UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

PRIVACY INTERNATIONAL; AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; and CIVIL LIBERTIES AND TRANSPARENCY CLINIC, Plaintiffs, v. FEDERAL BUREAU OF INVESTIGATION; DRUG ENFORCEMENT ADMINISTRATION; DEPARTMENT OF JUSTICE CRIMINAL DIVISION; U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT; U.S. CUSTOMS AND BORDER PROTECTION; INTERNAL REVENUE SERVICE; U.S. SECRET SERVICE; DEPARTMENT OF JUSTICE OFFICE OF THE INSPECTOR GENERAL; DEPARTMENT OF HOMELAND SECURITY OFFICE OF THE INSPECTOR GENERAL; DEPARTMENT OF THE TREASURY OFFICE OF THE INSPECTOR GENERAL; and TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Defendants.	Case No. 18-cv-1488

COMPLAINT FOR INJUNCTIVE RELIEF

INTRODUCTION

1. This is an action under the Freedom of Information Act, 5 U.S.C. § 552, seeking the release of records concerning the government's use of hacking to pursue ordinary law enforcement investigations. These records have been improperly withheld from Plaintiffs by the Defendants.

2. Law enforcement agencies throughout the federal government have used hacking tools and methods to accomplish a wide variety of intrusive surveillance. Hacking facilitates surreptitious, often remote, access to computers and therefore to personal, private data stored on people's cell phones, laptops, and other devices. Some tools allow the government to force computers to reveal identifying details about anonymous internet users. Others go much further, for example, allowing agents to engage in real-time surveillance by activating a device's microphone or camera to record without the user's knowledge or consent.

3. Law enforcement agencies have spent millions of dollars purchasing computer hacking tools or services. These tools and services are increasingly widespread and commercially accessible. Numerous private companies directly market sophisticated hacking tools and services to ordinary law enforcement agencies. Indeed, Plaintiff Privacy International has documented at least 500 surveillance technology companies around the world, including many that focus on hacking, that sell products and services exclusively to government clients for law enforcement and other purposes.

4. Increasingly, these tools are being used in ordinary day-to-day investigations, as contrasted with national security or foreign intelligence investigations. For example, in 2017, the FBI reportedly deployed hacking to identify a scammer impersonating a seafood vendor purporting to do business with Wegmans Food Markets. In that case, the FBI created a Microsoft Word document sent to the scammer that, when opened, connected the scammer's computer to an FBI server and transmitted the scammer's internet protocol ("IP") address and information relating to the scammer's computer's operating system. *See* Joseph Cox, *The FBI Created a Fake FedEx Website to Unmask a Cybercriminal*, Motherboard, Nov. 26, 2018.[1]

[1] Available at: https://motherboard.vice.com/en_us/article/d3b3xk/the-fbi-created-a-fake-fedex-website-to-unmask-a-cybercriminal.

5. Law enforcement use of hacking presents a unique threat to individual privacy. Hacking can be used to obtain volumes of personal information about individuals that would never previously have been available to law enforcement. Devices like cell phones and laptops store vast amounts of vital and extraordinarily sensitive information: detailed location records, intimate details of private communications, logs of everything that a person has read, written, or seen online, financial information, health information, and more. The notion that the government can access and obtain all of this information quickly and easily simply by running software on a person's device—and that it can even do so remotely and surreptitiously—represents a remarkable expansion of the government's surveillance powers.

6. There is also a significant concern that hacking can sweep up innocent users alongside those targeted by a government agency. Software can spread beyond a targeted device. In some instances, hacking techniques are designed to target a broad and undifferentiated class of individuals.

7. For example, one technique, commonly known as a "watering hole attack," involves commandeering and reconfiguring a website or internet service in order to deliver software to any device visiting the site. The FBI is known to have deployed this kind of attack on at least two occasions in order to surreptitiously gather information from infected computers and send it back to the FBI. In at least one instance, the FBI deployed this hack against an internet service suspected of hosting websites facilitating illicit activity, but which also hosted websites facilitating perfectly legal activity. Because the FBI cast its net too widely, numerous law-abiding civilians were likely affected.

8. Hacking also poses a serious threat to computer security. Hacking techniques exploit security vulnerabilities in electronic devices and the software that runs on them, which

many individuals may use. When law enforcement takes advantage of these vulnerabilities to conduct surveillance, it leaves a virtual door open for identity thieves, scammers, and others to similarly attack these devices. The government's use of hacking thus involves a trade-off against the general security of individuals' digital lives in favor of the government's surveillance powers.

9. Because of the privacy and security implications of hacking as well as its potential for misuse, the public has a strong interest in learning about how law enforcement is deploying and regulating hacking. At present, the public is in the dark about the extent to which ordinary law enforcement agencies use hacking. Even the rules and procedures that regulate law enforcement's use of hacking are largely secret.

10. For example, the public does not know when law enforcement agencies believe they can use hacking without obtaining a warrant or other judicial authorization. The public does not even know whether many of the defendant agencies have internal rules or protocols governing hacking. Without more information, the public is not able to exercise meaningful democratic oversight of this new and intrusive law enforcement capability. Even criminal defendants may not be fully aware of whether the government has engaged in hacking to search their devices, nor the scope and process of those searches. This degree of secrecy creates significant opportunities for misuse and abuse.

11. In order to remedy this problem, Plaintiffs Privacy International, the American Civil Liberties Union and the American Civil Liberties Union Foundation, and the Civil Liberties and Transparency Clinic of the University at Buffalo School of Law submitted FOIA requests to seven major federal law enforcement agencies and the inspectors general that oversee them. The requests seek information about what hacking tools and methods the government has acquired or developed; the legal interpretations, rules, and protocols, if any, that agencies have adopted to

govern such activities; how often they are used in ordinary criminal investigations; documented instances of misuse or abuse; and other basic information.

12. Plaintiffs filed the FOIA requests more than 100 days ago. Thus far, no Defendant has complied with its obligation to provide a prompt, full response. Nine of the Defendants have failed to provide any response at all; the other two provided cursory responses that were plainly insufficient, in violation of the FOIA.

13. Plaintiffs therefore bring this lawsuit to compel Defendants to comply with the FOIA and disclose information about computer hacking so that people can engage in meaningful public deliberation about when and how law enforcement agencies should be able to use this new and intrusive capability.

JURISDICTION AND VENUE

14. This Court has jurisdiction over the parties pursuant to 5 U.S.C. § 552(a)(4)(B) and 28 U.S.C. § 1331.

15. Venue lies in this district pursuant to 5 U.S.C. § 552(a)(4)(B) because Plaintiff Civil Liberties and Transparency Clinic has its principal place of business in Erie County, New York.

PARTIES

16. Privacy International ("PI") is a public interest, non-profit organization based in London, the United Kingdom, that defends the right to privacy around the world. PI is committed to ensuring that government surveillance complies with the rule of law and the international human rights framework. As part of this commitment, PI advocates for strong privacy protections and safeguards, including against the use of hacking by governments. PI further seeks to ensure that the public is informed about the conduct of governments in matters that affect the right to privacy. PI conducts research and investigations into government surveillance across the globe and shares

its findings with public officials, advocates, and the general public. PI is a registered charity in the U.K. and its principal place of business is in London.

17. The American Civil Liberties Union together with the American Civil Liberties Union Foundation (collectively, "ACLU") is a nationwide, non-profit, non-partisan organization with more than 2 million members dedicated to the constitutional principles of liberty and equality. The ACLU is committed to ensuring that the U.S. government acts in compliance with the Constitution and laws, including international legal obligations. The ACLU is also committed to principles of transparency and accountability in government, and seeks to ensure that the American public is informed about the conduct of its government in matters that affect civil liberties and human rights. The ACLU is headquartered in New York City. The American Civil Liberties Union Foundation is a separate § 501(c)(3) organization that educates the public about civil liberties and employs lawyers who provide legal representation free of charge in cases involving civil liberties.

18. The Civil Liberties & Transparency Clinic ("CLTC") is a public-interest legal clinic at the University at Buffalo School of Law. CLTC provides *pro bono* legal services and engages in policy research to defend free speech, privacy, and other individual rights, and to press for greater transparency and accountability in government.

19. Defendant Federal Bureau of Investigations ("FBI") is a component of the Department of Justice. FBI is an agency within the meaning of 5 U.S.C. § 552(f)(1).

20. Defendant Drug Enforcement Administration ("DEA") is a component of the Department of Justice. DEA is an agency within the meaning of 5 U.S.C. § 552(f)(1).

21. Defendant Department of Justice Criminal Division ("DOJ-CD") is a component of the Department of Justice. DOJ-CD is an agency within the meaning of 5 U.S.C. § 552(f)(1).

22. Defendant Immigration and Customs Enforcement ("ICE") is a component of the Department of Homeland Security. ICE is an agency within the meaning of 5 U.S.C. § 552(f)(1).

23. Defendant Customs and Border Protection ("CBP") is a component of the Department of Homeland Security. CBP is an agency within the meaning of 5 U.S.C. § 552(f)(1).

24. Defendant Internal Revenue Service ("IRS") is a component of the Department of the Treasury. IRS is an agency within the meaning of 5 U.S.C. § 552(f)(1).

25. Defendant United States Secret Service ("USSS") is a component of the Department of Homeland Security. USSS is an agency within the meaning of 5 U.S.C. § 552(f)(1).

26. Defendant Department of Justice Office of the Inspector General ("DOJ-OIG") is a component of the Department of Justice. DOJ-OIG is an agency within the meaning of 5 U.S.C. § 552(f)(1). DOJ-OIG is responsible for auditing and investigating DOJ programs for waste, fraud, abuse, and misconduct. DOJ-OIG has oversight authority over Defendants FBI, DOJ-CD, and DEA.

27. Defendant Department of Homeland Security Office of the Inspector General ("DHS-OIG") is a component of the Department of Homeland Security. DHS-OIG is an agency within the meaning of 5 U.S.C. § 552(f)(1). DHS-OIG is responsible for auditing and investigating DHS programs for waste, fraud, abuse, and misconduct. DHS-OIG has oversight authority over Defendants ICE, CBP, and USSS.

28. Defendant Department of the Treasury Office of the Inspector General ("Treasury-OIG") is a component of the Department of the Treasury. Treasury-OIG is an agency within the meaning of 5 U.S.C. § 552(f)(1). Treasury-OIG is responsible for auditing and investigating Treasury programs for waste, fraud, abuse, and misconduct. Treasury-OIG has oversight authority

over Defendant IRS. and other components of the Department of the Treasury that engage in criminal investigations.

29. Defendant Treasury Inspector General for Tax Administration ("TIGTA") is a component of the Department of the Treasury. TIGTA is an agency within the meaning of 5 U.S.C. § 552(f)(1). TIGTA is responsible for auditing and investigating IRS programs for waste, fraud, abuse, and misconduct.

FACTUAL BACKGROUND

30. Law enforcement agencies have begun using commercial and bespoke hacking tools and methods to interfere with computer systems in order to access and gather highly sensitive information, including individuals' locations, internet activities, communications, and personal files.

31. Hacking encompasses a diverse set of techniques, but generally refers to an act or series of acts that interfere with a computer system, causing it to act in a manner unintended or unforeseen by the manufacturer, user or owner of that system. Hacking often enables remote access to systems and potentially to all of the data stored on those systems.

32. In many instances, hacking involves surreptitiously installing software or code on a target device. That software—sometimes known as "malware"—can then cause the device to search for and report back information or exfiltrate data. Some hacking tools allow a remote user to activate a device's camera and microphone, to log keystrokes, or to otherwise hijack a computer's functions without the user's knowledge or consent.

33. Hacking is often used in conjunction with so-called "social engineering" techniques which, in this context, refer to the use of confidence tricks to gain a target's trust in order to facilitate hacking or otherwise gain access to a target system. For example, an investigator may

impersonate a trusted individual or organization in order to persuade the target to download a file or click a link that installs malware on the target's device.

34. The government's use of hacking raises deep concerns for several reasons: it threatens individual privacy; it threatens the security of computers and trust online; it is increasingly widespread; and it is not currently subject to clear rules.

Government hacking raises novel and profound privacy concerns

35. Hacking enables governments to remotely and surreptitiously access computers and the data stored on them. It also enables governments to conduct novel forms of real-time surveillance, such as by covertly turning on a device's microphone, camera or GPS-based locator technology. The information obtained through hacking can include details about a person's movements, communications, internet searches, personal files, and other private data. The government can then use this information to build a complete profile of that person or even reveal their most private innermost thoughts.

36. Before smartphones and laptops, much of this data, such as internet search and browsing history, simply did not exist. Similarly, it was not possible to obtain a record of a person's historical movements. And far fewer communications were stored, or even made in writing.

37. It is now a fact of modern life that electronic devices are collecting and storing massive amounts of personal data all of the time. As the Court noted in *Riley v. California*, "more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate." 134 S. Ct. 2473, 2479 (2014). Many phones automatically log a person's movements over time and some devices even track whether a person is running, walking, sitting, or sleeping. Every time a person shops for something

online, that information is saved. Every time a person sends a text message to a friend or family member, that text message is saved.

38. Mobile software applications or "apps" also generate and store personal, private data related to many different facets of a person's life. As the Court also noted in *Riley*, "There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely." 134 S. Ct. at 2490. All of this information is susceptible to capture through hacking.

39. Even hacking methods that do not acquire the most sensitive information about targets can still raise significant privacy concerns. Hacking software that forces a device to reveal its IP address to law enforcement can abridge a person's anonymity in contexts where there are First Amendment interests at stake. For example, in an operation involving an online entity known as "Freedom Hosting," the FBI seized a web server and configured it to deploy a piece of malicious code that de-anonymized all visitors. The operation was meant to target visitors to a child pornography website, but at least one perfectly legal website—a secure email service—was hosted on the same server and the FBI malware infected everyone visiting that site as well. *See* Joseph Cox, *Unsealed Court Docs Show FBI Used Malware Like 'A Grenade,'* Motherboard, Nov. 7, 2016.[2]

[2] Available at: https://motherboard.vice.com/en_us/article/wnxbqw/unsealed-court-docs-show-fbi-used-malware-like-a-grenade; Kevin Poulsen, *FBI Admits It Controlled TOR Servers Behind Mass Malware Attack*, Sept. 13, 2013, https://www.wired.com/2013/09/freedom-hosting-fbi/.

40. Government hacking attacks, such as these, demonstrate how readily hacking techniques can be deployed, and their potential to collect significant amounts of private information. More public information about government hacking is necessary in order to have a meaningful public dialogue about the threat that it poses to individuals' privacy.

Government hacking threatens the security of computers and trust online

41. Hacking by its very nature preys on the security weaknesses of computers or the software programs that run on them. Hacking perpetuates these vulnerabilities and potentially places every user of those devices or programs at risk. Today's government-exploited weakness may be tomorrow's international identity-theft opportunity.

42. For example, law enforcement agencies regularly hire companies to hack phones or other devices that are protected by passwords. These hacks can involve exploiting vulnerabilities in software. The government's use of hacking takes advantage of these vulnerabilities and creates incentives for the government to keep them secret rather than disclose them to companies so that they can be patched.

43. The government's use of hacking can also undermine trust online, particularly where the government uses "social engineering" techniques to impersonate trusted third-parties or otherwise gain a target's confidence.

44. For example, in 2007, an FBI agent impersonated a news reporter in order to trick a high school student into giving the investigator his identity. The agent, posing as an Associated Press ("AP") reporter, sent the student a link to a supposed AP story about prank bomb threats that had been sent to his school. The link directed the student, who was suspected of calling in the hoax threats, to a webpage showing a fake AP article that the FBI had created. The AP did not consent to the impersonation. The website delivered a virus to the student's computer that provided the

FBI with the student's IP address. The AP strongly criticized the FBI, noting that the FBI's actions threatened to undermine public trust in news organizations. *See* Mike Carter, *FBI Created Fake* Seattle Times *Web Page to Nab Bomb-Threat Suspect*, Seattle Times, Oct. 27, 2014.[3]

45. More recently, in 2017, the FBI deployed a fake FedEx webpage, designed to capture the IP address of an alleged internet scammer. The fake webpage displayed an error message, stating that it did not allow connection through unidentifiable proxy servers. This message was meant to force the alleged scammer to use an identifiable connection. It is unclear whether FedEx consented to the FBI's impersonation of their website. *See* Joseph Cox, *The FBI Created a Fake FedEx Website to Unmask a Cybercriminal*, Motherboard, Nov. 26, 2018.[4]

Government hacking tools are increasingly widespread and readily deployed

46. Government hacking poses increasingly urgent privacy and security risks because sophisticated hacking tools are becoming more widely available and increasingly easy to deploy. Law enforcement agencies can now purchase powerful hacking tools off the shelf from private companies or outsource hacking directly to such companies. PI has identified more than 500 surveillance technology companies around the world that sell products and services, including including many that focus on hacking, exclusively to government clients, for law enforcement and other purposes.

47. For example, ICE and the FBI have each spent at least $2 million on powerful phone and laptop hacking technology from the Israeli surveillance technology company Cellebrite.

48. Similarly, the DEA has expressed interest in hacking tools produced by NSO Group, according to documents obtained in response to a FOIA request.

[3] Available at: https://www.seattletimes.com/seattle-news/fbi-created-fake-seattle-times-web-page-to-nab-bomb-threat-suspect/.

[4] Available at: https://motherboard.vice.com/en_us/article/d3b3xk/the-fbi-created-a-fake-fedex-website-to-unmask-a-cybercriminal.

49. DEA has also reportedly spent almost $1 million on hacking technology sold by the Italian surveillance technology company Hacking Team.

50. The extent to which law enforcement agencies use hacking is largely unknown to the public; however, these reports and others suggest that their use is expanding.

Government hacking raises significant legal concerns

51. In light of the privacy and security implications of hacking, as well as its potential for misuse, these tools and methods should be subject to clear, public rules. At present, however, it is unclear what rules Defendants believe govern their use of hacking. It is also unclear whether law enforcement agencies have adopted internal protocols to regulate and oversee the deployment of hacking.

52. Under U.S. law, where the government seeks to search an individual's cell phone or computer for information stored there, a warrant is ordinarily required and must be founded upon probable cause that the device will contain evidence of a crime. Where the government seeks to intercept the content of communications in real time, the law generally requires a warrant founded upon probable cause not just that a person has committed or will commit a crime, but also that the targeted communication channels will be used in connection with the crime or are owned by the target.

53. More broadly, "searches and seizures" must comply with the Fourth Amendment's "reasonableness" requirement, which generally requires a warrant. Warrants, in turn, can be issued only upon a finding of probable cause and only when they describe with particularity the places or things to be searched or seized. Additionally, law enforcement agencies may be required to adopt minimization procedures to mitigate the privacy intrusion on individuals who are not the targets of an investigation.

54. Little is known about the internal rules that law enforcement agencies have adopted to regulate the deployment of hacking and related social engineering techniques by agency officials. It is unclear whether and when law enforcement agencies even regard hacking and related social engineering techniques as subject to warrant requirements or other legal constraints.

55. Hacking raises serious questions under the Fourth Amendment and various statutes. Yet the public does not know what the government's interpretations of these laws are, or what protocols the government has in place to ensure compliance with law. Transparency in this area is necessary in order for the public to be able to engage in a meaningful discussion regarding the lawfulness of law enforcement hacking.

THE FOIA REQUESTS

56. Plaintiffs submitted two FOIA requests (collectively, the "Requests") in order to shed light on the government's use of hacking for law enforcement purposes. The first request (the "Law Enforcement Request") seeks records from seven federal law enforcement agencies. The second request (the "OIG Request") seeks records from the Offices of Inspector General that oversee those law enforcement agencies.

57. Plaintiffs submitted the Law Enforcement Request to the federal law enforcement agencies that appear most likely to engage in hacking for domestic investigative purposes. The FBI and DEA are both known to have engaged in hacking to conduct investigations of domestic crimes. ICE and CBP are the principal immigration enforcement agencies and both engage in sophisticated electronic surveillance. The USSS and the IRS conduct investigations of financial and computer-based crimes. DOJ-CD is responsible for establishing policies, procedures, and legal interpretations regarding electronic surveillance methods and for litigating issues involving hacking in federal criminal cases.

58. The Law Enforcement Request seeks basic information concerning each of these agencies' use of hacking. It is attached hereto as **Exhibit A**.

59. Specifically, the Law Enforcement Request includes a definition of "hacking techniques" and seeks five specific categories of records on the subject, reproduced here:

1. Records relating to the agency's use, acquisition, borrowing, sale, loan, research, and/or development of hacking techniques or equipment, software and/or technology that implements or facilitates hacking techniques including, but not limited to:

    a. Purchase orders, lease agreements, invoices, receipts and/or contracts with entities providing such equipment, software and/or technology;

    b. Policies, guidelines, legal opinions and/or rules;

    c. Documents requiring or requesting that information regarding hacking techniques be kept confidential;

    d. Deployment and/or training materials, including materials from internal and external conferences, courses, training sessions, workshops, or similar events;

    e. Marketing, promotional, or informational materials, including materials from external conferences, trade shows, training sessions, workshops, or similar events that employees of the agency have attended.

2. Records that constitute or contain reports, audits, assessments, or statistical information about hacking techniques or law enforcement investigations in which a hacking technique was deployed.

3. Records reflecting internal approvals or authorizations (or disapprovals/denials) of the use of a hacking technique in a criminal or civil investigation, as well any standard forms, templates, checklists or similar documents that are used as part of any internal process(es) for obtaining approval to use hacking techniques.

4. Licenses, waivers, or agreements with local, state and/or federal agencies or foreign entities, including foreign law enforcement agencies, that concern the use of hacking techniques.

5. Communications with local, state and/or federal agencies or foreign entities, including foreign law enforcement agencies, that concern "computer network exploitation" or a "network investigative technique."

60. Plaintiffs submitted the OIG Request to four Offices of Inspector General, specifically the DOJ-OIG, DHS-OIG, Treasury-OIG, and TIGTA.

61. The OIG Request seeks reports and underlying records relating to OIG investigations of government hacking. The Request is attached hereto as **Exhibit B**.

62. Specifically, the OIG Request includes the same definition of "hacking techniques" as the Law Enforcement Request but seeks the following two categories of records:

1. Any reports, memoranda, summaries or similar documents arising out of an investigation, internal inquiry, audit, evaluation or other oversight activity that concerns hacking techniques or the use of equipment, software and/or technology that implements or facilitates hacking techniques.

2. Any records that the OIG relied upon in the course of preparing reports or other documents responsive to request (1) above.

63. Both Requests ask for expedited processing pursuant to 5 U.S.C. § 552(a)(6)(E).

64. Both Requests ask for a public interest fee waiver as defined in 5 U.S.C. § 552(a)(4)(a)(iii).

65. Both Requests ask for a waiver of search and review fees because Plaintiffs qualify for "news media" or "educational institution" status under 5 U.S.C. § 552(a)(4)(A)(ii).

66. As detailed below, Defendants have failed to provide the records requested by Plaintiffs in the Request, despite the Act's requirement of an agency response within twenty working days.

67. As further detailed below, Plaintiffs have exhausted applicable administrative remedies or are deemed to have exhausted administrative remedies because Defendants have failed to respond within the statutory deadlines. 5 U.S.C. § 552(a)(6)(C)(i).

AGENCY RESPONSES

Federal Bureau of Investigation

68. Plaintiffs submitted the Law Enforcement Request to the FBI by fax on September 13, 2018.

69. Defendant FBI acknowledged receipt of the Request on September 14, 2018 by email. A copy of the email is attached as **Exhibit C**.

70. The FBI has produced no documents responsive to the Law Enforcement Request, nor has the FBI provided any reasons for withholding responsive documents. More than twenty business days have elapsed without a response. Plaintiffs have therefore constructively exhausted their administrative remedies with respect to this issue. 5 U.S.C. §§ 552(a)(6)(A)(i), 552(a)(6)(C)(i).

71. By letter dated October 5, 2018, the FBI granted Plaintiffs' request for a fee limitation as an "educational institution" requester. A copy of the letter is attached as **Exhibit D**.

72. The FBI has not issued a determination with respect to Plaintiffs' request for a public interest fee waiver. Because the FBI has not issued a determination within twenty business days, Plaintiffs have constructively exhausted their administrative remedies on this issue.

73. In its October 5, 2018 letter, the FBI denied Plaintiffs' request for expedited processing.

74. Plaintiffs timely appealed the FBI's denial of expedited processing by letter dated December 12, 2018, which was received on December 13, 2018. A copy of Plaintiffs' appeal is attached as **Exhibit E.**

75. Plaintiffs' administrative appeal from the FBI's denial of expedited processing was denied by letter dated December 18, 2018, thereby exhausting Plaintiffs' administrative remedies. A copy of the decision is attached as **Exhibit F**.

76. The FBI has assigned Plaintiffs' FOIA request tracking number 1416471-000 and Plaintiffs' appeal tracking number is DOJ-AP-2019-001448.

Drug Enforcement Administration

77. Plaintiffs submitted the Law Enforcement Request to the DEA by email on September 10, 2018.

78. Defendant DEA formally acknowledged receipt of the Request by phone call on September 14, 2018.

79. In a letter dated September 18, 2018, DEA extended its time to respond beyond the statutory 10-day extension, citing "unusual circumstances." 5 U.S.C. § 552(a)(6)(B). A copy of the letter is attached as **Exhibit G**.

80. The DEA has produced no documents responsive to the Law Enforcement Request, nor has the DEA provided any reasons for withholding responsive documents. More than thirty business days have elapsed without a response. Plaintiffs have therefore constructively exhausted their administrative remedies with respect to this issue. 5 U.S.C. §§ 552(a)(6)(A)(i), 552(a)(6)(C)(i).

81. In its September 18, 2018 letter, the DEA granted Plaintiffs' request for a fee limitation as a "representative of the news media."

82. The DEA has not issued a determination with respect to Plaintiffs' request for a public interest fee waiver. Because the DEA has not issued a determination within twenty business days, Plaintiffs have constructively exhausted their administrative remedies on this issue.

83. In a letter dated September 24, 2018, the DEA denied Plaintiffs' request for expedited processing. A copy of the letter is attached as **Exhibit H.**

84. Plaintiffs timely appealed the DEA's denial of expedited processing by letter dated December 12, 2018, which was received on December 13, 2018. A copy of Plaintiffs' Appeal is attached as **Exhibit I**.

85. Plaintiffs' administrative appeal from DEA's denial of expedited processing was denied by letter dated December 18, 2018, thereby exhausting Plaintiffs' administrative remedies. A copy of the decision is attached as **Exhibit J**.

86. The DEA has assigned Plaintiffs' FOIA request tracking number 18-01069-F and Plaintiffs' appeal tracking number is DOJ-AP-2019-001447.

DOJ Criminal Division

87. Plaintiffs submitted the Law Enforcement Request to the DOJ-CD by email on September 10, 2018.

88. Defendant DOJ-CD formally acknowledged receipt of the Request in a letter dated September 20, 2018. A copy of the letter is attached as **Exhibit K**.

89. In its September 20, 2018 letter, DOJ-CD invoked a 10-day extension to respond to the request, citing "unusual circumstances." 5 U.S.C. § 552(a)(6)(B).

90. The DOJ-CD has produced no documents responsive to the Law Enforcement Request, nor has the DOJ-CD provided any reasons for withholding responsive documents. More than thirty business days have elapsed without a response. Plaintiffs have therefore constructively exhausted their administrative remedies with respect to this issue. 5 U.S.C. §§ 552(a)(6)(A)(i), 552(a)(6)(C)(i).

91. The DOJ-CD has not issued a determination with respect to Plaintiffs' request for a public interest fee waiver or a limitation of fees. Because the DOJ-CD has not issued a determination within twenty business days, Plaintiffs have constructively exhausted their administrative remedies on this issue.

92. In its September 20, 2018 letter, the DOJ-CD denied Plaintiffs' request for expedited processing.

93. Plaintiffs timely appealed the DOJ-CD's denial of expedited processing by letter dated December 12, 2018, sent via overnight courier. A copy of Plaintiffs' Appeal is attached as **Exhibit L.**

94. Plaintiffs' administrative appeal from DOJ-CD's denial of expedited processing was denied by letter dated December 18, 2018, thereby exhausting Plaintiffs' administrative remedies. A copy of the decision is attached as **Exhibit M**.

95. The DOJ-CD has assigned Plaintiffs' FOIA request tracking number CRM-300680988 and Plaintiffs' Appeal tracking number is DOJ-AP-2019-001449.

Immigration and Customs Enforcement

96. Plaintiffs submitted the Law Enforcement Request to ICE by email on September 10, 2018.

97. Defendant ICE formally acknowledged receipt of the Request in an email dated September 11, 2018. A copy of the email is attached as **Exhibit N**.

98. In its September 11, 2018 email, ICE invoked a 10-day extension to respond to the request, citing "unusual circumstances." 5 U.S.C. § 552(a)(6)(B).

99. ICE has produced no documents responsive to the Law Enforcement Request, nor has ICE provided any reasons for withholding responsive documents. More than thirty business

days have elapsed without a response. Plaintiffs have therefore constructively exhausted their administrative remedies with respect to this issue. 5 U.S.C. §§ 552(a)(6)(A)(i), 552(a)(6)(C)(i).

100. ICE has not issued a determination with respect to Plaintiffs' request for a public interest fee waiver. Because ICE has not issued a determination within twenty business days, Plaintiffs have constructively exhausted their administrative remedies on this issue.

101. ICE has not issued a determination with respect to Plaintiffs' request for expedited processing. Because ICE has not issued a determination within twenty business days, Plaintiffs have constructively exhausted their administrative remedies on this issue.

102. ICE has assigned Plaintiffs' FOIA request tracking number 2018-ICFO-60213.

Customs and Border Protection

103. Plaintiffs submitted the Law Enforcement Request to the CBP by letter postmarked September 10, 2018.

104. Defendant CBP formally acknowledged receipt of the Request by email on November 27, 2018. A copy of the email is attached as **Exhibit O**.

105. CBP has not issued a determination with respect to Plaintiffs' request on any issue. Because the CBP has not issued a determination within twenty business days, Plaintiffs have constructively exhausted their administrative remedies. 5 U.S.C. § 552(a)(6)(C)(i).

106. CBP has assigned Plaintiffs' FOIA request tracking number CBP-2019-013335.

Internal Revenue Service

107. Plaintiffs submitted the Law Enforcement Request to the IRS by fax on September 13, 2018.

108. Defendant IRS acknowledged receipt of the Request on September 13, 2018.

109. By letter dated October 4, 2018, the IRS indicated that it would not process Plaintiffs' request as written because it did not provide sufficient detail about the records requested. The letter instructed Plaintiffs to contact IRS by phone or to submit a letter in response by November 8, 2018. A copy of the letter is attached as **Exhibit P**.

110. Plaintiffs attempted to contact Disclosure Tax Law Specialist, Bernard McDade, by phone three times, on October 31, 2018, November 1, 2018, and November 5, 2018. On none of these occasions were Plaintiffs able to speak with Mr. McDade.

111. Plaintiffs responded to the IRS's October 4, 2018 letter by letter dated November 8, 2018, in which they provided additional details regarding the scope of the request and asked the IRS to process the request as written. A copy of Plaintiffs' response is attached as **Exhibit Q**.

112. Mr. McDade of the IRS responded to Plaintiffs' November 8, 2018 letter by voicemail message on November 19, 2018. Plaintiffs have since spoken with Mr. McDade and have exchanged information in an effort to facilitate IRS's search for responsive records.

113. IRS has yet to produce or withhold any responsive records or to provide a basis for denying the request. Because more than twenty business days have elapsed without a response, Plaintiffs have constructively exhausted their administrative remedies. 5 U.S.C. § 552(a)(6)(C)(i).

114. The IRS has not issued a determination with respect to Plaintiffs' request for a public interest fee waiver or limitation of fees. Because the IRS has not issued a determination within twenty business days, Plaintiffs have constructively exhausted their administrative remedies on this issue.

115. The IRS has not issued a determination with respect to Plaintiffs' request for expedited processing. Because the IRS has not issued a determination within ten business days, Plaintiffs have constructively exhausted their administrative remedies on this issue

116. The IRS has assigned Plaintiffs' FOIA request tracking number F18257-0012.

United States Secret Service

117. Plaintiffs submitted the Law Enforcement Request to the USSS by email on September 10, 2018.

118. Defendant USSS acknowledged receipt of the Request on October 9, 2018, by letter dated October 22, 2018. A copy of the letter is attached as **Exhibit R**.

119. The USSS has yet to produce or withhold any responsive records or to provide a basis for denying the request. Because more than twenty business days have elapsed without a response, Plaintiffs have constructively exhausted their administrative remedies. 5 U.S.C. § 552(a)(6)(C)(i).

120. The USSS granted Plaintiffs' request for a limitation of fees as an "educational institution" requester in its October 22, 2018 letter.

121. The USSS has not issued a determination with respect to Plaintiffs' request for a public interest fee waiver. Because the USSS has not issued a determination within twenty business days, Plaintiffs have constructively exhausted their administrative remedies on this issue.

122. The USSS has not issued a determination with respect to Plaintiffs' request for expedited processing. Because the USSS has not issued a determination within ten business days, Plaintiffs have constructively exhausted their administrative remedies on this issue

123. The USSS has assigned Plaintiffs' FOIA request tracking number 20190014.

DOJ Office of Inspector General

124. Plaintiffs submitted the OIG Request to the DOJ-OIG by email on September 10, 2018.

125. Defendant DOJ-OIG formally acknowledged receipt of the OIG Request by letter dated September 28, 2018, which also constituted DOJ-OIG's final response. A copy of the letter is attached as **Exhibit S.**

126. In its September 28, 2018 letter, DOJ-OIG provided Plaintiffs with links to three publicly available documents as its response to the request and notified Plaintiffs that it was closing the request.

127. Plaintiffs timely appealed DOJ-OIG's response by letter dated December 5, 2018, sent via overnight courier and received December 6, 2018. A copy of Plaintiffs' Appeal is attached as **Exhibit T**.

128. Plaintiffs have not yet exhausted administrative remedies with respect to this specific issue; DOJ-OIG must issue a response by January 7, 2019, twenty business days after the appeal was received. 5 U.S.C. § 552(a)(6)(A)(ii).

129. DOJ-OIG has not issued a determination with respect to Plaintiffs' request for a public interest fee waiver or limitation of fees. Because DOJ-OIG has not issued a determination within twenty business days, Plaintiffs have constructively exhausted their administrative remedies on this issue.

130. DOJ-OIG has not issued a determination with respect to Plaintiffs' request for expedited processing. Because DOJ-OIG has not issued a determination within ten business days, Plaintiffs have constructively exhausted their administrative remedies on this issue.

131. DOJ-OIG has assigned Plaintiffs' FOIA request tracking number 18-OIG-505. Plaintiffs' appeal tracking number is DOJ-AP-2019-001378.

DHS Office of Inspector General

132. Plaintiffs submitted the OIG Request to the DHS-OIG by fax on September 13, 2018.

133. Defendant DHS-OIG formally acknowledged receipt of the OIG Request on September 13, 2018, by letter dated September 21, 2018. A copy of the letter is attached as **Exhibit U**.

134. In its September 21, 2018 letter, DHS-OIG invoked a 10-day extension to respond to the request, citing "unusual circumstances." 5 U.S.C. § 552(a)(6)(B).

135. DHS-OIG has produced no documents responsive to the OIG Request, nor has the DHS-OIG provided any reasons for withholding responsive documents. More than thirty business days have elapsed without a response. Plaintiffs have therefore constructively exhausted their administrative remedies with respect to this issue. 5 U.S.C. §§ 552(a)(6)(A)(i), 552(a)(6)(C)(i).

136. DHS-OIG has not issued a determination with respect to Plaintiffs' request for a public interest fee waiver or limitation of fees. Because DHS-OIG has not issued a determination within twenty business days, Plaintiffs have constructively exhausted their administrative remedies on this issue.

137. DHS-OIG denied Plaintiffs' request for expedited processing in the September 21 letter.

138. Plaintiffs timely appealed DHS-OIG denial of expedited processing by letter dated December 12, 2018, sent via overnight courier. A copy of the Plaintiffs' appeal is attached as **Exhibit V**.

139. Plaintiffs have not yet exhausted administrative remedies with respect to this specific issue; DHS-OIG must issue a response by January 14, 2019, twenty business days after the appeal was received. 5 U.S.C. § 552(a)(6)(A)(ii).

140. DHS-OIG has assigned Plaintiffs' FOIA request tracking number 2018-IGFO-00203.

Treasury Office of Inspector General

141. Plaintiffs submitted the OIG Request to the Treasury-OIG by fax on September 13, 2018.

142. Defendant Treasury-OIG formally acknowledged receipt of the OIG Request by letter dated September 14, 2018. A copy of the letter is attached as **Exhibit W**.

143. In its September 14, 2018 letter, Treasury-OIG invoked a 10-day extension to respond to the request, citing "unusual circumstances." 5 U.S.C. § 552(a)(6)(B).

144. Treasury-OIG has produced no documents responsive to the Law Enforcement Request, nor has the Treasury-OIG provided any reasons for withholding responsive documents. More than thirty business days have elapsed without a response. Plaintiffs have therefore constructively exhausted their administrative remedies with respect to this issue. 5 U.S.C. §§ 552(a)(6)(A)(i), 552(a)(6)(C)(i).

145. Treasury-OIG has not issued a determination with respect to Plaintiffs' request for a public interest fee waiver or limitation of fees. Because Treasury-OIG has not issued a determination within twenty business days, Plaintiffs have constructively exhausted their administrative remedies on this issue.

146. In its September 14, 2018 letter, Treasury-OIG granted Plaintiff's request for expedited processing.

147. Treasury-OIG has assigned Plaintiffs' FOIA request tracking number 2018-09-072

Treasury Inspector General for Tax Administration

148. Plaintiffs submitted the OIG Request to the TIGTA by email on September 10, 2018.

149. Defendant TIGTA formally acknowledged receipt of the OIG Request by letter dated September 12, 2018. A copy of the letter is attached as **Exhibit X**.

150. In a letter dated October 4, 2018, TIGTA reported that it had conducted a search and did not find any documents responsive to Plaintiffs' FOIA request. A copy of the letter is attached as **Exhibit Y**.

151. Plaintiffs timely appealed TIGTA's October 4, 2018 response by letter dated December 5, 2018, sent via overnight courier. A copy of Plaintiffs' appeal is attached at **Exhibit Z**.

152. Plaintiffs have not yet exhausted administrative remedies with respect to this specific issue; TIGTA must issue a response by January 7, 2019, twenty business days after the appeal was received. 5 U.S.C. § 552(a)(6)(A)(ii).

153. In its October 4, 2018 letter, TIGTA determined Plaintiffs' fee waiver request to be moot, as the costs incurred were less than twenty-five dollars. Plaintiffs' December 5, 2018 appeal reasserts their entitlement to a fee waiver and limitation of fees.

154. Defendant TIGTA denied Plaintiffs' request for expedited processing in its initial September 12, 2018 letter acknowledging receipt.

155. Plaintiffs timely appealed TIGTA's denial of expedited processing within the ten-day deadline, by letter postmarked on September 22, 2018, sent via USPS Priority Mail. A copy of Plaintiffs' appeal is attached as **Exhibit AA**.

156. In a letter dated October 5, 2018, TIGTA indicated that it considered Plaintiffs' September 22, 2018 appeal on the issue of expedited processing moot because TIGTA had issued a final response to the request in its October 4, 2018 letter. A copy of the letter is attached as **Exhibit BB**. Plaintiffs' December 5, 2018 appeal challenging TIGTA's final response reasserts Plaintiffs' entitlement to expedited processing.

157. TIGTA assigned Plaintiffs' FOIA request tracking number 2018-FOI-00260.

FIRST CAUSE OF ACTION
(Failure to provide records promptly)

158. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

159. Defendants have failed to make the records sought in the Requests promptly available in violation of 5 U.S.C. § 552(a)(3)(A).

160. This claim is not asserted against Defendants TIGTA and DOJ-OIG because an administrative appeal remains pending related to this issue and the statutory deadline for a decision has not yet passed.

SECOND CAUSE OF ACTION
(Failure to provide a timely response)

161. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

162. Defendants have failed to provide a response to the Requests in violation of 5 U.S.C. § 552(a)(6)(A).

163. This claim is not asserted against Defendants TIGTA and DOJ-OIG because an administrative appeal remains pending related to this issue and the statutory deadline for a decision has not yet passed.

THIRD CAUSE OF ACTION
(Failure to make a reasonable effort to search for records)

164. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

165. Defendants have failed to make a reasonable effort to search for records responsive to Plaintiffs' request in violation of 5 U.S.C. § 552(a)(3)(C).

166. This claim is not asserted against Defendants TIGTA and DOJ-OIG because an administrative appeal remains pending related to this issue and the statutory deadline for a decision has not yet passed.

FOURTH CAUSE OF ACTION
(Improperly withheld records)

167. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

168. Defendants have wrongfully withheld specific responsive records, or portions thereof, in violation of 5 U.S.C. §§ 552(a)(3)(A) and (6)(A). Defendants have no proper basis to withhold responsive records under 5 U.S.C. § 552(b) or otherwise. Nor do Defendants have a proper basis to exclude records from FOIA under 5 U.S.C. § 552(c).

FIFTH CAUSE OF ACTION
(Failure to grant public interest fee waiver)

169. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

170. Defendants have failed to grant Plaintiffs' request for a public interest fee waiver in violation of 5 U.S.C. § 552(a)(4)(A).

SIXTH CAUSE OF ACTION
(Failure to grant limitation of fees)

171. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

172. Defendants have failed to grant Plaintiffs' request for a limitation of fees in violation of 5 U.S.C. § 552(a)(4)(A).

173. This claim is not asserted against Defendants FBI, DEA, and USSS to the extent that those agencies have granted one or more Plaintiffs a fee limitation as either an "educational institution" or "representative of the news media."

SEVENTH CAUSE OF ACTION
(Failure to grant expedited processing)

174. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

175. Defendants have failed to grant Plaintiffs' request for expedited processing in violation of 5 U.S.C. § 552(a)(6)(E).

176. This claim is not asserted against Defendant Treasury-OIG because it granted Plaintiffs expedited processing, and the claim is not asserted against Defendant DHS-OIG because an administrative appeal remains pending on this issue and the statutory deadline for a decision has not yet passed.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

A. Order Defendants to search for all records responsive to the Requests;

B. Order Defendants to process and release all records responsive to the Requests immediately;

C. Declare whether any exemptions claimed prior to and in the course of this litigation are proper, and order disclosure of all non-exempt records or portions thereof;

D. Declare that Defendants wrongfully failed to grant Plaintiffs' request for expedited processing;

E. Order Defendants to process Plaintiffs' Requests expeditiously;

F. Enjoin Defendants from charging Plaintiffs search, review, or duplication fees for processing the Requests;

G. Declare that Plaintiffs are entitled to a public interest fee waiver;

H. Declare that Plaintiffs are entitled to a limitation of fees;

I. Award Plaintiffs their costs and reasonable attorneys' fees incurred in this action pursuant to 5 U.S.C. § 552(a)(4)(E); and

J. Grant any such other relief as the Court may deem just and proper.

Respectfully submitted,

/s/Jonathan Manes

Jonathan Manes
Alex Betschen, *Student Attorney*†
RJ McDonald, *Student Attorney*†
Colton Kells, *Student Attorney*†
Civil Liberties and Transparency Clinic
University at Buffalo School of Law
507 O'Brian Hall, North Campus
Buffalo, NY 14260-1100
Tel: 716-645-6222
Fax: 716-645-6199
jmmanes@buffalo.edu

Brett Max Kaufman*
Vera Eidelman*
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Tel: 212-549-2500
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*
Caroline Wilson Palow*
Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom
Tel: +44 (0)203-422-4321
scarlet@privacyinternational.org

.

*Not yet admitted in this District.

†Application for student practice pursuant to L. Civ. R. 83.6 forthcoming.

Dated: December 21, 2018
Buffalo, New York