EXHIBIT A



KNIGHT
FIRST AMENDMENT
INSTITUTE at
COLUMBIA UNIVERSITY

475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
info@knightcolumbia.org

February 2, 2022

VIA ONLINE SUBMISSION

Douglas Hibbard
Chief, Initial Request Staff
Office of Information Policy
Department of Justice
6th Floor
441 G Street, N.W.
Washington, D.C. 20530
https://doj-foia.entellitrak.com/etk-doj-foia-prod/login.request.do

Federal Bureau of Investigation
Attn: Initial Processing Operations Unit
Record/Information Dissemination Section
200 Constitution Drive
Winchester, VA 22602
https://efoia.fbi.gov/

Drug Enforcement Administration
Freedom of Information and Records Management Section
Attn: Intake Unit
8701 Morrissette Drive
Springfield, VA 22152
https://ifa.dea.gov/foia/

VIA EMAIL

Melissa Golden
Lead Paralegal and FOIA Specialist
Department of Justice
Room 5511, 950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530-0001
usdoj-officeoflegalcounsel@usdoj.gov

Arnetta Mallory
Government Information Specialist
National Security Division
Department of Justice
3 Constitution Square
175 N Street, N.E., 12th Floor
Washington, D.C. 20530-0001
nsdfoia@usdoj.gov

Amanda Marchand Jones, Chief
FOIA/PA Unit
Criminal Division
Department of Justice
Suite 1127
1301 New York Avenue, N.W.
Washington, DC 20530-0001
crm.foia@usdoj.gov

U.S. Army Freedom of Information Act Office
Records Management Directorate
9301 Chapek Road, Building 1458
Fort Belvoir, VA 22060-5605
usarmy.belvoir.hqda-oaa-ahs.mbx.rmda-foia@army.mil

Gregory Koch
Director, Information Management Office
ATTN: FOIA/PA
Office of the Director of National Intelligence
Washington, D.C. 20511
dni-foia@dni.gov

VIA FEDEX

FOIA/PA Mail Referral Unit
Department of Justice
Room 115
LOC Building
Washington, D.C. 20530-0001

Information and Privacy Coordinator
Central Intelligence Agency
Washington, D.C. 20505

U.S. Secret Service FOIA Office
245 Murray Lane Building T-5
Washington, D.C. 20223

National Security Agency
Attn: FOIA/PA Office
9800 Savage Road, Suite 6932
Fort George G. Meade, MD 20755-6932

Re: Freedom of Information Act Request
Expedited Processing Requested

To whom it may concern,

The Knight First Amendment Institute at Columbia University ("Knight Institute" or "Institute")[1] submits this request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, for records concerning "spyware," a form of digital surveillance technology,[2] developed or provided by NSO Group.[3]

I. Background

NSO Group is a company that develops and sells spyware to governments around the world—including governments that have engaged in serious human rights abuses. NSO Group'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.[4] Moreover, Pegasus can use the smartphone's microphone to record surrounding sounds, turning the device into a wandering wiretap, and use the smartphone's camera to capture snapshots, enabling real-time video surveillance.[5] Thus, Pegasus—and spyware tools like it—offer previously unimaginable access to the lives of others.[6]

---

[1] The Knight First Amendment Institute 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.

[2] As used in this Request, "spyware" refers to a type of malicious software that can be installed on a smartphone without the smartphone user's consent and that can gain access to, and/or control of, the device.

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

[4] Nicole Perlroth, *How Spy Tech Firms Let Governments See Everything on a Smartphone*, N.Y. Times (Sept. 2, 2016), https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html; *see also* Ronen Bergman & Mark Mazzetti, *The Battle for the World's Most Powerful Cyberweapon*, N.Y. Times (Jan. 28, 2022), https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.

[5] Perlroth, *supra* note 4.

[6] Marketing materials for the U.S. version of Pegasus, called "Phantom," describe similar capabilities. According to a Westbridge Technologies brochure, Phantom can be installed "remotely . . . with either minimal or no engagement from the target" and

Predictably, authoritarian governments have used Pegasus to pursue and persecute their critics. NSO Group has reportedly sold its spyware to Hungary, India, Mexico, Panama, Poland, Saudi Arabia, and the United Arab Emirates ("UAE"),[7] though the list of government customers is likely much longer.[8] Hungarian Prime Minister Viktor Orbán has allegedly used Pegasus against social activists, journalists, and members of his political opposition.[9] Mexican officials have allegedly used Pegasus to target journalists and lawyers investigating corruption and human rights abuses.[10] Saudi authorities allegedly used Pegasus to target Canada-based activist Omar Abdulaziz[11] (a friend of journalist Jamal Khashoggi, whom Saudi agents brutally murdered in 2018), as well as another Saudi dissident, an Amnesty International researcher,[12] and an American New York Times journalist who had reported on the country.[13] UAE human rights activist Ahmed Mansoor was the target of a Pegasus attack and subsequently robbed, beaten, and imprisoned for posts he made on Facebook

---

with "[n]o cooperation from a third party," such as AT&T, Verizon, Apple, or Google; 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 overcome encryption and other security hurdles, leaving "no traces whatsoever" on the target device. Westbridge/NSO Group Brochure for Phantom, https://www.documentcloud.org/documents/6888574-Westbridge-NSO-Group-Brochure-for-Phantom; Joseph Cox, *NSO Group Pitched Phone Hacking Tech to American Police*, VICE (May 12, 2020), https://www.vice.com/en/article/8899nz/nso-group-pitched-phone-hacking-tech-american-police.

[7] Bergman & Mazzetti, *supra* note 4.

[8] Bill Marczak et al., *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, Citizen Lab (Sept. 18, 2018), https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

[9] Bergman & Mazzetti, *supra* note 4; Keno Verseck, *Pegasus Scandal: In Hungary, Journalists Sue State Over Spyware*, Deutsche Welle (Jan. 29, 2022), https://www.dw.com/en/pegasus-scandal-in-hungary-journalists-sue-state-over-spyware/a-60598885.

[10] John Scott-Railton et al., *Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware*, Citizen Lab (June 19, 2017), https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/.

[11] Bill Marczak et al., *The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil*, Citizen Lab (Oct. 1, 2018), https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/.

[12] *Amnesty International Among Targets of NSO-powered Campaign*, Amnesty Int'l (Aug. 1, 2018, 1:19 PM), https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/.

[13] Bill Marczak et al., *Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator*, Citizen Lab (Jan. 28, 2020), https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/.

and Twitter.[14] And in El Salvador, at least thirty-five journalists and members of civil society allegedly had their phones infected with Pegasus while reporting on sensitive issues involving President Bukele's administration.[15]

The Biden Administration has recognized the threat Pegasus poses to human rights. In November 2021, the U.S. Commerce Department added NSO Group to the "Entity List"[16] 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 to silence dissent."[17] The Commerce Department framed the blacklisting 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."[18]

Nonetheless, recent reporting suggests that multiple agencies within the U.S. government have communicated and even contracted with NSO Group. The Federal Bureau of Investigation ("FBI") reportedly purchased and tested a version of Pegasus in 2019.[19] Employees of the Central Intelligence Agency ("CIA"), the Drug Enforcement Agency ("DEA"), the U.S. Secret Service, and the U.S. Army have also reportedly communicated with NSO Group or its U.S. affiliate, Westbridge Technologies, about the possible purchase of Pegasus or similar spyware tools.[20] And the U.S. Department of Justice ("DOJ") has reportedly considered whether the use of such tools would violate U.S. law.[21]

---

[14] Bergman & Mazzetti, *supra* note 4; Bill Marczak & John Scott-Railton, *The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against a UAE Human Rights Defender*, Citizen Lab (Aug. 24, 2016), https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

[15] John Scott-Railton et al., *Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware*, Citizen Lab (Jan. 12, 2022), https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/.

[16] Addition of Certain Entities to the Entity List, 86 Fed. Reg. 60,759, 60,759 (Nov. 4, 2021), https://www.govinfo.gov/content/pkg/FR-2021-11-04/pdf/2021-24123.pdf.

[17] 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.

[18] *Id.*

[19] Bergman & Mazzetti, *supra* note 4.

[20] *Id.*; *see also* Joseph Cox, *NSO Group Pitched Its Spyware to the Secret Service*, VICE (July 23, 2020), https://www.vice.com/en/article/m7jp43/nso-group-pitched-its-spyware-to-the-secret-service; Joseph Cox, *The DEA Didn't Buy Malware From Israel's Controversial NSO Group Because It Was Too Expensive*, VICE (Sept. 11, 2019), https://www.vice.com/en/article/3kxk9j/dea-didnt-buy-malware-nso-group-too-expensive.

[21] Bergman & Mazzetti, *supra* note 4.

Because of the scope and sensitivity of the information accessible through smartphones, surreptitious government surveillance of them poses grave threats to 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 seeks to inform the public about extent of the U.S. government's contacts, and possible contracts, with NSO Group.

II. Records requested

The Knight Institute seeks the following records:

1. All records concerning spyware developed or provided by NSO Group, including but not limited to:

    a. All solicitation materials, including requests for proposals and responses to requests for proposals;

    b. All marketing materials, including press releases, pamphlets, brochures, PowerPoint presentations, and video presentations;

    c. All contracts, including formal or informal agreements and memoranda of understanding;

    d. All testing materials, including records relating to any pilot programs;

    e. All training materials, including instruction manuals, tutorials, PowerPoint presentations, and video presentations; and

    f. All communications, including communications with any employees or other representatives of NSO Group.

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

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

We ask that you disclose all segregable portions of otherwise exempt records. *See* 5 U.S.C. § 552(b). We also ask that you provide responsive electronic records in their native file format. *See* 5 U.S.C. § 552(a)(3)(B). If the records are not producible in that format, please provide the records electronically in a text-searchable, static-image format (*e.g.*, PDF), in the best image quality in the agency's possession, and in separate, Bates-stamped files.

III. Application for expedited processing

We request expedited processing pursuant to 5 U.S.C. § 552(a)(6)(E). There is a "compelling need" for the records sought because the information they contain is "urgent[ly]" needed by an organization primarily engaged in

disseminating information "to inform the public about actual or alleged Federal Government activity." 5 U.S.C. § 552(a)(6)(E)(v)(II).

A. The Knight Institute is primarily engaged in disseminating information in order to inform the public about actual or alleged government activity.

The Knight First Amendment Institute was established at Columbia University to defend and strengthen the freedoms of speech and the press in the digital age. Research and public education are essential to the Institute's mission.[22] Obtaining information about government activity, analyzing that information, and publishing and disseminating it to the press and public are among the core activities the Institute performs. *See ACLU v. DOJ*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004) (finding non-profit public interest group that "gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw material into a distinct work, and distributes that work to an audience" to be "primarily engaged in disseminating information" (quoting *Elec. Privacy Info. Ctr. v. DOD*, 241 F. Supp. 2d 5, 11 (D.D.C. 2003))).[23]

For example, the Institute disseminates information about government activity—including information about government activity obtained under FOIA—through a variety of means, including its website,[24] Twitter account,[25] press releases,[26] blog posts,[27] op-eds,[28] and regular engagement with the press.[29] The Institute also publishes records obtained through FOIA in

---

[22] *See About the Knight Institute*, Knight First Amendment Inst., https://perma.cc/8UYT-RUUZ.

[23] *See id.* (explaining that a priority of the Knight Institute's work is "ensuring access to information necessary for self-government").

[24] *See* Knight First Amendment Inst., https://knightcolumbia.org.

[25] *See* Knight First Amendment Inst. (@knightcolumbia), Twitter, https://twitter.com/knightcolumbia (Knight Institute account with over 13,000 followers).

[26] *See, e.g.*, *Knight Institute Calls on DOJ's Executive Office for Immigration Review to Suspend Policy Silencing Immigration Judges*, (Jan. 6, 2020), https://perma.cc/GT69-A8SC (describing an agency policy obtained through FOIA).

[27] *See, e.g.*, Anna Diakun, *Redactions in CDC Communications Policies Leave Key Questions Unanswered*, Knight First Amendment Inst. (June 12, 2020), https://perma.cc/GQX3-WKCN; Stephanie Krent, *Recently Released OLC Opinions from 1974 Shed Light on Current Legal Debates*, Knight First Amendment Inst. (May 18, 2020), https://perma.cc/34N2-UAQ3.

[28] *See, e.g.*, Anna Diakun, *Biden Promised Transparency. Has He Delivered?*, CNN (Jan. 21, 2022), https://perma.cc/J2XX-8HDQ; Anna Diakun & Trevor Timm, *For the Biden Administration, Who Counts as News Media?*, Colum. Journalism Rev. (June 9, 2021), https://perma.cc/PR7T-75FQ; Jameel Jaffer & Ramya Krishnan, *We May Never See John Bolton's Book*, N.Y. Times (Jan. 30, 2020), https://perma.cc/HGY9-638T.

[29] *See, e.g.*, Nilay Patel, *Can We Regulate Social Media Without Breaking the First Amendment?*, The Verge (Dec. 16, 2021), https://perma.cc/JKC8-VDBV (discussing Knight Institute amicus brief in lawsuit challenging Florida social media regulations); Jessica Jerreat, *CDC Media Guidance Blacklists VOA Interview Requests,* VOA News (June 14, 2020), https://perma.cc/2KVX-WGYR (reporting on CDC email obtained by

"Reading Rooms" on the Institute's website, which allow the public to search, filter, and view the records.[30]

Through its research program, the Institute has published multiple influential essay series, including one focused on reimagining the First Amendment in the digital age, one addressing the technology giants' power to shape public discourse, and another on the relationship between big data and self-government.[31] In addition, the Institute has convened four research symposia—drawing practitioners, lawyers, academics, and journalists—to debate, discuss, and reflect on key issues in First Amendment doctrine and free speech theory. The first, "A First Amendment for All? Free Expression in an Age of Inequality," was held in March 2018;[32] the second, "The Tech Giants, Monopoly Power, and Public Discourse," was held in November 2019;[33] the third, "Data and Democracy," was held virtually in October 2020;[34] and the fourth, "Reimagine the Internet," was held virtually in May 2021.[35]

B. *The records sought are urgently needed to inform the public about actual or alleged government activity.*

The records sought are urgently needed to inform the public about actual or alleged government activity. *See* 5 U.S.C. § 552(a)(6)(E)(v)(II). Specifically, the requested records relate to the U.S. government's contacts, and possible contracts, with NSO Group.

As detailed above, spyware like Pegasus is perhaps the most invasive digital surveillance technology developed to date. And it has already been used

---

the Knight Institute under FOIA); Ellen Nakashima, *U.S. Spy Agencies Sued for Records on Whether They Warned Khashoggi of Impending Threat of Harm*, Wash. Post (Nov. 20, 2018, 8:57 PM), https://perma.cc/C6CW-TSDA (describing FOIA lawsuits); Cora Currier, *Government Can Spy on Journalists in the U.S. Using Invasive Foreign Intelligence Process*, Intercept (Sept. 17, 2018), https://perma.cc/YQ7F-NZ5R (reporting on DOJ rules obtained by the Knight Institute under FOIA); Charlie Savage, *U.S. Government Went Through These People's Phones at the Border. Read Their Stories.*, N.Y. Times (Dec. 22, 2017), https://perma.cc/H7P2-RK2T (describing and publishing several hundred complaints obtained by the Knight Institute about warrantless searches of electronic devices at the border).

[30] *See*, *e.g.*, *The OLC's Opinions*, Knight First Amendment Inst., https://knightcolumbia.org/reading-room/olc-opinions; *Ideological Screening at the Border*, Knight First Amendment Inst., https://knightcolumbia.org/reading-room/ideological-screening-at-the-border.

[31] *See Research*, Knight First Amendment Inst., https://perma.cc/TVD9-39RK.

[32] *A First Amendment for All? Free Expression in an Age of Inequality*, Knight First Amendment Inst. (Mar. 23, 2018, 8:30 AM); https://perma.cc/DM59-74KG.

[33] *Leading Legal Scholars, Economists, and Technologists to Headline Fall Symposium*, Knight First Amendment Inst. (Jan. 8, 2020), https://perma.cc./86DE-TPQS.

[34] *Data and Democracy*, Knight First Amendment Inst., https://perma.cc/2ARV-CUTY.

[35] *Reimagine the Internet*, Knight First Amendment Inst., https://perma.cc/7CNP-5F2S.

countless times to surveil and silence government critics, as well as journalists and activists, around the world. The Biden Administration itself has characterized spyware as a "digital tool[] used for repression."[36] Yet agencies within the U.S. government have reportedly communicated with providers of this tool over the past several years to explore its possible use. This past week, the New York Times reported that the FBI had contracted with NSO Group to purchase and test this tool.[37] And just today, the FBI acknowledged as much.[38]

Disclosure of the requested records will shed light on the extent to which the U.S. government has considered the use of spyware that threatens significant intrusions into Americans' privacy and significant burdens on the exercise of their First Amendment rights.

For these reasons, the Knight Institute is entitled to expedited processing.

IV. Application for waiver or limitation of fees

The Knight Institute requests a waiver of document search, review, and duplication fees on the grounds that disclosure of the requested records is in the public interest and that disclosure is "likely to contribute significantly to the public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester." 5 U.S.C. § 552(a)(4)(A)(iii).

For the reasons explained above, disclosure of the records would be in the public interest. Moreover, disclosure would not further the Knight Institute's commercial interest. The Institute will make any information disclosed available to the public at no cost. Thus, a fee waiver would fulfill Congress's legislative intent in amending FOIA to ensure "that it be liberally construed in favor of waivers for noncommercial requesters." *See Judicial Watch, Inc. v. Rossotti*, 326 F.3d 1309, 1312 (D.C. Cir. 2003).

The Knight Institute also requests a waiver of search and review fees on the grounds that it qualifies as an "educational . . . institution" whose purposes include "scholarly . . . research" and the records are not sought for commercial use. 5 U.S.C. § 552(a)(4)(A)(ii)(II). The Institute has a substantial educational mission. Situated within a prominent academic research university, the Institute performs scholarly research on the application of the First Amendment in the digital era. As described above, the Institute's research program brings together academics and practitioners of different disciplines to study contemporary First Amendment issues and offer informed, non-partisan commentary and solutions. It publishes that commentary in many forms, including in scholarly publications and in short-form essays.

---

[36] Press Release, Dep't of Com., *supra* note 17.

[37] Bergman & Mazzetti, *supra* note 4.

[38] 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/.

The Knight Institute also requests a waiver of search and review fees on the grounds that it is a "representative[] of the news media" within the meaning of FOIA and the records are not sought for commercial use. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

The Institute meets the statutory definition of a "representative of the news media" because it is an "entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience." 5 U.S.C. § 552(a)(4)(A)(ii); *see also Nat'l Sec. Archive v. DOD*, 880 F.2d 1381, 1387 (D.C. Cir. 1989) (finding that an organization that gathers information, exercises editorial discretion in selecting and organizing documents, "devises indices and finding aids," and "distributes the resulting work to the public" is a "representative of the news media" for purposes of the FOIA); *accord Serv. Women's Action Network v. DOD*, 888 F. Supp. 2d 282 (D. Conn. 2012); *ACLU of Wash. v. DOJ*, No. C09-0642RSL, 2011 WL 887731, at *10 (W.D. Wash. Mar. 10, 2011); *ACLU*, 321 F. Supp. 2d at 30 n.5. Courts have found other non-profit organizations, whose mission of research and public education is similar to that of the Knight Institute, to be "representatives of the news media." *See, e.g.*, *Cause of Action v. IRS*, No. 13-0920, 2015 WL 5120863 (D.C. Cir. Aug. 28, 2015); *Elec. Privacy Info. Ctr.*, 241 F. Supp. 2d at 10–15 (finding non-profit group that disseminated an electronic newsletter and published books was a "representative of the news media" for purposes of the FOIA); *Nat'l Sec. Archive*, 880 F.2d at 1387; *Judicial Watch, Inc. v. DOJ*, 133 F. Supp. 2d 52, 53–54 (D.D.C. 2000) (finding Judicial Watch, self-described as a "public interest law firm," a news media requester).

For these reasons, the Knight Institute is entitled to a fee waiver.

* * *

Thank you for your attention to our request. We would be happy to discuss its terms with you over the phone or via email to clarify any aspect of it.

/s/ *Carrie DeCell*
Carrie DeCell
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