UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY, Plaintiff, v. CENTRAL INTELLIGENCE AGENCY, DEPARTMENT OF THE ARMY, DEPARTMENT OF JUSTICE, NATIONAL SECURITY AGENCY, and OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, Defendants.	Civil Action No. 1:22-cv-01542

COMPLAINT FOR INJUNCTIVE RELIEF

INTRODUCTION

1. This lawsuit under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, seeks the expedited processing and immediate release of records concerning "spyware"—a form of digital surveillance software that can be used to surreptitiously gain access to, and control of, smartphones—including spyware developed or provided to U.S. government agencies by NSO Group.[1]

2. Smartphones keep detailed logs of nearly every aspect of our lives: they store our private thoughts, document our personal exchanges with friends, capture our family photographs, and record videos of our celebrations. They connect us to our religious and recreational

[1] As used in this Complaint, "NSO Group" includes NSO Group Technologies Ltd. and its affiliates, including but not limited to Q Cyber Technologies Ltd. and Westbridge Technologies, Inc.

communities. They transmit correspondence to colleagues and clients. They catalogue our contacts, calendar our commitments, and trace our curiosities. They track our physical location at every step. For some, they are indispensable tools of public service. Journalists rely on smartphones to gather and report news of urgent public interest. Dissidents and activists rely on smartphones to rally against repressive regimes.

3. NSO Group is a foreign company that develops and sells spyware to government customers. The company's signature spyware product, called "Pegasus," can reportedly infect smartphones undetected to give the spyware's operators essentially full control of the device, which can be used to extract contact lists, calendar entries, text messages, emails, search histories, and GPS locations. Moreover, Pegasus can enable the smartphone's microphone to record surrounding sounds, turning the device into a wandering wiretap, and it can use the smartphone's camera to capture snapshots, enabling real-time visual surveillance. Pegasus—and spyware tools like it—offer previously unimaginable access to the lives of others.

4. Multiple agencies within the U.S. government appear to have communicated or even contracted with NSO Group. According to recent, confirmed reports, the Federal Bureau of Investigation purchased and tested a version of Pegasus in 2019. The Central Intelligence Agency reportedly assisted the government of Djibouti in acquiring Pegasus. And employees of the Army, the Drug Enforcement Administration, and the Secret Service have reportedly communicated with NSO Group or its U.S. affiliate, Westbridge Technologies, about the possible purchase of Pegasus or similar spyware tools. Meanwhile, the Department of Justice has reportedly considered whether the use of such tools would violate U.S. law.

5. To help the public better understand the U.S. government's consideration of the use of spyware and the extent of government's contacts, and possible contracts, with NSO Group,

Plaintiff, the Knight First Amendment Institute at Columbia University ("Plaintiff" or the "Knight Institute"), submitted identical FOIA requests ("the Request") to Defendants and the Secret Service on February 2 and 3, 2022. Plaintiff sought expedited processing to ensure timely public access to records responsive to the Request.

6. Plaintiff has commenced this action because Defendants have denied or constructively denied Plaintiff's request for expedited processing and have failed to process and release records responsive to the Request within the timeline mandated by FOIA. Plaintiff seeks the injunctive relief necessary to ensure Defendants' compliance with FOIA's requirements.

JURISDICTION AND VENUE

7. This Court has jurisdiction over this action pursuant to 5 U.S.C. § 552(a)(4)(B) and 28 U.S.C. § 1331.

8. Venue is proper in this district pursuant to 5 U.S.C. § 552(a)(4)(B).

PARTIES

9. The Knight First Amendment Institute at Columbia University is a New York not-for-profit corporation based at Columbia University that works to preserve and expand the freedoms of speech and the press through strategic litigation, research, and public education. Public education is essential to the Knight Institute's mission. Obtaining information about government activity, analyzing that information, and publishing and disseminating it to the press and public are among the core activities the Knight Institute was established to conduct. The Knight Institute is a "person" within the meaning of 5 U.S.C. § 551(2).

10. Defendant Central Intelligence Agency ("CIA") is an "agency" within the meaning of 5 U.S.C. § 552(f). The CIA has possession and control over requested records.

11. Defendant Department of the Army ("Army") is a component of the Department of Defense and an "agency" within the meaning of 5 U.S.C. § 552(f). The Army has possession and control over requested records.

12. Defendant Department of Justice ("DOJ") is a department of the executive branch of the U.S. government and is an "agency" within the meaning of 5 U.S.C. § 552(f). The DOJ and its components the Drug Enforcement Administration ("DEA"), the Federal Bureau of Investigation ("FBI"), the Criminal Division ("DOJ Crim"), the National Security Division ("NSD"), the Office of Information Policy ("OIP"), and the Office of Legal Counsel ("OLC"), have possession and control over requested records.

13. Defendant National Security Agency ("NSA") is an "agency" within the meaning of 5 U.S.C. § 552(f). The NSA has possession and control over requested records.

14. Defendant Office of the Director of National Intelligence ("ODNI") is an "agency" within the meaning of 5 U.S.C. § 552(f). The ODNI has possession and control over requested records.

FACTUAL ALLEGATIONS

Background

15. NSO Group develops and markets Pegasus and similar spyware products. As noted above, Pegasus can be installed on a user's smartphone without that user's awareness (i.e., through a "zero-click" attack). It then gives the Pegasus operator access to, and significant control of, the device. Marketing materials for the U.S. version of Pegasus, called "Phantom," elaborate on these capabilities: Phantom can be installed "remotely . . . with either minimal or no engagement from the target" and with "no third party involvement from cellphone carriers"; it can "[c]overtly gather all data on a target smartphone," including "contact list, text messages, call history, emails, instant messaging, call interception, room wiretap, camera snapshots, calendar, GPS tracking, browser

history and app data such as Skype and Facebook"; and it can circumvent security hurdles, leaving "no traces whatsoever on the [target] device."[2]

16. NSO Group has apparently sold Pegasus to more than forty governments around the world, several of which have reportedly used Pegasus to persecute journalists, dissidents, human rights advocates, and activists. For example, Saudi authorities allegedly used Pegasus to target Canada-based activist Omar Abdulaziz—a friend of journalist Jamal Khashoggi, whom Saudi agents brutally murdered in 2018—as well as another Saudi dissident, an Amnesty International researcher, and an American *New York Times* journalist who had reported on the country. Authorities in the United Arab Emirates apparently used Pegasus to target human rights activist Ahmed Mansoor, who was subsequently robbed, beaten, and imprisoned for comments he posted on Facebook and Twitter. Hungarian Prime Minister Viktor Orbán has allegedly used Pegasus to target journalists, social activists, and members of his political opposition. Mexican officials have allegedly used Pegasus to target journalists and lawyers investigating corruption and human rights abuses. And in El Salvador, authorities allegedly used Pegasus to target at least thirty-five journalists and members of civil society who reported on or challenged President Nayib Bukele's administration.

17. The Biden Administration has recognized the threat that Pegasus poses to human rights. In November 2021, the Commerce Department added NSO Group to the "Entity List" based on evidence that it had "supplied spyware to foreign governments that used this tool to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers," as well as to target "dissidents, journalists and activists outside of their sovereign borders

[2] Westbridge, *Phantom*, https://s3.documentcloud.org/documents/6888574/Westbridge-NSO-Group-Brochure-for-Phantom.pdf [https://perma.cc/XZV2-PYFW].

to silence dissent."[3] The Commerce Department described the designation of NSO Group as part of a broader effort to "stem the proliferation of digital tools used for repression" and to "improv[e] citizens' digital security, combat[] cyber threats, and mitigat[e] unlawful surveillance."[4]

18. Recent reporting, however, has revealed that the U.S. government itself considered using spyware like Pegasus, even contracting with NSO Group to test it. In 2019, the FBI admittedly purchased and tested a version of Pegasus.[5] Army, DEA, and Secret Service employees have also reportedly communicated with NSO Group or its U.S. affiliate about the possible purchase of Pegasus or similar spyware tools. And the DOJ has reportedly considered whether the use of such tools would violate U.S. law.

19. Because of the scope and sensitivity of the information accessible through smartphones, surreptitious government surveillance of them poses grave threats to the freedoms of speech, association, and the press, as well as to individual privacy and to democracy. Given these concerns, and in light of recent reporting, the Knight Institute submitted the Request at issue here.

The FOIA Request

20. On February 2 and 3, 2022, the Knight Institute submitted the Request to Defendants and the Secret Service, seeking the following records:[6]

---

[3] Press Release, U.S. Dep't of Com., Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities (Nov. 3, 2021), https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list [https://perma.cc/CD5C-3K47].

[4] *Id.*

[5] *See* Ellen Nakashima, *FBI Acknowledges It Tested NSO Group's Spyware*, Wash. Post (Feb. 2, 2022), https://www.washingtonpost.com/technology/2022/02/02/pegasus-fbi-nso-test/ [https://perma.cc/YVL6-EGKD].

[6] A true and correct copy of the Request is attached hereto as Exhibit A.

a. All records concerning spyware developed or provided by NSO Group, including but not limited to: all solicitation materials, including requests for proposals and responses to requests for proposals; all marketing materials, including press releases, pamphlets, brochures, PowerPoint presentations, and video presentations; all contracts, including formal or informal agreements and memoranda of understanding; all testing materials, including records relating to any pilot programs; all training materials, including instruction manuals, tutorials, PowerPoint presentations, and video presentations; and all communications, including communications with any employees or other representatives of NSO Group.

b. All policies, procedures, or guidelines regarding the use of spyware, including but not limited to spyware developed or provided by NSO Group.

c. All policy or legal memoranda addressing spyware, including but not limited to spyware developed or provided by NSO Group.

21. The Knight Institute requested expedited processing of the Request on the ground that it is an organization "primarily engaged in disseminating information" and there is a "compelling need" for the records sought because they contain information "urgent[ly]" needed to "inform the public concerning actual or alleged Federal Government Activity." 5 U.S.C. § 552(a)(6)(E)(v)(II).

22. The Knight Institute requested a waiver of document search, review, and duplication fees on three independent grounds: (a) that disclosure of the requested records is in the public interest and is "likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester," *id.* § 552(a)(4)(A)(iii); (b) that the Knight Institute is a "representative of the news media" within the meaning of FOIA and the records are not sought for commercial use, *id.* § 552(a)(4)(A)(ii)(II); and (c) that the Knight Institute is an "educational . . . institution" whose purposes include "scholarly . . . research" and the records are not sought for commercial use, *id.* § 552(a)(4)(A)(ii)(II).

Agency Responses

23. By automated emails dated February 2, 2022, the Army, the OLC, and the FBI each confirmed receipt of the Request on that date. To date, the Army, the OLC, and the FBI have not responded to the Knight Institute's requests for expedited processing and a fee waiver.

24. By letter dated February 7, 2022, the OIP acknowledged receipt of the Request on February 2, 2022; assigned the Request reference number FOIA-2022-00723; denied the Knight Institute's request for expedited processing; and stated that a decision regarding the Knight Institute's request for a fee waiver would be made at a later time. A true and correct copy of the letter is attached hereto as Exhibit B.

25. By letter dated February 9, 2022, the Secret Service acknowledged receipt of the Request on February 8, 2022; assigned the Request reference number 20220207; granted the Knight Institute's request for expedited processing; and stated that the Knight Institute's request for a fee waiver "will be held in abeyance pending the quantification of responsive records." A true and correct copy of the letter is attached hereto as Exhibit C.

26. By letter dated February 10, 2022, the DEA acknowledged receipt of the Request; assigned it reference number 22-00352-F; and denied the Knight Institute's request for expedited processing. A true and correct copy of the letter is attached hereto as Exhibit D. To date, the DEA has not responded to the Knight Institute's request for a fee waiver.

27. By letter dated February 11, 2022, DOJ Crim acknowledged receipt of the Request; assigned it reference number CRM-301699723; and denied the Knight Institute's request for expedited processing. A true and correct copy of the letter is attached hereto as Exhibit E. To date, DOJ Crim has not responded to the Knight Institute's request for a fee waiver.

28. By letter received on February 14, 2022, the ODNI acknowledged receipt of the Request on February 4, 2022; assigned it reference number DF-2022-00139; denied the Knight

Institute's request for expedited processing; and granted the Knight Institute's request for a fee waiver. A true and correct copy of the letter is attached hereto as Exhibit F.

29. By letter dated February 17, 2022, the NSA acknowledged receipt of the Request on February 9, 2022; assigned it reference number 113663; and denied the Knight Institute's request for expedited processing. A true and correct copy of the letter is attached hereto as Exhibit G. To date, the NSA has not responded to the Knight Institute's request for a fee waiver.

30. To date, the CIA and the NSD have not acknowledged the Request or responded to the Knight Institute's requests for expedited processing and a fee waiver.

31. To date, Defendants have not released any records responsive to the Request or adequately explained their failure to do so.

CAUSES OF ACTION

1. Defendants' failure to grant Plaintiff's request for expedited processing violates FOIA, 5 U.S.C. § 552(a)(6)(E), and Defendants' corresponding regulations.

2. Defendants' failure to process the Request as soon as practicable violates FOIA, 5 U.S.C. § 552(a)(6)(E)(iii), and Defendants' corresponding regulations.

3. Defendants' failure to make records responsive to the Request promptly available violates FOIA, 5 U.S.C. § 552(a)(3)(A), (a)(6)(A), and Defendants' corresponding regulations.

4. With the exception of the ODNI, Defendants' failure to grant Plaintiff's request for a waiver of search, review, and duplication fees violates FOIA, 5 U.S.C. § 552(a)(4)(A)(ii)(II), (iii), and Defendants' corresponding regulations.

PRAYER FOR RELIEF

Plaintiff respectfully requests that this Court:

A. Order Defendants to conduct a thorough search for records responsive to Plaintiff's request;

B. Order Defendants to immediately process and release any responsive records;

C. Award Plaintiff its reasonable costs and attorneys' fees incurred in this action; and

D. Grant such other and further relief as the Court may deem just and proper.

Respectfully submitted,

/s/ *Carrie DeCell*

Carrie DeCell
Jameel Jaffer
Evan Welber Falcón
Knight First Amendment Institute
at Columbia University
475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
carrie.decell@knightcolumbia.org

Counsel for Plaintiff

February 24, 2022