epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

VIA EMAIL

December 21, 2022

Drug Enforcement Administration
Freedom of Information and Privacy Act Unit
Attn: Intake Sub-Unit
8701 Morrissette Drive
Springfield, Virginia 22152
DEA.FOIA@dea.gov

Dear DEA FOIA Officer:

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. §552(a)(3), and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the United States Drug Enforcement Administration ("DEA") of the United States Department of Justice ("DOJ").

EPIC requests records related to the DEA's communications with spyware makers NSO Group and Paragon. In particular, EPIC seeks any records of communications between the DEA and NSO Group or Paragon about their spyware tools—Pegasus (NSO Group) and Graphite (Paragon)—that grant attackers virtually unfettered access to targets' smartphone data.

Documents Requested

EPIC requests disclosure of the following documents:

1. All emails, communications, and memoranda:
    a. shared between the DEA and any representatives from Paragon Solutions Ltd. ("Paragon"); Battery Ventures; NSO Group Technologies; Westbridge Technology, Inc. (or "Westbridge Technologies"); Q Cyber Technologies; L.E.G.D. Company; Lavie Management Co.; OSY Holdings; or OSY Technologies SARL;
    b. or shared between the DEA and any of the following individuals: Ehud Schneorson; Ehud Barak; Idan Nurick; Igor Bogudlov; Liad Avraham; Omri Lavie, Niv Carmi, Shalev Hulio, Chaim Gelfand, Terrence ("Terry") Divittorio, or Joshua ("Josh") Shaner;
    c. shared between the DEA and any email address ending with @battery.com; @nsogroup.com, @qtechnologies.com, or @westbrg.com;
    d. or referencing Paragon, Graphite, Pegasus, Phantom, Q Suite, or Chrysaor;
2. Any contracts or agreements between the DEA and Paragon Solutions Ltd. ("Paragon"); Battery Ventures; NSO Group Technologies; Westbridge Technology, Inc. (or

"Westbridge Technologies"); Q Cyber Technologies; L.E.G.D. Company; Lavie Management Co.; OSY Holdings; or OSY Technologies SARL;
3. All Paragon or Battery Ventures presentations and sales materials or presentations and sales materials mentioning Paragon, Graphite, NSO Group, Westbridge, Pegasus, Phantom, Chrysaor, or Q Suite.

Background

Over the last several years, media organizations have published a series of investigations into the use of hacking technology on the phones of over a thousand political figures, journalists, and businesspeople.[1] Scandals involving spyware have erupted throughout the world, including most recently in the European Union.[2]

Much of this media coverage has focused on an Israeli corporation called NSO Group, which produces a spyware tool called Pegasus (also known by other names including "Phantom").[3] Pegasus works by installing itself onto an iPhone or Android cellular phone through software vulnerabilities or malicious links.[4] Upon installation, the spyware can access virtually any data from a phone, including SMS and WhatsApp messages, emails, media, location data, contacts, the phone's microphone, and the phone's camera. Through Pegasus, an attacker can also gain access to administrative privileges on a smartphone—doing "more than what the owner of the device can do."[5]

Recent media scrutiny of U.S. government deployment of spyware has also highlighted ties between the DEA and several spyware makers, including NSO Group and Paragon, another Israeli corporation.[6] Media reports indicate that the DEA has an existing contract with Paragon for its

[1] *See About the Pegasus Project*, FORBIDDEN STORIES, https://forbiddenstories.org/about-the-pegasus-project.
[2] *See* Morgan Meaker, *Spyware Scandals Are Ripping Through Europe*, WIRED (Aug. 15, 2022), https://www.wired.com/story/europe-spyware-scandals-greece/.
[3] NSO Group has had numerous parent companies, owners, subsidiaries, and affiliated companies, including Westbridge Technology, Inc.; OSY Technologies SARL; OSY Holdings Ltd.; Q Cyber Technologies; Triangle Holdings SA; Square 2 SARL; L.E.G.D. Company; Novalpina Capital Group SARL; Novalpina Capital Partners I GP SARL; Novalpina Capital Partners I SCSp. *See* OPERATING FROM THE SHADOWS: INSIDE NSO GROUP'S CORPORATE STRUCTURE, AMNESTY INT'L, PRIVACY INT'L, & SOMO 31–33, 38–44, 49 (2021), https://www.somo.nl/wp-content/uploads/2021/05/Operating-from-the-Shadows.pdf. Westbridge, which is NSO Group's U.S. arm, has pitched Pegasus as "Phantom" in demonstrations to U.S. agencies. *See* William Turton, *Israel's NSO Group Linked to Hacking Tool Pitched to U.S. Police*, BLOOMBERG (May 12, 2020), https://www.bloomberg.com/news/articles/2020-05-12/israel-snso-group-linked-to-hacking-tool-pitched-to-u-s-police. "Chrysaor" is reportedly an additional variant of Pegasus. *See* Tom Spring, *Android Variant of Notorious Pegasus Spyware Found*, THREATPOST (Apr. 4, 2017), https://threatpost.com/androidvariant-of-notorious-pegasus-spyware-found/124781.
[4] *See* David Pegg & Sam Cutler, *What Is Pegasus Spyware and How Does It Hack Phones?*, GUARDIAN (July 18, 2021), https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones.
[5] *Id.*
[6] Paragon was reportedly founded in 2019 by Ehud Schneorson, a former commander of Unit 8200, Israel's equivalent of the National Security Agency, but beyond that, Paragon has no website and there is little other public information on the company. *See* Mark Mazzetti, Ronen Bergman & Matina Stevis-Gridneff, *How the Global Spyware Industry Spiraled Out of Control*, N.Y. TIMES (Dec. 8, 2022), https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html.

spyware tool, Graphite, for use in operations against drug cartels.[7] NSO Group has reportedly also pitched Pegasus technology to the DEA,[8] the Secret Service,[9] and at least two municipal law enforcement agencies.[10]

Graphite is sold by Paragon, an Israeli corporation that has received significant funding from an American firm called Battery Ventures.[11] As with other spyware tools, Graphite spyware can gain access to virtually any data, including SMS and WhatsApp messages, emails, media, location data, contacts, the phone's microphone, and the phone's camera. However, unlike Pegasus, which accesses data stored inside the phone itself, Graphite primarily targets data stored in the cloud.[12] Therefore, it is more difficult to detect whether a device has been hacked using Graphite spyware, and whether any information has been exfiltrated.

Graphite's capacity to gain secret and unconstrained access to electronic device data poses an unquestionable risk to privacy rights and serves as a troubling sign of growing global mass surveillance. The public has a right to transparency concerning the DEA's purchase and use of spyware technology.

Request for Expedited Processing

EPIC is entitled to expedited processing of this request under DOJ's FOIA regulations.[13] Those regulations state that a FOIA request "shall be processed on an expedited basis whenever" it involves "[a]n urgency to inform the public about an actual or alleged Federal Government activity, if made by a person who is primarily engaged in disseminating information"; or "[a] matter of widespread and exceptional media interest in which there exist possible questions about the government's integrity that affect public confidence."[14] EPIC's request fulfills both of these standards and therefore should be expedited under either.

---

[7] *Id.*

[8] Drew Harwell, *How Washington Power Brokers Gained from NSO's Spyware Ambitions*, WASH. POST (July 19, 2021), https://www.washingtonpost.com/technology/2021/07/19/nso-business-us; Joseph Cox, *The DEA Didn't Buy Malware from Israel's Controversial NSO Group Because It Was Too Expensive*, MOTHERBOARD (Sept. 11, 2019), https://www.vice.com/en/article/3kxk9j/dea-didnt-buy-malwarenso-group-too-expensive (quoting an email from the then-Director of the DEA Office of Special Intelligence calling the technology "exciting"); Joseph Cox, *The DEA Met with Controversial iPhone Hackers NSO Group*, MOTHERBOARD (Aug. 2, 2017), https://www.vice.com/en/article/gygxk9/the-dea-met-with-controversial-iphone-hackers-nso-group.

[9] Joseph Cox, *NSO Group Pitched Its Spyware to the Secret Service*, MOTHERBOARD (July 23, 2020), https://www.vice.com/en/article/m7jp43/nso-group-pitched-its-spyware-to-the-secret-service.

[10] Harwell, *supra* note 8; Joseph Cox, *LAPD Got Tech Demos from Israeli Phone Hacking Firm NSO Group*, MOTHERBOARD (June 9, 2020), https://www.vice.com/en/article/n7wna7/lapd-phone-hacking-nso-group-westbridge.

[11] *See* Mazzetti et al., *supra* note 6; *see also* BATTERY, *List of All Companies*, https://www.battery.com/list-of-all-companies/ (listing Paragon Solutions Ltd. among active investments as of Q4 2022).

[12] *Id.*

[13] 28 C.F.R. § 16.5(e)(1); *see also* 5 U.S.C. §§ 552(a)(6)(E)(i)(I), 552(a)(6)(E)(v)(II).

[14] 28 C.F.R. § 16.5(e)(1).

(1) EPIC is an organization "primarily engaged in disseminating information" and the records sought concern "[a]n urgency to inform the public" of an "alleged Federal Government activity."

EPIC's request fulfills the first standard because there is an "urgency" to inform the public about whether the DEA has communicated with a company that sells intrusive spyware technology, and EPIC is an organization "primarily engaged in disseminating information."[15] As the Court explained in *EPIC v. DOD*, "EPIC satisfies the definition of 'representative of the news media'" entitling it to preferred fee status under FOIA.[16] EPIC is a non-profit organization committed to privacy, open government, and civil liberties that consistently discloses documents obtained through FOIA on its website, EPIC.org, and its online newsletter, the *EPIC Alert*.[17]

There is also an "urgency to inform the public about an actual or alleged Federal Government activity."[18] Media organizations have reported on DEA's continued interest in, and active deployment of, spyware technology. The DEA's reported contract with Paragon for Graphite spyware comes after previous reports of DEA communication with NSO Group and Westbridge, the U.S. arm of NSO Group, about their spyware known as Pegasus or Phantom.[19] The DEA's Office of Special Intelligence met with Westbridge, and Westbridge allegedly "conducted a demonstration of [NSO Group's] technology/product" to DEA employees.[20] Media reports have also linked the DEA to other spyware providers including the Italy-based Hacking Team.[21]

Recent events create a patent "urgency to inform the public" about the federal government's relationship with Paragon and the NSO Group. According to media reports, the DEA has an existing contract with Paragon for use to its Graphite spyware.[22] There is growing media scrutiny of spyware, and in particular, the federal government's use of foreign commercial spyware.[23] Media reports also indicate that, in response to these concerns, both Congress and the Biden administration are developing restrictions on the federal government's use of foreign commercial spyware tools like Pegasus and Graphite.[24] However, according to media reports, the Biden administration's restrictions exempt the DEA's existing contract with Paragon for its operations against drug cartels.[25] EPIC's request thus satisfies the first standard for expedited processing because there is an urgency to

---

[15] *ACLU v. U.S. Dep't of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).
[16] 241 F. Supp. 2d 5, 15 (D.D.C. 2003).
[17] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.
[18] 28 C.F.R. § 16.5(e)(1).
[19] *See* Cox, *The DEA Didn't Buy Malware from Israel's Controversial NSO Group Because It Was Too Expensive*, supra note 8; Cox, *The DEA Met with Controversial iPhone Hackers NSO Group*, supra note 8.
[20] *See* Cox, *The DEA Met with Controversial iPhone Hackers NSO Group*, *supra* note 8.
[21] *See* Lorenzo Franceschi-Bicchierai, *The DEA Has Been Secretly Buying Hacking Tools from an Italian Company*, MOTHERBOARD (Apr. 15, 2015), https://www.vice.com/en/article/kbz57w/the-dea-has-been-secretly-buying-hacking-tools-from-an-italian-company.
[22] Mazzetti et al., *supra* note 6.
[23] *See id.*; Mark Mazzetti & Ronen Bergman, *Internal Documents Show How Close the F.B.I. Came to Deploying Spyware*, N.Y. TIMES (Nov. 12, 2022), https://www.nytimes.com/2022/11/12/us/politics/fbi-pegasus-spyware-phones-nso.html.
[24] Mazzetti et al., *supra* note 6.
[25] *Id.*

inform the public of the DEA's communications with and concerning Paragon and Graphite, and EPIC "is primarily engaged in disseminating information."[26]

(2) The Federal Government's ties to the spyware Pegasus are "[a] matter of widespread and exceptional media interest" and those alleged ties present "questions about the government's integrity that affect public confidence."

Second, EPIC's request also fulfills the DOJ regulation's standard for expedited review because the federal government's alleged communications with Paragon and NSO Group present "[a] matter of widespread and exceptional media interest in which there exist possible questions about the government's integrity that affect public confidence."[27] There has been recent "widespread and exceptional media interest" in the use of spyware and the federal government's connections to companies that sell it, including NSO Group and Paragon.[28] Media organizations including the *Washington Post* have reported on connections between spyware companies and U.S. federal and local agencies, former U.S. federal officials, and U.S. companies.[29] Media publications have also taken significant interest in whether, and to what extent, DOJ and its subcomponents like the DEA deploy spyware tools.[30]

The DEA's deployment of Paragon spyware and interest in other spyware tools present grave questions about federal government actions that risk infringing on Americans' privacy rights. Releasing information about the DEA's communications with Paragon is crucial to addressing mounting public concern about the relationship between U.S. agencies and foreign spyware companies, as well as the public's concern about the mass surveillance of their electronic devices generally. EPIC's request therefore also satisfies the second standard for expedited review.

In submitting this request for expedited processing, EPIC certifies that this explanation is true and correct to the best of its knowledge and belief.[31]

---

[26] 28 C.F.R. § 16.5(e)(1).
[27] *Id.*
[28] In 2016, researchers at Citizen Lab at the University of Toronto published an initial investigation into the NSO Group. *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. Since then, coverage of NSO Group and other spyware makers has skyrocketed; the *New York Times* alone has published over 50 articles mentioning NSO Group since 2017. *See* NSO Group, N.Y. TIMES, https://www.nytimes.com/search?query=nso+group. Along with sustained media coverage, NSO Group has been subject to several lawsuits in U.S. courts. *See WhatsApp Inc. v. NSO Group Tech. Ltd.*, 491 F. Supp. 3d 584 (N.D. Cal. 2020); Compl., *Apple v. NSO Group Tech. Ltd.*, No. 3:21-cv-0907 (N.D. Cal. Nov. 23, 2021), https://www.apple.com/newsroom/pdfs/Apple_v_NSO_Complaint_112321.pdf; Compl., *Dada v. NSO Group*, No. 5:22-cv-07513 (N.D. Cal. Nov. 30, 2022), https://knightcolumbia.org/documents/c3wrjy7rzp.
[29] Harwell, *supra* note 8; Cox, *The DEA Didn't Buy Malware from Israel's Controversial NSO Group Because It Was Too Expensive*, *supra* note 8; Cox, *The DEA Met with Controversial iPhone Hackers NSO Group*, supra note 8.
[30] *See* Mazzetti et al., *supra* note 6; Mazzetti & Bergman, *supra* note 23.
[31] 5 U.S.C. § 552(a)(6)(E)(vi); 28 C.F.R. § 16.5(e)(3).

Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for fee classification purposes.[32] Based on EPIC's status as a "news media" requester, EPIC is entitled to receive the requested record with only duplication fees assessed.[33]

Further, any duplication fees should also be waived because disclosure is (1) "in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government" and (2) "not primarily in the commercial interests of" EPIC, the requester.[34] EPIC's request satisfies this standard based on the DOJ's three factors for granting a fee waiver.[35]

The DOJ considers the following three factors in their analysis: (1) the "subject matter of the request" concerns "identifiable operations or activities of the Federal Government with a connection that is direct and clear, not remote or attenuated"; (ii) disclosure "would be likely to contribute significantly to public understanding of those operations or activities"; and (iii) "disclosure [is] not [] primarily in the commercial interest of the requester."[36]

First, the news media-reported contract between Paragon and the DEA concerning Graphite spyware technology—and the DEA's subsequent use of Graphite—constitutes a "direct and clear" and "identifiable . . . "activit[y] of the Federal Government."[37]

Second, disclosure is "likely to contribute significantly to public understanding of those operations or activities."[38] Disclosure would "be meaningfully informative about government operations or activities" because there is no publicly available information about the scope of communications between Paragon and the DEA. Disclosure of the records requested will provide the public with a better and more comprehensive understanding of the nature of the federal government's negotiations and collaborations with Paragon. Disclosure will also provide the public with an insight into how decisions regarding their electronic privacy are being weighed by federal employees.

Furthermore, disclosure will "contribute to the understanding of a reasonably broad audience of persons interested in that subject" because it "shall be presumed that a representative of the news media," like EPIC, satisfies this consideration.[39]

Third, disclosure of the requested information is "not primarily in the commercial interest" of EPIC.[40] Again, EPIC is a non-profit organization committed to privacy, open government, and civil

[32] *EPIC v. DOD*, 241 F. Supp. 2d 5, 15 (D.D.C. 2003).
[33] 5 U.S.C. § 552(a)(4)(A)(ii)(II); 28 C.F.R. § 16.10(c).
[34] 5 U.S.C. § 552(a)(4)(A)(iii); 28 C.F.R. § 16.10(k)(1).
[35] 28 C.F.R. § 16.10(k)(2).
[36] 28 C.F.R. § 16.10(k)(2)(i)-(iii).
[37] 28 C.F.R. § 16.10(k)(2)(i); *see* Mazzetti et al., *supra* note 6 (reporting on the existence of a contract between the DEA and Paragon for use of Graphite in operations against drug cartels).
[38] 28 C.F.R. § 16.10(k)(2)(ii)(A)-(B).
[39] 28 C.F.R. § 16.10(k)(2)(ii)(B).
[40] 28 C.F.R. § 16.10(k)(2)(iii).

liberties.[41] Moreover, the DOJ "components ordinarily will presume that when a news media requester has satisfied the requirements of paragraphs (k)(2)(i) and (ii) of this section, the request is not primarily in the commercial interest of the requester."[42] As a non-profit research organization, EPIC has no commercial interest in the requested information. Therefore, as demonstrated above, EPIC is a news media requester and satisfies the public interest standard under (k)(2)(i) and (ii).

For these reasons, a fee waiver should be granted.

Conclusion

Thank you for your consideration of this request. EPIC anticipates your determination on its request within ten calendar days.[43] For questions regarding this request contact Chris Baumohl at 610-283-2913 or FOIA@epic.org, cc: baumohl@epic.org.

Respectfully submitted,

/s Jeramie Scott
Jeramie Scott
Senior Counsel

/s Chris Baumohl
Chris Baumohl
EPIC Law Fellow

[41] *See* EPIC, *supra* note 17.
[42] 28 C.F.R. § 16.10(k)(2)(iii)(B).
[43] 5 U.S.C. § 552(a)(6)(E)(ii)(I).