivalent surveillance spyware

- 19 April: Exchange of views with Forbidden stories consortium/Citizen lab/Amnesty International.

EP internal checks for possible hacking

The EP has set up a tool to test if phones of MEPs are hacked, based on open source code provided by Amnesty International. The problem with such tools is that they can only detect old variants of Pegasus hack (one year ago).

EDPS has also established a similar tool to check if phones of EDPS staff members have been hacked.

Council of Europe report on Pegasus

On 20 June 2022 the Council of Europe published own report 'Pegasus spyware and its impacts on human rights'. Similarly to the EDPS Preliminary Remarks, the CoE report provides a technical description of the Pegasus spyware and analyses the impact it may have on human rights and fundamental freedoms, in particular the right to privacy and freedom of expression, as well as offers some practical advice regarding security.

Few specific takeaways from CoE report:

- Modus Operandi of the Pegasus clearly reveals its capacity to be used for targeted as well as **indiscriminate surveillance**[3]**;**

- Pegasus is designed for devices running not only the most widely used operating systems, such as Android and iOS, but also Windows, as well as **Blackberry** and **Symbian**[4]**;**

- Confirmation that Pegasus also monitors the keystrokes on an infected device, all written communications, including **passwords are visible to the attacker**[5]**;**

- **200 journalists** worldwide had been targeted using Pegasus spyware[6];

[3] CoE report 'Pegasus spyware and its impacts on human rights', page 10.
[4] Ibid, page 7.
[5] Ibid, page 8.
[6] Ibid, page 15.

- The **price** of Pegasus is quite high: an indication from 2016 suggests a $600K annual fee on top of a $500K setup fee for a system capable of tracking 10 targets simultaneously[7];

Other developments

There have been a number of media reports that the US defence contractor L3Harris is in talks to take over NSO Group's surveillance technology, in a possible deal that would give the American company control over Pegasus[8]. However, any agreement would require approval by the US and Israeli governments, which have not yet given the green light to a deal. Moreover, a senior White House official has already expressed concerns about the potential deal.[9]

Case officers / contact points

- [redacted]
- [redacted]

[7] Ibid, page 22.
[8] See e.g. the Guardian https://www.theguardian.com/world/2022/jun/14/nso-group-pegasus-us-l3harris
[9] See https://gizmodo.com/white-house-nso-group-pegasus-l3harris-acquisition-isra-1849063061