ARIANNA DEMAS (*pro hac vice* application forthcoming)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Telephone: 212-549-2500
Fax: 212-549-2652
ademas@aclu.org

JENNIFER STISA GRANICK (CA Bar No. 168423)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
Telephone: 415-343-0758
Fax: 415-255-1478
jgranick@aclu.org

JACOB A. SNOW (CA Bar No. 270988)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Telephone: 415-621-2493
Fax: 415-255-1478
jsnow@aclunc.org

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO-OAKLAND DIVISION

AMERICAN CIVIL LIBERTIES UNION FOUNDATION,

Plaintiff,

v.

DEPARTMENT OF JUSTICE and FEDERAL BUREAU OF INVESTIGATION,

Defendants.

No. _____

COMPLAINT FOR INJUNCTIVE RELIEF FOR VIOLATION OF THE FREEDOM OF INFORMATION ACT

INTRODUCTION

1. This is an action under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, to enforce the public's right to information about the Defendant federal agencies' abilities to access encrypted information on electronic devices. Specifically, Plaintiff seeks records reflecting the governing policies and forensic capabilities of an FBI unit, the Electronic Device Analysis Unit ("EDAU").

2. The FBI and other law enforcement agencies have claimed that encryption technology is a significant hindrance in criminal investigations, making many devices inaccessible to law enforcement. In response to that claimed hindrance—which the government has dubbed the "going dark" problem—law enforcement officials have sought to legally require that encryption technologies be circumventable by law enforcement.

3. According to publicly available information, multiple units of Defendant FBI, including the EDAU, already have technical capabilities permitting them to decrypt, unlock, or otherwise access information on secured personal devices.

4. On June 26, 2018, Plaintiff American Civil Liberties Union Foundation (the "ACLU"), submitted a FOIA request ("Request") to Defendants seeking the release of records pertaining to the EDAU. (Exhibit 1). Plaintiff sought expedited processing and a waiver of fees.

5. To date, the Defendants have not released a single responsive record. Indeed, with respect to a number of Plaintiff's requests, Defendants have offered only "Glomar" responses, refusing to even confirm or deny whether responsive records exist at all.

6. Additional information about Defendants' ability to access encrypted information is necessary to better inform the public debate over law enforcement access to encrypted devices. The public interest in the records sought by Plaintiff's requests is clear. Because the government's forensic capabilities are a central aspect of the policy debate over law enforcement access to encrypted communications, the public needs to know about the governing policies and forensic capabilities of relevant FBI units, including the EDAU.

JURISDICTION

7. This Court has subject-matter jurisdiction over this action and personal jurisdiction over the parties pursuant to 5 U.S.C. §§ 552(a)(4)(A)(vii), (4)(B), and (6)(E)(iii). The Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1331 and 5 U.S.C. §§ 701–06.

VENUE AND INTRADISTRICT ASSIGNMENT

8. Venue is proper in this district under 5 U.S.C. § 552(a)(4)(B) because agency records are situated in this district.

9. Pursuant to Local Rules 3-2(c) and (d), assignment to the San Francisco or Oakland division is proper because a substantial portion of the events giving rise to this action occurred in this district and division.

PARTIES

10. Plaintiff American Civil Liberties Union Foundation is a non-profit, non-partisan 501(c)(3) organization dedicated to the principles of liberty and equality and to ensuring that the government complies with the Constitution and laws of the United States. It educates the public about civil liberties and employs lawyers who provide legal representation free of charge in cases involving civil liberties. It is also committed to 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. Obtaining information about government activity, analyzing that information, and widely publishing and disseminating it to the press and the public (in both its raw and analyzed form) are critical and substantial components of its work.

11. Defendant Department of Justice ("DOJ") is a department of the Executive Branch of the United States government and is an agency within the meaning of 5 U.S.C. § 552(f)(1). The Office of the Attorney General ("AG") and the Office of the Inspector General ("OIG") are components of DOJ.

12. Defendant Federal Bureau of Investigation ("FBI") is a component of DOJ and is an agency within the meaning of 5 U.S.C. § 552(f)(1). The Office of Information Policy ("OIP"), which handled the administrative appeals of the FBI Requests, is also a component of DOJ.

FACTUAL BACKGROUND

13. There is a vigorous public policy debate over whether the FBI and other law enforcement agencies need certain technological capabilities for investigations and prosecutions of criminal activity. High-ranking officials in those agencies have claimed for years that criminals are using strong encryption and other security measures to dangerously frustrate information gathering in criminal investigations. They have dubbed this the "going dark" problem. Charlie Savage, *Justice Dept. Revives Push to Mandate a Way to Unlock Phones*, N.Y. Times (Mar. 24, 2018), https://www.nytimes.com/2018/03/24/us/politics/unlock-phones-encryption.html. Some government officials have pushed for a technical mechanism that would guarantee law enforcement access to encrypted communications—an "encryption backdoor."

14. The public needs more information about the FBI's capabilities to unlock, decrypt, or otherwise access information on personal devices to better inform the debate over encryption backdoors and the proper scope of law enforcement access to information stored on encrypted devices.

15. The public record indicates that the EDAU, a unit of the FBI, has these capabilities.

16. According to the agency, the EDAU is tasked with "perform[ing] forensic extractions and advanced data recovery on locked and damaged devices." FBI, *Supervisory Electronics Engineer, GS (FBI Employees Only) Job*, Lensa (Aug. 9, 2020), https://lensa.com/supervisory-electronics-engineer-gs-fbi-employees-only-jobs/lenexa/jd/6b56ed0fdf09bfd64ffb51238f80311c. Additional public information sheds some more light on the agency's tasks and mission. An order issued by the Honorable Jeffrey S. White, District Court Judge of the Northern District of California, concerning law enforcement access to a cellphone indicates that, as of February 5, 2018, the EDAU was capable of bypassing encryption and enabling access to the contents of a cellphone. Order Denying Def.'s Mot. to Suppress at 3–4, *United States v. Conerly*, No. 17-CR-00578 (N.D. Cal. May 30, 2018), ECF No. 43, *available at* https://www.documentcloud.org/documents/4490173-Order-on-Motion-to-

Suppress.html (Exhibit 2). The order indicates that the FBI Special Agent investigating the case submitted a "Mobile Device Unlock Request" to the EDAU after the Regional Computer Forensics Laboratory in Menlo Park, California, was unable to bypass the password security feature on the phone. The EDAU is apparently capable of doing so, since it reported to the agent that if the phone was encrypted, it would "further slow," but not stop, "the retrieval process." *Id.*

17. Other public sources also indicated that the EDAU has acquired and/or is in the process of acquiring technology that allows it to decrypt, unlock, or otherwise access information on secured personal devices. For example, the FBI issued a public call for bids to provide a "GreyKey GreyShift Forensic Workstation" for the EDAU.[1] *GreyKey Forensic Extraction Systems*, GovTribe, https://govtribe.com/opportunity/federal-contract-opportunity/greykey-forensic-extraction-systems-djf181800pr0006154 (March 8, 2018, 11:49 AM); *see also* FBI, *Request for Quotation*, GovTribe (March 8, 2018), https://govtribe.com/file/government-file/djf181800pr0006154-djf-18-1800-pr-0006154-rfq-dot-pdf. GrayKey is a forensic software tool that acquires and searches data stored on Apple smartphones and tablets. FBI, *Justification for Limited Competition/Simplified Acquisition* 1 (2018), https://govtribe.com/file/government-file/djf181800pr0005744-greykey-justification-djf-18-1800-pr-0005744-redacted-dot-pdf ("GreyKey [sic] . . . provides native support to acquire, search, parse and present relevant data from iOS devices (iPhone, iPad, etc.)."). The FBI expects that the number of examiners that use the GrayKey GrayShift software will grow. *Id.* Finally, the bid mentions the FBI's interest in and acquisition of similar products. Since not all mobile devices are covered by each forensic analysis solution, "it takes several products, like GreyShift/GreyKey [sic], to ensure mission success"—*i.e.*, that the agency can access information on mobile devices. *Id.* It appears that on April 19, 2018, the contract was awarded to GrayShift, LLC. FBI, *GreyShift GreyKey Forensic Extraction Systems*, GovTribe, https://govtribe.com/opportunity/federal-contract-

[1] The FBI consistently refers to the company and program as "GreyKey GreyShift," but the proper spelling is "GrayKey GrayShift."

opportunity/greyshift-greykey-forensic-extraction-systems-djf181800pr0005744 (March 18, 2018, 11:49 AM).

18. In addition to obtaining GrayKey GrayShift software, in March of 2017, the EDAU sought a contract with Checkpoint Technologies for service on its InfraScan 300TD. *Checkpoint Technologies, L.L.C.*, GovTribe, https://govtribe.com/vendors/checkpoint-technologies-llc-3c3k4 (last visited Dec. 18, 2020). Checkpoint Technologies was awarded the contract for $155,400. *Purchase Order DJF171200P0000647*, GovTribe, https://govtribe.com/award/federal-contract-award/purchase-order-djf171200p0000647 (Dec. 4, 2020). While the Checkpoint website no longer mentions the InfraScan300TD, the website describes its apparent successor, the InfraScan 400TDM. The InfraScan technology appears to permit detailed microscopic views of electronics hardware in a way that could assist investigators with determining secret encryption keys stored on hardware like the Apple iPhone. Eric Limer, *The Last-Ditch Method the FBI Could Use to Break Into That iPhone Without Apple's Help*, Popular Mechanics (Feb. 22, 2016), https://www.popularmechanics.com/technology/gadgets/a19538/fbi-could-use-decapping-to-access-san-bernardino-phone-data/.

19. In addition to these examples of the EDAU acquiring technology that enables the FBI to access encrypted personal devices, a public FBI job posting explicitly states that the unit extracts data from such locked devices. The posting is for an open position for a "Supervisory Electronics Engineer" for the EDAU, posted August 9, 2020. The position requires a degree in "professional engineering" (or adequate experience in engineering), and some of the major duties of the role include: "Perform[ing] forensic extractions and advanced data recovery on locked and damaged devices which are both commercially available as well as custom one-off electronic devices"; "Work[ing] on the development and application of advanced engineering tools and techniques to execute the mission of the Electronic Device Analysis Unit (EDAU);" and "Coordinat[ing] and plan[ning] with EDAU's Senior Technical Director to ensure continuity of EDAU technical functions." FBI, *Supervisory Electronics Engineer, GS (FBI Employees Only)*

Job, Lensa (Aug. 9, 2020), https://lensa.com/supervisory-electronics-engineer-gs-fbi-employees-only-jobs/lenexa/jd/6b56ed0fdf09bfd64ffb51238f80311c.

The ACLU's FOIA Request

20. On June 26, 2018, the ACLU submitted its FOIA Request to the AG's office, OIG, and the FBI, seeking the release of five categories of records pertaining to the EDAU:

(1) Any records concerning policies applicable to the EDAU;

(2) Any records concerning the EDAU's technological capabilities to unlock, search, or otherwise access electronic devices, including user interface automation, debugging tools, reverse engineering tools, fault injection systems, decapping or semiconductor lapping systems, laser or electron microscopy or other imaging machinery, electrical or optical probes, and/or parallel computing or supercomputing clusters used for automated search such as key recovery or password cracking;

(3) Any records concerning the EDAU's requests for, purchases of, or uses of technology, systems, or services described using terms such as "Network Investigation Technique" or "NIT," "Computer Network Exploitation" or "CNE," "Computer and Internet Protocol Address Verifier" or "CIPAV," "Internet Protocol Address Verifier" or "IPAV," "Remote Access Search and Surveillance" or "RASS," "Remote Computer Search," "Remote Access Search," "Remote Search," "Web Bug," "Sniffer," "Computer Tracer," "Internet Tracer," "Remote Computer Trace," "lawful access," or "forensic analysis";

(4) Any records concerning the EDAU's requests for, purchases of, or uses of equipment, software, services, and/or technology for conducting remote searches or bypassing encryption or other security measures, including but not limited to: Remote Control System a.k.a. RCS or Galileo (marketed by Hacking Team); Finfisher, FinFisher Relay, FinSpy, and FinFly (marketed by Lench IT Solutions); Pegasus (marketed by NSO Group), and various tools marketed by VUPEN

Security. *See, e.g.*, *The Surveillance Catalog: How Government Gets Their Tools*, Wall St. J., last updated Feb. 7, 2012, https://graphics.wsj.com/surveillance-catalog/; and/or

(5) Any records concerning inspector general or other investigations of the EDAU.

21. The ACLU sought expedited processing of the Request on the basis that the ACLU is primarily engaged in disseminating information, and the records are urgently needed to inform the public about actual or alleged federal government activity. *See* 5 U.S.C. § 552(a)(6)(E)(v); 6 C.F.R. § 5.5(e) (2020); 28 C.F.R. § 16.5(e) (2020); 22 C.F.R. § 171.11(f) (2020).

22. The ACLU also sought a waiver of document search, review, and duplication fees on the grounds that disclosure of the requested records is in the public interest because it is "likely to contribute significantly to public understanding of the operations or activities of the government" and is not in the ACLU's commercial interest. *See* 5 U.S.C. § 552(a)(4)(A)(iii); 6 C.F.R. § 5.11(k) (2020); 28 C.F.R. § 16.10(k) (2020); 22 C.F.R. § 171.16 (2020). The ACLU further sought a fee waiver because it qualifies as a "representative of the news media" and the records are not for commercial use. *See* 5 U.S.C. § 552(a)(4)(A)(ii)(II); 6 C.F.R. § 5.11(d)(1) (2020); 28 C.F.R. § 16.10(b)(6) (2020); 22 C.F.R. § 171.14(b) (2020).

23. None of the Defendants have released any responsive records. Plaintiff requests that this Court order the AG and OIG to conduct a comprehensive search and release all responsive records; order that the FBI process and release records responsive to FBI Requests 1 and 4 (as described below); and overturn the administrative appeals decisions as to FBI Requests 2 and 3. Plaintiff does not challenge the FBI's handling of Request 5.

Office of the Attorney General

24. By letter dated July 5, 2018, the AG's office acknowledged receipt of the Request. In the same letter, the AG's office denied the ACLU's request for expedited processing and deferred a decision on the request for a fee waiver.

25. The July 5, 2018 letter asserted that due to "unusual circumstances," the AG's office would need to extend the time limit to respond to the Request beyond the additional ten-day extension provided in the FOIA. *See* 5 U.S.C. § 552(a)(6)(B)(i)–(iii).

26. To date, over two years since the ACLU submitted the Request, the AG's office has neither released responsive records nor explained its failure to do so.

Office of the Inspector General

27. To date, OIG has not acknowledged receipt of the Request, released any responsive records, or explained its failure to do so.

Federal Bureau of Investigation

28. By letter dated July 5, 2018, the FBI acknowledged receipt of the Request.

29. By letter dated October 11, 2018, the FBI divided the five numbered items in the Request into five distinct requests for "administrative tracking purposes." The FBI assigned additional Freedom of Information/Privacy Act ("FOIPA") tracking numbers to each of the items requested: FOIPA Request No. 1411153-000 addresses numbered item 1 in the initial Request ("FBI Request 1"); FOIPA Request No. 1418450-0 addresses numbered item 2 in the initial Request ("FBI Request 2"); FOIPA Request No. 1418454-0 addresses numbered item 3 in the initial Request ("FBI Request 3"); FOIPA Request No. 1418456-0 addresses numbered item 4 in the Request ("FBI Request 4"); and FOIPA Request No. 1418457-0 addresses numbered item 5 in the Request ("FBI Request 5").

30. By letter dated February 4, 2019, the FBI responded to FBI Request 1 by stating "[y]our request is overly broad and it does not comport with the requirements of 28 C.F.R. § 16.3(b), as it does not provide enough detail to enable personnel to locate records 'with a reasonable amount of effort.'"

31. By letter dated February 4, 2019, the FBI responded to FBI Request 2 by stating that, "pursuant to FOIA exemption (b)(7)(E) [5 U.S.C. § 552(b)(7)(E)], the FBI neither confirms nor denies the existence of records."

32. By letter dated February 4, 2019, the FBI responded to FBI Request 3 by stating that, "pursuant to FOIA exemption (b)(7)(E) [5 U.S.C. § 552(b)(7)(E)], the FBI neither confirms nor denies the existence of records."

33. By letter dated February 4, 2019, the FBI responded to FBI Request 4 by stating that, "pursuant to FOIA exemption (b)(7)(E) [5 U.S.C. § 552(b)(7)(E)], the FBI neither confirms nor denies the existence of records."

34. By letter dated February 4, 2019, the FBI responded to FBI Request 5 by stating "[w]e were unable to locate records responsive to your request."

35. By letter dated March 26, 2019, the ACLU administratively appealed the FBI's determinations as to FBI Requests 1–5, as well as the FBI's denial of expedited processing. In the same letter, the ACLU presented evidence as to why the Glomar responses were unjustified because the FBI failed to adequately explain its responses and were implausible because of the public information already available about the EDAU. The also ACLU requested expedited processing on all five appeals.

36. By email on March 29, 2019, the DOJ Office of Information Policy acknowledged receipt of the ACLU's five administrative appeal and denied the ACLU's request for expedited processing of the appeals. In that same email, OIP assigned appeal tracking numbers to each request as follows: DOJ-AP-2019-003224 (FBI Request 1); DOJ-AP-2019-003360 (FBI Request 2); DOJ-AP-2019-003361 (FBI Request 3); DOJ-AP-2019-003362 (FBI Request 4); and DOJ-AP-2019-003363 (FBI Request 5).

37. By email dated April 15, 2019, the Office of Information Policy affirmed the FBI's action as to FBI Request 5.

38. By email dated June 17, 2019, the Office of Information Policy affirmed the FBI's action as to FBI Request 3.

39. By email dated August 22, 2019, the Office of Information Policy affirmed the FBI's action as to FBI Request 2.

40. By email dated September 18, 2019, the Office of Information Policy reversed the FBI's action as to FBI Request 4, remanding the request to the FBI for further processing. Specifically, the Office of Information Policy reversed "the FBI's refusal to confirm or deny the existence of records responsive to [the] request."

41. By email dated November 21, 2019, the Office of Information Policy reversed the FBI's action as to FBI Request 1, remanding the request to the FBI for further processing. Specifically, the Office of Information Policy reversed "the FBI's determination that [the] request was not reasonably described."

42. By letter dated July 1, 2020, the FBI acknowledged the remanded appeal of FBI Request 4.

43. By letter dated July 1, 2020, the FBI acknowledged the remanded appeal of FBI Request 1.

44. To date, the ACLU has received no further response to remanded appeals of FBI Requests 1 and 4.

CAUSES OF ACTION

45. Defendants' failure to make a reasonable effort to search for records sought by the Request violates the FOIA, 5 U.S.C. § 552(a)(3), and Defendants' corresponding regulations.

46. Defendants' failure to timely respond to the Request violates the FOIA, 5 U.S.C. § 552(a)(6)(A), and Defendants' corresponding regulations.

47. Defendants' failure to process the Request expeditiously and as soon as practicable violates FOIA, 5 U.S.C. § 552(a)(6)(E), and Defendants' corresponding regulations.

48. Defendants' failure to make promptly available the records sought by the Request violates the FOIA, 5 U.S.C. § 552(a)(3)(A), and Defendants' corresponding regulations.

49. The failure of Defendants to grant Plaintiff's request for a limitation of fees violates the FOIA, 5 U.S.C. § 552(a)(4)(A)(iii), and Defendants' corresponding regulations.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court:

1. Order Defendants to conduct a thorough search for all responsive records;

2. Order Defendant DOJ to immediately process and release all records responsive to the Request directed to the AG's office and OIG;

3. Order Defendant FBI to immediately process and release all records responsive to FBI Requests 1, 2, 3, and 4.

4. Enjoin Defendants from charging Plaintiff search, review, or duplication fees for the processing of the Request and FBI Requests 1–5;

5. Award Plaintiff its costs and reasonable attorneys' fees incurred in this action; and

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

Respectfully submitted,

DATED: December 22, 2020

/s/ *Jennifer Stisa Granick*
Arianna Demas (*pro hac vice* application forthcoming)
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Telephone: 212-549-2500
Fax: 212-549-2652
ademas@aclu.org

Jennifer Stisa Granick
American Civil Liberties Union Foundation
39 Drumm Street
San Francisco, CA 94111
Telephone: 415-343-0758
Fax: 415-255-1478
jgranick@aclu.org

Jacob Snow
American Civil Liberties Union Foundation of Northern California
39 Drumm Street
San Francisco, CA 94111
Telephone: 415-621-2493

Fax: 415-255-1478
jsnow@aclunc.org

Attorneys for Plaintiff