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 Fax

October 29, 2021

Michael G. Seidal, Section Chief
Record/Information Dissemination Section
Records Management Division
Federal Bureau of Investigation
Department of Justice
200 Constitution Drive
Winchester, VA 22602
Fax: (540) 868-4997

Dear Mr. Seidal:

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 Department of Justice's ("DOJ") Federal Bureau of Investigation ("FBI").

EPIC requests records related to the FBI's communications with NSO Group Technologies ("NSO Group") and its U.S. arm Westbridge Technology, Inc. ("Westbridge"). In particular, EPIC seeks any records of communications between the FBI and Westbridge about Westbridge's Phantom (more commonly known as "Pegasus"), a spyware that grants 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 FBI and any representatives from 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 FBI and any of the following individuals: Omri Lavie, Niv Carmi, Shalev Hulio, Chaim Gelfand, Terrence ("Terry") Divittorio, or Joshua ("Josh") Shaner;
    c. shared between the FBI and any email address ending with @nsogroup.com, @qtechnologies.com, or @westbrg.com;
    d. or referencing Pegasus, Phantom, Q Suite, or Chrysaor;

2. Any contracts or agreements between the FBI and 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 NSO Group or Westbridge presentations and sales materials or presentations and sales materials mentioning NSO Group, Westbridge, Pegasus, Phantom, Chrysaor, or Q Suite.

Background

In August 2021, Forbidden Stories, Amnesty International, and over a dozen media organizations published the Pegasus Project,[1] the results of a collaborative investigation into use of the hacking technology Pegasus on the phones of over a thousand political figures, journalists, and businesspeople around the globe.[2] Investigators found a list of 50,000 phone numbers that may have been targeted by the spyware, and upon further examination of the list linked the numbers to "more than 1,000 people spanning more than 50 countries."[3] Those targeted by Pegasus include French President Emmanuel Macron,[4] those close to Dubai's Princess Latifa,[5] those close to Jamal Khashoggi,[6] as well as other prominent academics, lawyers, and journalists.[7]

Pegasus (also known by other names including "Phantom"[8]) is sold by NSO Group, an Israeli corporation with an American arm called Westbridge Technology, Inc. ("Westbridge").[9] Pegasus works by installing itself onto an iPhone or Android cellular phone through software vulnerabilities

[1] *About the Pegasus Project*, FORBIDDEN STORIES, https://forbiddenstories.org/about-the-pegasus-project.
[2] Washington Post Staff, *Takeaways from the Pegasus Project*, WASH. POST (Aug. 2, 2021), https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project.
[3] *Id*.; The Wire Staff, *Pegasus Project: 161 Names Revealed by The Wire on Snoop List So Far*, The Wire (Aug. 4, 2021), https://thewire.in/rights/project-pegasus-list-of-names-uncovered-spyware-surveillance.
[4] *France's Macron Targeted in Project Pegasus Spyware Case*, REUTERS (JULY 21, 2021), https://www.reuters.com/technology/french-prosecutor-opens-probe-after-pegasus-spyware-complaint-2021-07-20.
[5] Washington Post Staff, *supra* note 2.
[6] Dana Priest, Souad Mekhennet, & Arthur Bouvart, *Jamal Khashoggi's Wife Targeted with Spyware Before His Death*, WASH. POST (July 18, 2021), https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/?itid=lk_inline_manual_21.
[7] *See* OPERATING FROM THE SHADOWS: INSIDE NSO GROUP'S CORPORATE STRUCTURE, AMNESTY INT'L, PRIVACY INT'L, & SOMO 25-26 (2021), https://www.somo.nl/wp-content/uploads/2021/05/Operating-from-the-Shadows.pdf (listing and discussing targets of Pegasus including Mexican journalist Carmen Aristegui, Moroccan academic Maati Monjib, and Moroccan human rights lawyer Abdessadak El Bouchattaoui); 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 (discussing the use of Pegasus against UAE-based activist Ahmed Mansoor and Mexican journalist Rafael Cabrera).
[8] Westbridge has pitched Pegasus as "Phantom." *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-s-nso-group-linked-to-hacking-tool-pitched-to-u-s-police. An additional variant of Pegasus is "Chrysaor." *See* Tom Spring, *Android Variant of Notorious Pegasus Spyware Found*, THREATPOST (Apr. 4, 2017), https://threatpost.com/android-variant-of-notorious-pegasus-spyware-found/124781.
[9] 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, *supra* note 7, at 31-33, 38-44, 49.

or malicious links.[10] 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."[11]

Researchers at Citizen Lab at the University of Toronto have uncovered several vulnerabilities exploited by Pegasus, the most recent of which was an Apple software vulnerability made public on September 13, 2021.[12] This recent vulnerability, coined "FORCEDENTRY" by Citizen Lab researchers, has reportedly "been active since at least February" and allows an attacker using Pegasus to secretly hack into Apple devices without device owners' knowledge.[13] Apple's release of an update designed to resolve the vulnerability generated substantial media coverage[14] and has added to the burgeoning public concern over Pegasus technology and its use by governments.

Recent media scrutiny into Pegasus has also highlighted ties between the Federal Government and NSO Group. NSO Group has been associated with former federal officials,[15] U.S.

[10] *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.
[11] *Id*. For more about how Pegasus works, see also *Ep 100: NSO*, DARKNET DIARIES (Aug. 31, 2021), https://darknetdiaries.com/transcript/100 (podcast transcript), and 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.
[12] The September 2021 Apple software vulnerability was not the first of its kind. In 2016, Apple discovered and corrected a vulnerability called "Trident"—"three zero days" that permit "an attacker to take complete control of an iPhone or iPad with just one click." Tom Spring, *Emergency iOS Update Patches Zero Days Used by Government Spyware*, THREATPOST (Aug. 25, 2016), https://threatpost.com/emergency-ios-update-patches-zero-days-used-by-government-spyware/120158.
[13] *See* Craig Timberg et al., *Update Your Apple Devices Now. New Pegasus Hack Found Targeting Apple Devices Through iMessage, Researchers Say*, WASH. POST (Sept. 14, 2021), https://www.washingtonpost.com/technology/2021/09/13/pegasus-spyware-new-exploit-apple.
[14] *See, e.g.*, *id*.; Carrie Mihalcik, Bree Fowler, *Apple's iOS 14.8 Pegasus Security Fix: iPhone Users Urged to Update Immediately*, CNET (Sept. 14, 2021), https://www.cnet.com/tech/services-and-software/apple-ios-14-8-pegasus-security-fix-iphone-users-urged-to-update-immediately; Josephine Wolff, *You Really, Really Need to Update Your iPhone and Other Apple Devices*, SLATE (Sept. 14, 2021), https://slate.com/technology/2021/09/apple-forcedentry-nso-group-pegasus-citizen-lab.html; Frank Bajak, *Apple Releases Emergency Update to Fix Security Vulnerability*, HUFFPOST (Sept. 13, 2021), https://www.huffpost.com/entry/cybersecurity-apple-security-update_n_613faff0e4b0628d095f108e; Nicole Perlroth, *Apple Issues Emergency Security Updates to Close a Spyware Flaw*, NY TIMES (Sept. 13, 2021), https://www.nytimes.com/2021/09/13/technology/apple-software-update-spyware-nso-group.html.
[15] For example, NSO Group has connections to Michael Flynn, Tom Ridge, Dan Jacobsen, and Jeh Johnson. *See* Harwell, *supra* note 11.

firms,[16] and U.S. states.[17] According to media reports, the NSO Group pitched Pegasus technology to the DEA, [18] the Secret Service,[19] and at least two municipal law enforcement agencies.[20]

Pegasus' 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 Federal Government's communications regarding the purchase or use of such a technology.

Request for Expedited Processing

EPIC is entitled to expedited processing of this request under DOJ's FOIA regulations.[21] 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."[22] EPIC's request fulfills both of these standards and therefore should be expedited under either.

(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 FBI has communicated with a company that sells intrusive spyware technology, and EPIC is an organization "primarily engaged in disseminating information."[23] As the Court explained in *EPIC v. DOD*, "EPIC satisfies the definition of 'representative of the news media'"

[16] NSO Group has directly or through its parent companies hired Mercury Public Affairs, *see* OPERATING FROM THE SHADOWS: INSIDE NSO GROUP'S CORPORATE STRUCTURE 53, *supra* note 7; Paul Weiss, *see* Harwell, *supra* note 11; SKDK, *see id*.; and King & Spalding, *see id*.
[17] Two funds associated with the Oregon and Alaska state governments have invested in Novalpina Capital Partner I SCSp, which owns NSO Group. *See* OPERATING FROM THE SHADOWS: INSIDE NSO GROUP'S CORPORATE STRUCTURE 44, *supra* note 7; AP News Wire, *Oregon Examines Spyware Investment Amid Controversy*, INDEPENDENT (Aug. 4, 2021), https://www.independent.co.uk/news/oregon-examines-spyware-investment-amid-controversy-oregon-nso-group-salem-emmanuel-macron-israeli-b1897116.html. Jasmine Levy, *Oregon Considers Investing in Spyware in Controversy*, PA. NEWS TODAY (Aug. 4, 2021), https://pennsylvanianewstoday.com/oregon-considers-investing-in-spyware-in-controversy-work/201799.
[18] Harwell, *supra* note 11; 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-malware-nso-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.
[19] 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.
[20] Harwell, *supra* note 11; 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.
[21] 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).
[22] 28 C.F.R. § 16.5(e)(1).
[23] *ACLU v. U.S. Dep't of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

entitling it to preferred fee status under FOIA.[24] 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*.[25]

There is also an "urgency to inform the public about an actual or alleged Federal Government activity."[26] Other federal agencies—including the DEA, another federal agency under the DOJ—have communicated with NSO Group and expressed interest in Pegasus technology. The DEA has reportedly communicated with Westbridge, the U.S. arm of NSO Group about the spyware known as "Pegasus" or "Phantom."[27] 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.[28] In addition to the DEA, the Secret Service has also reportedly communicated with NSO Group about Pegasus,[29] and at least two municipal law enforcement agencies have heard pitches from NSO Group.[30]

Recent events create a patent "urgency to inform the public" about the federal government's relationship with NSO Group. In August 2021, over a dozen media organizations, Forbidden Stories, and Amnesty International published the results of an investigation called the "Pegasus Project."[31] The Pegasus Project uncovered the use of NSO Group's Pegasus spyware technology on thousands of phones globally, including those belonging to prominent activists, politicians, and journalists.[32] Further, on September 13, 2021, Apple released a new software update after Citizen Lab discovered a software vulnerability that allowed Pegasus to hack Apple devices.[33] Apple's release of the update reignited the already growing media scrutiny on Pegasus spyware and NSO Group.[34] EPIC's request thus satisfies the first standard for expedited processing because there is an urgency to inform the public of the FBI's communications with and concerning Westbridge and NSO Group, and EPIC "is primarily engaged in disseminating information."[35]

(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."

---

[24] 241 F. Supp. 2d 5, 15 (D.D.C. 2003).
[25] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.
[26] 28 C.F.R. § 16.5(e)(1).
[27] *See* Cox, *The DEA Didn't Buy Malware from Israel's Controversial NSO Group Because It Was Too Expensive*, *supra* note 18; Cox, *The DEA Met with Controversial iPhone Hackers NSO Group*, *supra* note 18; *see also* OPERATING FROM THE SHADOWS: INSIDE NSO GROUP'S CORPORATE STRUCTURE 49, *supra* note 7 (discussing Westbridge's relationship with NSO Group); *supra* note 8 and accompanying text (discussing the aliases of Pegasus).
[28] *See* Cox, *The DEA Met with Controversial iPhone Hackers NSO Group*, *supra* note 18.
[29] *See* Cox, *NSO Group Pitched Its Spyware to the Secret Service*, *supra* note 19.
[30] *See* Cox, *LAPD Got Tech Demos from Israeli Phone Hacking Firm NSO Group*, *supra* note 20; Harwell, *supra* note 11.
[31] *See supra* note 1 and accompanying text.
[32] *See* Washington Post Staff, *supra* note 2.
[33] *See* Timberg et al., *supra* note 13.
[34] *See, e.g.*, *supra* note 14; Musadiq Bidar, *Apple Says Its Security Flaw Was Fixed. Cyber Analysts Warn Zero-Click Threats Will Persist*, CBS NEWS (Sept. 15, 2021), https://www.cbsnews.com/news/iphone-apple-security-flaw-zero-click-threats; Stephen Shankland, *Pegasus Spyware: Apple's iPhone Fix and Everything Else You Need to Know*, CNET (Sept. 14, 2021), https://www.cnet.com/tech/mobile/pegasus-spyware-apple-iphone-fix-and-everything-else-you-need-to-know.
[35] 28 C.F.R. § 16.5(e)(1).

Second, EPIC's request also fulfills the DOJ regulation's standard for expedited review because the federal government's alleged communications with 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."[36] There has been recent "widespread and exceptional media interest" in Pegasus spyware and the federal government's connections to the company that sells it, NSO Group. This media interest began in at least 2016, with Citizen Lab's publication of an investigation into Pegasus spyware,[37] but has reached an all-time high since WhatsApp filed a lawsuit in federal court against NSO Group in 2019,[38] dozens of organizations published the joint investigation "Pegasus Project" in August 2021,[39] and Apple released an update in September 2021 to resolve a software vulnerability exploited by Pegasus.[40] These events have corresponded with heightened media scrutiny into Pegasus, as well as NSO Group's relationship with U.S. government agencies.[41] Media publications including the *Washington Post* have reported on connections between NSO Group and U.S. federal and local agencies, former U.S. federal officials, and U.S. companies.[42]

The DOJ's ties to NSO Group and interest in Pegasus spyware present grave "questions" about the Federal Government's interest in protecting Americans' privacy rights against intrusive surveillance technology. Releasing information about the FBI's communications with NSO Group and Westbridge Technologies 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

---

[36] 28 C.F.R. § 16.5(e)(1).
[37] Marczak & Scott-Railton, *supra* note 7.
[38] WhatsApp Inc. v. NSO Group Tech. Ltd., 491 F. Supp. 3d 584 (N.D. Cal. 2020); *see* Josh Gerstein, *NSO Falters in Bid to Shut Down Suit over Hacking of WhatsApp*, POLITICO (Apr. 12, 2021), https://www.politico.com/news/2021/04/12/nso-falters-lawsuit-whatsapp-hacking-481073.
[39] *See About the Pegasus Project*, *supra* note 1; Washington Post Staff, *supra* note 2
[40] *See* Timberg et al., *supra* note 13.
[41] *See, e.g.*, OPERATING FROM THE SHADOWS: INSIDE NSO GROUP'S CORPORATE STRUCTURE, *supra* note 7; Harwell, *supra* note 15; Spencer S. Hsu, *Three Former U.S. Intelligence Operatives Admit to Working as 'Hackers-for-Hire' for the UAE*, WASH. POST (Sept. 15, 2021); Daniel Estrin, *What to Know About the Spying Scandal Linked to Israeli Tech Firm NSO*, NPR (Aug. 25, 2021), https://www.npr.org/2021/08/25/1027397544/nso-group-pegasus-spyware-mobile-israel; Drew Harwell & Shane Harris, *White House Has Spoken to Israeli Officials About Spyware Concerns Following Pegasus Project Revelations*, WASH. POST (July 29, 2021), https://www.washingtonpost.com/technology/2021/07/29/pegasus-white-house-israel-concerns; 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.

The collection of articles released under the Pegasus Project in and of itself represents "a widespread and exceptional media interest." In fact, "more than 80 reports from 17 media organizations in 10 countries" participated in the Pegasus Project. *See About the Pegasus Project*, *supra* note 1.
[42] Harwell, *supra* note 14; Jasmine Levy, *Oregon Considers Investing in Spyware in Controversy*, PA. NEWS TODAY (Aug. 4, 2021), https://pennsylvanianewstoday.com/oregon-considers-investing-in-spyware-in-controversy-work/201799; AP News Wire, *Oregon Examines Spyware Investment Amid Controversy*, INDEPENDENT (Aug. 4, 2021), https://www.independent.co.uk/news/oregon-examines-spyware-investment-amid-controversy-oregon-nso-group-salem-emmanuel-macron-israeli-b1897116.html; *see also* Cox, *The DEA Didn't Buy Malware from Israel's Controversial NSO Group Because It Was Too Expensive*, *supra* note 18; Cox, *The DEA Met with Controversial iPhone Hackers NSO Group*, *supra* note 18; DJ Pangburn, *The Secretive Billion-Dollar Company Helping Governments Hack Our Phones*, FAST CO. (Nov. 30, 2017), https://www.fastcompany.com/40469864/the-billion-dollar-company-helping-governments-hack-our-phones.

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.[43]

Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for fee classification purposes.[44] Based on EPIC's status as a "news media" requester, EPIC is entitled to receive the requested record with only duplications fees assessed.[45]

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.[46] EPIC's request satisfies this standard based on the DOJ's three factors for granting a fee waiver.[47]

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."[48]

First, news media-reported communications and meetings between Westbridge and officials within the DEA, another law enforcement agency under the DOJ, concerning Pegasus/Phantom spyware technology constitutes a "direct and clear" and "identifiable . . . "activit[y] of the Federal Government."[49]

Second, disclosure is "likely to contribute significantly to public understanding of those operations or activities."[50] Disclosure would "be meaningfully informative about government operations or activities" because there is no publicly available information about the scope of communications between NSO Group and the FBI. 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 NSO Group. Disclosure will also provide the public with an insight into how decisions regarding their electronic privacy are being weighed by federal employees.

---

[43] 5 U.S.C. § 552(a)(6)(E)(vi); 28 C.F.R. § 16.5(e)(3).
[44] *EPIC v. DOD*, 241 F. Supp. 2d 5, 15 (D.D.C. 2003).
[45] 5 U.S.C. § 552(a)(4)(A)(ii)(II); 28 C.F.R. § 16.10(c).
[46] 5 U.S.C. § 552(a)(4)(A)(iii); 28 C.F.R. § 16.10(k)(1).
[47] 28 C.F.R. § 16.10(k)(2).
[48] 28 C.F.R. § 16.10(k)(2)(i)-(iii).
[49] 28 C.F.R. § 16.10(k)(2)(i); *see supra* note 18 and accompanying text (reporting that NSO Group pitched its spyware technology to the DEA); *supra* note 19 and accompanying text (reporting that NSO Group pitched its spyware technology to the Secret Service).
[50] 28 C.F.R. § 16.10(k)(2)(ii)(A)-(B).

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.[51]

Third, disclosure of the requested information is "not primarily in the commercial interest" of EPIC.[52] Again, EPIC is a non-profit organization committed to privacy, open government, and civil liberties.[53] 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."[54] 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.[55] For questions regarding this request contact Jeramie Scott at 202-483-1140 x108 or FOIA@epic.org, cc: jscott@epic.org.

Respectfully submitted,

/s Jeramie Scott
Jeramie Scott
EPIC Senior Counsel

/s Dana Khabbaz
Dana Khabbaz
EPIC Law Fellow

[51] 28 C.F.R. § 16.10(k)(2)(ii)(B).
[52] 28 C.F.R. § 16.10(k)(2)(iii).
[53] *See* EPIC, *supra* note 25.
[54] 28 C.F.R. § 16.10(k)(2)(iii)(B).
[55] 5 U.S.C. § 552(a)(6)(E)(ii)(I).