IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

THE ASSOCIATED PRESS;
450 West 33rd Street
New York, NY 10001

GANNETT SATELLITE INFORMATION NETWORK LLC d/b/a USA TODAY;
7950 Jones Branch Drive
McLean, VA 22108

and VICE MEDIA LLC,
49 South 2nd Street
Brooklyn, NY 11249

Plaintiffs,

v.

FEDERAL BUREAU OF INVESTIGATION,
935 Pennsylvania Avenue, NW
Washington, D.C. 20535-0001

Defendant.

Case No. 16-cv-1850

COMPLAINT

Plaintiffs The Associated Press ("AP"), Gannett Satellite Information Network LLC d/b/a USA TODAY ("USA TODAY"), and Vice Media, LLC ("Vice") (together, "News Organizations"), by and through their undersigned attorneys, allege:

1. This action is brought pursuant to the Freedom of Information Act ("FOIA"), 5 U.S.C. §§ 552, *et seq.*, for basic contracting information from the Federal Bureau of Investigation ("FBI") regarding one of its most publicly-discussed and controversial acquisitions: a technological tool openly purchased from a third-party vendor that was used to circumvent the

need for a court order to access the locked iPhone of Syed Rizwan Farook, one of the perpetrators of the mass killings in San Bernardino, California. Mr. Farook and his wife were both killed in the attack, appear to have acted alone, and investigators long ago stated that they had uncovered no connection between the shooters and any foreign terrorist groups.[1] The News Organizations seek injunctive and other appropriate relief, including release of agency records from the FBI.

2. More specifically, through this action, the News Organizations seek to compel the FBI to provide records of the publicly-acknowledged business transaction that resulted in the purchase this March of the so-called iPhone access tool. The public interest in receiving this information is significant. The FBI's purchase of this tool allowed government access to Mr. Farook's phone, providing new information about one of the deadliest attacks on American soil in recent years, but also apparently failing to reveal any evidence of links between Mr. Farook and foreign terrorists or terrorist organizations.[2] At the same time, the tool sparked tremendous nationwide debate about both the proper balance between national security and privacy in personal communications, and the degree to which law enforcement should be empowered to compel access to encrypted and protected devices.[3] FBI Director James Comey has himself stressed the essential importance of a nationwide "adult conversation" about whether and when

---

[1] *See* Doug Stanglin and Kevin Johnson, *FBI: No evidence San Bernardino killers were part of a cell*, USA TODAY (Dec. 5, 2015), *available at*: http://www.usatoday.com/story/news/nation/2015/12/04/suspects-family-shocked-killings/76773382/.

[2] *See, e.g.* Ellen Nakashima and Adam Goldman, *No links to foreign terrorists found on San Bernardino iPhone so far, officials say*, The Wash. Post (Apr. 14, 2016), *available at* https://www.washingtonpost.com/world/national-security/no-links-to-foreign-terrorists-found-on-san-bernardino-iphone-so-far-officials-say/2016/04/14/f1aa52ce-0276-11e6-9203-7b8670959b88_story.html.

[3] *See, e.g.*, Elizabeth Weise, *Apple v. FBI timeline: 43 days that rocked tech*, USA TODAY (Mar. 30, 2016) (collecting coverage and summarizing history of debate), *available at* http://www.usatoday.com/story/tech/news/2016/03/15/apple-v-fbi-timeline/81827400/.

law enforcement should be able to access encrypted devices because, "'We've got to get to a point where we can reach [wrongdoers] as easily as they can reach us and change behavior by that reach-out.'"[4] Mr. Comey also noted the need for increased information sharing with the public, an acknowledgment particularly critical given the potential of future legislative action on this issue, noting, "'We need to understand in the FBI, how is this exactly affecting our work, and then share that with folks.'"[5]

3. Moreover, the FBI's purchase of the technology – and its subsequent verification that it had successfully obtained the data it was seeking thanks to that technology – confirmed that a serious undisclosed security vulnerability existed (and likely still exists) in one of the most popular consumer products in the world.[6] And in order to exploit that vulnerability, the FBI contracted with an unidentified third-party vendor, effectively sanctioning that party to retain this potentially dangerous technology without any public assurance about what that vendor represents, whether the vendor has adequate security measures, whether the vendor is a proper recipient of government funds, or whether it will act only in the public interest.

4. Information about the FBI's contracting arrangement would also ensure transparency about the expenditure of public funds. Understanding the amount that the FBI deemed appropriate to spend on the tool, as well as the identity and reputation of the vendor it did business with, is essential for the public to provide effective oversight of government

[4] *See*, Eric Tucker, *Comey: FBI wants 'adult conversation' on device encryption*, The Associated Press (Aug. 30, 2016), *available at*: http://bigstory.ap.org/article/7d57f576e3f74b6ca4cd3436fbebf160/comey-fbi-wants-adult-conversation-device-encryption.
[5] *Id.*
[6] *See, e.g.*, Tami Abdollah, *FBI continues to debate sharing iPhone hack with Apple*, The Associated *Press* (Apr. 7, 2016), *available at* http://bigstory.ap.org/article/7672f8a300f542baaa35a2a237820ec1/fbi-debates-sharing-iphone-hacking-details-apple.

functions and help guard against potential improprieties. Further, the public is entitled to know the nature of the vendors the Government finds it necessary to deal with in cases of access to private information, including whether or not the FBI feels compelled to contract with groups of hackers with suspect reputations, because it will inform the public debate over whether the current legislative apparatus is sufficient to meet the Government's need for such information.

PARTIES

5. Plaintiff The Associated Press is a not-for-profit cooperative whose members are U.S. newspapers and broadcasters. AP is one of the oldest and most trusted newsgathering organizations in the world, with more than one billion readers, listeners, and viewers. AP's headquarters are at 450 West 33rd Street, New York, NY 10001.

6. Plaintiff USA TODAY is the nation's largest-selling daily newspaper and USATODAY.com is one of the top newspaper sites on the Internet. USA TODAY's headquarters are at 7950 Jones Branch Drive, McLean, VA 22108.

7. Plaintiff Vice Media LLC is a preeminent news organization, youth media company, and content creation studio. Vice operates in over 30 countries, and includes a network of digital channels, a weekly and daily news programming partnership, a television and feature film production studio, a magazine, a book-publishing division, and a television network. Vice's headquarters are at 49 South 2nd Street, Brooklyn, NY 11249.

8. Defendant Federal Bureau of Investigation is an agency of the federal government within the meaning of 5 U.S.C. § 552(f)(1) that has possession, custody and/or control of the records that the News Organizations seek. The FBI is headquartered at 935 Pennsylvania Avenue, NW, Washington, D.C. 20535-0001.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action and personal jurisdiction over the FBI pursuant to 28 U.S.C. § 1331 and 5 U.S.C. § 552(a)(4)(B).

10. Venue is proper in this district pursuant to 5 U.S.C. § 552(a)(4)(B).

11. The News Organizations each have exhausted all administrative remedies available in regard to the requests at issue. The FBI denied each of the News Organizations' timely-filed administrative appeals in their entirety, and therefore the News Organizations are entitled to seek judicial review of those denials pursuant to 5 U.S.C. § 552(a)(4)(B).

FACTS

A. Background

12. On December 2, 2015, 14 people were killed and 22 people were seriously injured when Mr. Farook, a county government employee, and his wife, Tashfeen Malik, opened fire on innocent civilians at the Inland Regional Center in San Bernardino, California. The attack was defined as an act of terrorism by President Barack Obama, and evidence emerged that Ms. Malik had sworn allegiance to the Islamic State prior to the attack. Both Mr. Farook and Ms. Malik were subsequently killed by police, and the FBI soon announced that it had uncovered no evidence linking them to foreign terrorist organizations. The mass killing captured significant national attention, particularly in light of the seemingly random and vulnerable civilian targets and the outwardly normal lives led by the perpetrators. The documents sought by the FOIA requests at issue here relate to reporting done by the News Organizations in the aftermath of that attack, and to the subsequent counter-terrorism investigation opened by the FBI.

13. Not long after the FBI had begun its investigation, the agency's director, James Comey, told a Senate panel on February 9, 2016, that the agency was unable to access one of

Mr. Farook's Apple iPhones due to its security and encryption technology. Because the FBI regarded the information contained on the phone as potentially important to its investigation, it asked Apple for its assistance to create software that would allow the phone's security features to be disabled. When Apple declined, the FBI took the unique step of obtaining a federal court order under the All Writs Act directing the company to assist the agency in obtaining access to the phone. When Apple again refused, the Government moved to compel Apple to do so. *See* Government's Motion to Compel Apple to Comply, *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, No. 5:16-cm-10-SP ("All Writs Act Proceeding") (C.D. Cal. Feb. 19, 2016), Dkt. No. 1 .

14. The public debate over whether Apple should be compelled to assist the FBI was intense and extensive. At issue was not only whether the FBI would be able to adequately obtain evidence to fully investigate an act of terrorism, but also whether a private company should be required to create the means to circumvent its own security protections to further that investigation. Apple, for instance, argued that any tool allowing such a circumvention would inevitably compromise the security of all of its iPhone customers, and would create an undesirable precedent that would invite repeated requests for such circumventions in untold numbers of future investigations, diminishing the value of personal security and privacy.

15. As this public debate intensified, the Government unexpectedly moved to continue the proceedings on the motion to compel. In its court filing, the Government represented that "an outside party demonstrated to the FBI a possible method for unlocking Farook's iPhone. Testing is required to determine whether it is a viable method that will not compromise data on Farook's iPhone. If the method is viable, it should eliminate the need for

the assistance from Apple … set forth in the All Writs Act Order in this case." All Writs Act Proceeding, Dkt. No. 191 at 3. On March 28, 2016, the Government confirmed it was able to access Farook's iPhone data, and the original Order directing Apple to assist the FBI was vacated the next day. All Writs Act Proceeding at Dkt. Nos. 209, 210. The Government has not identified or provided any detailed information about this third party, which presumably still possesses the technology to exploit a major iPhone security vulnerability, and which was presumably approved as an appropriate vendor for the receipt of Government funds.

16. Not long after the FBI gained access to the iPhone, federal law enforcement officials confirmed that the data contained within Mr. Farook's iPhone revealed no links to foreign terrorist organizations. It appears that the access tool in this case is no longer in active use, and the FBI has already obtained whatever data it originally sought.

B. Subsequent Official Disclosures

17. While the Government's statements in the All Writs Act Proceeding regarding the method used to unlock Mr. Farook's phone were somewhat cryptic, the FBI's director soon began publicly confirming significant details about the technological tool it had obtained, commenting on, among other matters, the financial cost of the tool and the structure of the specific deal the FBI entered into with the vendor to obtain it. Mr. Comey similarly suggested publicly that the tool was not then being used in *any* other investigations, and that a chief reason why the FBI did not want to disclose more information was to ensure that it would be able to drive a good bargain in potential future technology purchasing negotiations. Mr. Comey has not explained how the FBI vetted the vendor from which it purchased the tool, why the FBI regards the vendor as an appropriate one, or whether that vendor can itself resell the technology to foreign governments, or terrorist or criminal organizations.

18. On April 21, 2016, Mr. Comey was asked about the cost of the tool by Brooke Masters of the Financial Times. Mr. Comey responded, "A lot… More than I will make in the remainder of this job, which is seven years and four months, for sure." Mr. Comey continued that this payment was, "in my view, worth it, because it's a tool that helps us with a 5C running iOS9." This statement set off a flurry of news reports, which estimated, based on Mr. Comey's publicly-available salary data, a sales price between $1 million and $1.3 million.[7]

19. At a briefing with reporters on May 11, 2016, Mr. Comey revealed other key details of the agreement to obtain the tool:[8]

a. **Cost:** In response to a question about the cost of the tool, Mr. Comey responded: "I probably shouldn't have been cute trying to estimate for you how much it costs. It costs a lot of money. . . . In my view it was well worth it."

b. **Lack of Use in Other Cases:** In response to a question of whether the tool had been used in other cases, Mr. Comey responded: "I don't think we have yet. We're trying to figure out a mechanism where we can use the tool to help in other investigations. Again, it's a narrow thing which is a 5C operating at on an iOS 9 system. We're trying to figure out how we can help state and local law enforcement, if they have a court order. How we can do that and still maintain the viability of the tool. That work is underway right now. I expect in the near future we'll have figured out how we're going to do it. Then we'll tell law enforcement, 'If you send us a phone here are the rules.' Look, I want to make sure that if there are ways to use it in appropriate cases we do, but I don't think we've used it yet."

c. **Structure of the Purchasing Agreement:** In response to a question about whether the FBI was avoiding an internal government process (called "VEP")

---

[7] *See, e.g.*, Joshua Kopstein, *FBI Director: We Paid More Than $1.2 Million for San Bernardino iPhone Hack*, Vice Motherboard (Apr. 21, 2016), *available at* http://motherboard.vice.com/read/fbi-director-we-paid-more-than-1-2-million-for-san-bernardino-iphone-hack; *FBI head suggests agency paid more than $1M to access iPhone*, The Associated Press (Apr. 21, 2016), *available at* http://bigstory.ap.org/article/3540c3cb330e4c50a8c4c7f841d383b4/fbi-head-suggests-agency-paid-more-1m-access-iphone.

[8] *See Director Comey Remarks During May 11 'Pen and Pad' Briefing with Reporters*, FBI Press Release, *available at* https://www.fbi.gov/news/pressrel/press-releases/director-comey-remarks-during-may-11-2018pen-and-pad2019-briefing-with-reporters.

for vetting whether security vulnerabilities discovered by government agencies should be disclosed to companies for public security reasons by purchasing only a tool, as opposed to the details of the security vulnerability information itself, Mr. Comey responded: "Sometimes you can buy the guts of the tool, right? The software behind it, the code behind it. There's a difference between those two things. Our goal, I know you've all heard me say this many times, the goal in San Bernardino was to investigate the case and get into that phone. We bought what was necessary to get into that phone. We tried not to spend more money than we needed to spend, but we spent the money we needed to to get into that phone. We did not in any form or fashion, structure the transaction of the thing with an eye towards avoiding the VEP. I would be shocked if anybody even thought about the VEP or the VEP at the time this was going on. We bought what we needed to buy, to get into the phone."

d. **Reason for Not Specifying Amount Paid:** In response to a question about why Mr. Comey would not be more precise about the cost of the tool, Mr. Comey responded: "A variety of reasons that I don't want to get into. I'm not comfortable giving you the precise number." Comey later added that "I don't want to waste your tax payers money," presumably by revealing a price point for future negotiations with other companies.

e. **Complete Absence of Target Investigations That Would Use Technology:** In response to a question about how widely the tool could be used on other types of phones, Mr. Comey responded: "My recollection is we're highly confident that it works only on a 5C, running on iOS9." When asked whether any of the roughly 500 additional phones the FBI has identified as important to other investigations but which are currently locked and inaccessible are iPhone 5Cs running iOS9, Mr. Comey responded: "I think, and you can get the answer on this, I think the answer is none. I don't think any in that set … I think that's right."

C. The USA TODAY Request

20. On March 29, 2016, the day after the All Writs Act Order was vacated, USA TODAY reporter Brad Heath filed a FOIA request (the "USA TODAY Request") with the FBI seeking "[c]omplete copies of any records memorializing agreements or expenditures to the 'outside party' that assisted the FBI in unlocking Syed Rizwan Farook's iPhone." The USA TODAY Request sought only the agreements or expenditure records themselves, not the actual content of the purchased technology.

21. On June 6, 2016, the FBI denied the USA TODAY Request. The FBI stated that it had located responsive records, but that it would withhold those records from disclosure. Specifically, the FBI cited FOIA Exemption 7(A), 5 U.S.C. § 552(b)(7)(A), which permits agencies to withhold "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information … could reasonably be expected to interfere with enforcement proceedings." Rather than explain the basis of its decision to invoke this exemption, the FBI instead merely reiterated the statutory standards by way of analysis: "The records responsive to your request are law enforcement records; there is a pending or prospective law enforcement proceeding relevant to these responsive records, and release of the information in these responsive records could reasonably be expected to interfere with enforcement proceedings."

22. On June 20, 2016, USA TODAY timely appealed the denial, arguing that the FBI had applied Exemption 7(A) in violation of the law.

23. On September 2, 2016, the FBI, through the Department of Justice Office of Information Policy, summarily denied the appeal citing Exemption 7(A).

D. <u>The AP Request</u>

24. On April 21, 2016, AP reporter Eric Tucker filed a FOIA request (the "AP Request") with the FBI for records functionally identical to those requested by USA TODAY. The AP Request sought: (i) "Any FBI contract, request for proposal, written arrangement or business transaction, signed between the dates of March 20, 2016 and March 22, 2016, for technology used to unlock the iPhone 5C used by Syed Rizwan Farook"; and (ii) "Alternatively, any record of payment, receipt, etc., that the FBI or U.S. government or any entity acting on its behalf made for [the] technique." As with the USA TODAY Request, the AP Request sought

only the financial agreements underlying the business transaction to obtain the technology, not the details of the technology itself.

25. On May 11, 2016, the FBI denied the AP Request. The FBI stated that it had located responsive records, but that it would withhold those records from disclosure. Specifically, the FBI cited Exemption 7(A). Rather than explain the basis of its decision to invoke this exemption, the FBI instead merely reiterated the statutory standards by way of analysis: "The records responsive to your request are law enforcement records; there is a pending or prospective law enforcement proceeding relevant to these responsive records, and release of the information in these responsive records could reasonably be expected to interfere with enforcement proceedings."

26. On June 1, 2016, the AP timely appealed the denial, arguing that the FBI had applied Exemption 7(A) in violation of the law.

27. On June 6, 2016, the FBI, through the Department of Justice Office of Information Policy, summarily denied the appeal citing Exemption 7(A).

E. <u>The Vice Request</u>

28. On April 21, 2016, Vice reporter Jason Leopold filed a FOIA request (the "Vice Request") with the FBI for "A copy of financial documents, including approval forms, decision analysis memorandum, authorization documents, copies of any and all electronic check transfers, associated with the payment made by the FBI for technical assistance in accessing an iPhone that was allegedly owned by one of the suspects in the San Bernardino shooting last year."[9]

[9] For the purposes of this litigation, Vice has limited the scope of its Request to solely those records also responsive to the USA TODAY Request and the AP Request.

29. On June 6, 2016, the FBI denied the Vice Request. Specifically, the FBI cited Exemption 7(A), stating that it could not turn over responsive records because they are located in an investigative file.

30. On June 13, 2016, Vice timely appealed the denial, arguing that the FBI had applied Exemption 7(A) in violation of the law.

31. On July 22, 2016, the FBI, through the Department of Justice Office of Information Policy, summarily denied the appeal citing Exemption 7(A).

FIRST CAUST OF ACTION
(Violation of FOIA for failure to conduct a reasonable search)

32. The News Organizations repeat, reallege, and incorporate the allegations in the foregoing paragraphs as though fully set forth herein.

33. The FBI is an agency subject to FOIA, 5 U.S.C. § 552(f), and therefore had an obligation to conduct a search reasonably calculated to uncover all records responsive to the three Requests.

34. On information and belief, the FBI's limited search of its records was legally inadequate, and as a result the FBI has manifestly failed to satisfy its obligations to diligently search for responsive records under FOIA, 5 U.S.C. § 552(a)(3).

SECOND CAUSE OF ACTION
(Violation of FOIA for failure to make records available)

35. The News Organizations repeat, reallege, and incorporate the allegations in the foregoing paragraphs as though fully set forth herein.

36. The FBI is an agency subject to FOIA, 5 U.S.C. § 552(f), and therefore must disclose in response to a FOIA request all responsive records in its possession at the time of the

Request that are not specifically exempt from disclosure under FOIA, and must provide a lawful reason for withholding any records as to which it is claiming an exemption.

37. The News Organizations have exhausted all administrative remedies, having filed administrative appeals that were denied. The News Organizations are therefore entitled to seek judicial review of those denials pursuant to 5 U.S.C. § 552(a)(4)(B).

38. There is no lawful basis under FOIA for the FBI's denial of the three Requests that are the subject of this action, and its withholding of the responsive documents identified in connection with those Requests is unlawful in violation of FOIA.

39. Even if parts of the requested documents are properly subject to an exemption, the FBI has an obligation to redact non-exempt portions of the documents and release those portions that are non-exempt under FOIA.

40. Accordingly, the News Organizations are entitled to an order compelling the FBI to produce the records sought by the Requests.

REQUEST FOR RELIEF

WHEREFORE, the News Organizations respectfully request that this Court:

a. Declare that the records sought by the three Requests, as more particularly described above, are public records pursuant to 5 U.S.C. § 552, and that the records must be disclosed;

b. Order that the FBI conduct an adequate search for the requested records;

c. Order the FBI to provide those records to the News Organizations, including electronic copies of records stored in electronic format, within 20 business days of the Court's order;

d. Award to the News Organizations the costs of this proceeding, including reasonable attorney's fees, as authorized by FOIA; and

e. Grant to the News Organizations such other and further relief as this Court deems just and proper.

Dated: September 16, 2016
Washington, D.C.

Respectfully submitted,

LEVINE SULLIVAN KOCH & SCHULZ, LLP

By: /s/ Jay Ward Brown

Jay Ward Brown (D.C. Bar No. 437686)
1899 L Street, N.W., Suite 200
Washington, D.C. 20036
Telephone: (202) 508-1136
Fax: (202) 861-9888
E-mail: jbrown@lskslaw.com

Jeremy A. Kutner
(*Pro Hac Vice Application Pending*)
321 West 44th Street, Suite 1000
New York, NY 10036
Telephone: (212) 850-6100
Fax: (212) 850-6299
E-mail: jkutner@lskslaw.com

Counsel for Plaintiffs The Associated Press, USA TODAY, and Vice Media LLC.

Of Counsel:

Karen Kaiser
Brian Barrett
The Associated Press
450 West 33rd Street
New York, NY 10001
Telephone: (212) 621-7547
Fax: (212) 506-6131
E-mail: kkaiser@ap.org
E-mail: bbarrett@ap.org

Barbara Wall
Thomas Curley
Gannett Co., Inc.
7950 Jones Branch Drive
McLean, VA 22107
Telephone: (703) 854-6417
Fax: (703) 854-2031
E-mail: bwall@gannett.com
E-mail: tcurley@gannett.com