Exhibit E

University at Buffalo
Clinical Legal Education
School of Law

December 12, 2018

Freedom of Information Act Appeal re: Expedited Processing
Director, Office of Information Policy
U.S. Department of Justice
Suite 11050
1425 New York Avenue, NW
Washington, DC 20530-0001

RE: FOIA Appeal of Expedited Processing
Request No. 1416471-000

Dear Sir or Madam:

We write on behalf of the co-requestors Privacy International ("PI"), the American Civil Liberties Union, and the American Civil Liberties Union Foundation (together, the "ACLU"), and the Civil Liberties and Transparency Clinic of the University at Buffalo School of Law ("CLTC"), to appeal the Federal Bureau of Investigation's ("FBI") October 5, 2018, decision denying expedited processing of our September 10, 2018, Freedom of Information Act ("FOIA") request.

I. Background

By letter dated September 10, 2018, PI, ACLU, and CLTC requested from the FBI copies of records related to any reports, guidelines, correspondence, or any other records pertaining to the acquisition and/or development of computer hacking tools by law enforcement agencies. The FOIA request (attached hereto as Exhibit A) sought two categories of records and asked for expedited processing under 5 U.S.C. § 552(a)(6)(E).

As of today, we have received one letter in response to our request to the FBI. The letter, from Section Chief David M. Hardy of the Information Management Division and dated October 5, 2018, acknowledged receipt of our request and denied expedited processing (attached as Exhibit B). We have received no documents from the FBI responsive to our request, nor has the FBI cited any FOIA exemptions as a basis for refusing to disclose records.[1]

II. Basis for Appeal

Pursuant to the U.S. Department of Justice ("DOJ") FOIA regulations, we hereby timely appeal the FBI's refusal to grant expedited processing. 28 C.F.R § 16.5(e). The FBI's denial letter does not cite to specific department regulations in support of its denial. Instead,

[1] This appeal is timely filed within 90 days of receipt of Mr. Hardy's letter denying our request for expedited processing. We received that letter on October 5, 2018.

507 O'Brian Hall, Buffalo, NY 14260-1100
716.645.6222 (F) 716.645-2167
jmmanes@buffalo.edu

www.buffalo.edu

the letter simply concludes that the request "ha[s] not provided enough information concerning the statutory requirements permitting expedition." Ex. B at 1. For the reasons stated at length in our original request, summarized and elaborated here, that denial is incorrect.

A. Requestors have demonstrated an "urgency to inform the public."

PI, the ACLU and CLTC's detailed FOIA request amply demonstrates that there is an urgency to inform the public about the governments use of hacking tools. FOIA and DOJ regulations requires expedited processing of requests when a "compelling need" for information that creates an "urgency to inform the public concerning actual or alleged Federal Government activity". 5 U.S.C. § 552(a)(6)(E); 28 C.F.R § 16.5(e)(ii). DOJ regulations elaborate that the requester "must establish a particular urgency…that extends beyond the public's right to know about government activities generally." 28 C.F.R § 16.5(e)(3). Importantly, DOJ regulations provide that "the existence of numerous articles published on a given subject can be helpful to establishing the requirement that there be an 'urgency to inform' the public on the topic." *Id.*

PI, ACLU, and CLTC's request satisfies the criteria specified in the statute and the DOJ's regulation. The request demonstrates that these there is an "urgency to inform the public" concerning government hacking technologies and, in particular, any FBI policies, procedures or investigations that involve the use of these technologies. The request elaborates in great detail on the matter or activity in question and why the records sought are necessary to be provided on an expedited basis. Indeed, the request includes more than eight pages of information about law enforcement agencies' deployment of hacking and related social engineering techniques to access and gather information on computer systems. *See* Ex. A, at 1-8, 16-17. These explanations are supported by numerous footnoted citations to sources and authority. *Id.*

The request demonstrates that the government's use and misuse of hacking technology has created an "urgency to inform the public"[2] by citing to "numerous articles published" on the subject, 28 C.F.R § 16.5(e)(3), as well as recent reports from NGOs and other sources that concern government hacking. – including an OIG report from another law enforcement agency. Nearly all of these sources are from the past two years. *See* Ex. A, at notes 3-21, 34-36, 43, 55-56 and accompanying text. Additionally, numerous breaking stories have recently been published on the government's use of hacking tools. *See* Ex. A, at 16 & n.55. At least one of these breaking news stories, which concerned the FBI's use of hacking, resulted in an OIG investigation that itself was the subject of considerable media interest. *See id.* at 21 n. 56. In the short time since the request was filed, there have been yet more news stories about government hacking, including by the FBI.[3] All of these sources

[2] U.S. Department of Justice, *Department of Justice Freedom of Information Act Reference Guide,* Jan. 30, 2017, https://www.justice.gov/oip/department-justice-freedom-information-act-reference-guide#b1 (last visited Oct. 1, 2018)

[3] See, e.g., Thomas Brewster, Trump's Immigration Cops Just Gave America's Hottest iPhone Hackers Their Biggest Payday Yet, Forbes, Sep. 18, 2018, https://www.forbes.com/sites/thomasbrewster/2018/09/18/ice-just-gave-americas-hottest-iphone-hackers-their-biggest-payday-yet/#216552b04d02; Lorenzo Franceschi-Bicchierai, *Malware Companies Are Finding New*

demonstrate, individually and collectively, that there is an immediate, current, and ongoing public interest in this topic and there is an "urgency to inform the public." 28 C.F.R § 16.5(e)(ii).

The request elaborates specific reasons why this subject matter is of *current* exigency to the American public. The request shows, for example, that these techniques are proliferating rapidly, particularly now that they are available commercially to law enforcement agencies. As the request explains, Privacy International has identified over 500 surveillance technology companies that sell products and services exclusively to government clients for law enforcement and intelligence-gathering purposes,[4] including tools to enable hacking. Failure to obtain prompt disclosure would compromise a significant recognized interest of the general public in understanding how the government is using—and whether the government is misusing—this new and extraordinarily intrusive investigative technology.

The rapid proliferation of this technology raises grave concerns about individual privacy and technological security. As the request explains in detail, hacking is a particularly intrusive technology, permitting both remote access to systems as well as novel forms of real-time surveillance. *See* Ex. A at 7. These techniques create a significant potential for misuse, as government actors can wield these techniques covertly and on a wide scale. *See* Ex. A at 8. A single hacking operation can sweep up individuals who are unrelated to a government investigation, potentially violating their rights to privacy and risking the exposure or sensitive information. *See* Ex. A at 8. For example, the FBI's use of "watering hole attacks" can expose hundreds – if not thousands – of website users to harmful malware that can infect their device regardless of whether they are of interest to the FBI. *See* Ex. A at 7 n. 20.

Similarly, the use of hacking raises concerns about device security. The government's use of malware might proliferate to systems beyond the target device, and may lead to similar attacks by other actors. *See* Ex. A at 7. Given the potential for misuse of these tools, they should be subject to clear, public rules. *See* Ex. A at 8. This is especially true for understanding when and where a warrant is required for the government to collect information through the use of hacking tools. *See* Ex. A at 8.

The public thus has an exigent need for information about the kinds of hacking that the government is engaged in and, especially, the internal protocols that govern the use of these invasive technologies by the FBI in its investigations. This information is critical to inform the ongoing and urgent public debate about the wisdom and legality of these

---

Ways to Spy on iPhones, Motherboard, Nov. 27, 2018, https://motherboard.vice.com/en_us/article/mby7kq/malware-to-spy-hack-iphones; Joseph Cox, *The FBI Created a Fake FedEx Website to Unmask a Cybercriminal*, Motherboard, Nov. 26, 2018, https://motherboard.vice.com/en_us/article/d3b3xk/the-fbi-created-a-fake-fedex-website-to-unmask-a-cybercriminal;

[4] Privacy International, *Privacy International Launches the Surveillance Industry Index & New Accompanying Report*, Oct. 23, 2017, https://www.privacyinternational.org/blog/54/privacy-international-launches-surveillance-industry-index-new-accompanying-report (last visited July 18, 2018).

methods, and to inform the public about whether the public's constitutional and statutory privacy interests are being respected.

B. Requesters are "primarily engaged in disseminating information to the public."

PI, the ACLU, and CLTC also satisfy the second prong of the expedited processing requirement because they are "primarily engaged in disseminating information" within the meaning of the statute and regulation. 5 U.S.C. § 552(a)(6)(E)(v)(II); 28 C.F.R § 16.5(e)(ii). The request provides more than five pages of evidence to establish this point. *See* Ex. A. at 10-16. To summarize briefly, PI engages in research and litigation specifically in order to shine light on overreaching state and corporate surveillance. PI achieves this goal primarily by disseminating information it gathers to the public by publishing reports, websites, blog posts, and several other types of material meant for general public consumption. *See* Ex. A, at 10-11 & nn. 29-36. Similarly, the ACLU works to defend and preserve the individual rights and liberties guaranteed by the Constitution and laws of the United States by gathering and disseminating information. Indeed, obtaining information about government activity, analyzing that information, and widely publishing and disseminating that information to the press and public are critical and substantial components of the ACLU's work and are among its primary activities. *See* Ex. A, at 11-14 & nn. 37-49. Finally, CLTC is a legal clinic that works in its own name and on behalf of clients to obtain and disseminate information on issues involving technology & privacy and law enforcement accountability, among others. *See* Ex. A., at 15 & nn. 50-53. There is thus no doubt that the requesters satisfy the requirement of being "primarily engaged in disseminating information."[5]

For these reasons, there is an "urgency to inform the public" that justifies expedited processing, and the FBI's denial should be reversed.

III. Request for Relief

For the foregoing reasons, we submit that PI, the ACLU, and CLTC are entitled to expedited processing. We respectfully request that you grant expedited processing and immediately begin processing the requested records for potential release.

Please direct all correspondence relating to this request to:

Jonathan Manes
Civil Liberties & Transparency Clinic
University at Buffalo School of Law
507 O'Brian Hall, North Campus
Buffalo, NY 14260-1100
(716) 645-6222
jmmanes@buffalo.edu

[5] Only one of the requestors needs to qualify in order for expedited processing to be required. *See ACLU v. DOJ*, 321 F. Supp. 2d at 30 n. 5 (citing *Al-Fayed v. CIA*, 254 F.3d 300, 309 (D.C. Cir. 2001) ("[A]s long as one of the plaintiffs qualifies as an entity 'primarily engaged in disseminating information,' this requirement is satisfied.").

Thank you for your prompt attention to this matter.

Sincerely,

Jonathan Manes, *supervising attorney*
Alex Betschen, *student attorney*
RJ McDonald, *student attorney*
Colton Kells, *student attorney*
Civil Liberties and Transparency Clinic
University at Buffalo School of Law, SUNY
507 O'Brian Hall, North Campus
Buffalo, NY 14260-1100
Tel: 716.645.6222
jmmanes@buffalo.edu

Brett Max Kaufman
Vera Eidelman
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
bkaufman@aclu.org
veidelman@aclu.org

Jennifer Stisa Granick
American Civil Liberties Union Foundation
39 Drumm Street
San Francisco, CA 94111
Tel: 415.343.0758
jgranick@aclu.org

Scarlet Kim
Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom
Tel: +44 (0)203 422 4321
scarlet@privacyinternational.org