

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

ASSOCIATED PRESS, ET AL,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	Civ. Action No. 1:16-cv-01850-TSC
	)	
UNITED STATES DEPARTMENT	)	
OF JUSTICE,	)	
	)	
Defendant.	)	

**SECOND DECLARATION OF DAVID M. HARDY**

I, David M. Hardy, declare as follows:

(1) I am the Section Chief of the Record/Information Dissemination Section (“RIDS”), Records Management Division (“RMD”), in Winchester, Virginia. I have held this position since August 1, 2002. Prior to my joining the Federal Bureau of Investigation (“FBI”), from May 1, 2001 to July 31, 2002, I was the Assistant Judge Advocate General of the Navy for Civil Law. In that capacity, I had direct oversight of Freedom of Information Act (“FOIA”) policy, procedures, appeals, and litigation for the Navy. From October 1, 1980 to April 30, 2001, I served as a Navy Judge Advocate at various commands and routinely worked with FOIA matters. I am also an attorney who has been licensed to practice law in the State of Texas since 1980.

(2) In my official capacity as Section Chief of RIDS, I supervise approximately 251 employees who staff a total of ten (10) Federal Bureau of Investigation Headquarters (“FBIHQ”) units and two (2) field operational service center units whose collective mission is to effectively plan, develop, direct, and manage responses to requests for access to FBI records and

information pursuant to the FOIA as amended by the OPEN Government Act of 2007 and the OPEN FOIA Act of 2009; the Privacy Act of 1974; Executive Order 13,526; Presidential, Attorney General, and FBI policies and procedures; judicial decisions; and Presidential and Congressional directives. My responsibilities also include the review of FBI information for classification purposes as mandated by Executive Order 13,526,<sup>1</sup> and the preparation of declarations in support of Exemption 1 claims asserted under the FOIA. I have been designated by the Attorney General of the United States as an original classification authority and a declassification authority pursuant to Executive Order 13,526, §§ 1.3 and 3.1. The statements contained in this declaration are based upon my personal knowledge, upon information provided to me in my official capacity, and upon conclusions and determinations reached and made in accordance therewith.

(3) Due to the nature of my official duties, I am familiar with the procedures followed by the FBI in responding to Plaintiffs' requests for information from its files pursuant to the provisions of the FOIA, 5 U.S.C. § 552. Specifically, I am aware of the FBI's handling of each of the FOIA requests submitted by the Plaintiffs to FBIHQ, seeking access to records related to the FBI's unlocking of the San Bernardino shooter's iPhone.

(4) This Declaration is being filed to supplement my first declaration justifying the FBI's handling of Plaintiffs' FOIA requests (*See* Docket No. 14, Attachment No. 2) and in response to Plaintiffs' Cross Motion for Summary Judgment. (*See* Docket No. 16.)

#### **PLAINTIFFS' NARROWED CHALLENGES**

(5) In Plaintiffs' Cross Motion for Summary Judgment, Plaintiffs limit their challenges of FBI withholdings to "the identity of and the amount of money paid to the party

---

<sup>1</sup> 75 Fed. Reg. 707 (2010).

that, the FBI has openly acknowledged, sold to the FBI a tool to break the security protections of at least one model of iPhone.” (See Docket No. 16, page 1.). Plaintiff challenges the applicability of the FBI’s assertions of FOIA Exemptions (b)(1), (b)(3), (b)(4), and (b)(7)(E) to withhold this information.

***Protection of the Identity of the Third Party Vendor***

(6) The FBI asserted FOIA Exemptions 1, 3, and 7E, 5 U.S.C. §§ 552 (b)(1), (b)(3), and (b)(7)(E), to protect the identity of the third party vendor because release of this information would reveal classified intelligence activities (including covert action), intelligence sources, or methods (E.O. 13,526, § 1.4(c)); intelligence sources and methods requiring withholding per the National Security Act of 1947 (50 U.S.C. § 3024 (i)(1)); and techniques and procedures for law enforcement investigations, the release of which would allow for circumvention of the law.

Applicability of Exemptions 1, 3, and 7E to Protect the Identity of the Third Party Vendor

(7) Plaintiffs claim the FBI has failed to explain how release of the vendor’s identity “could reasonably be expected to cause identifiable or describable damage to the national security.” (See Docket No. 16, page 12.) In my previous declaration, I explained that I determined the “intelligence activities or methods withheld in this case are still used by and/or useful to the FBI today to gather intelligence information” and “disclosure of this information could reasonably be expected to cause serious damage to national security as it would allow hostile entities to discover the current intelligence gathering methods used, as well as the capabilities and limitations of these methods.” (See Hardy Declaration, ¶36.) I have determined that this holds true in regards to the iPhone unlocking technology obtained by the FBI; the vendor identity is properly classified as it pertains to intelligence sources and method. In order

to fully protect this classified intelligence gathering method, the FBI must continue to protect the identity of the vendor who created the technology.

(8) When creating proprietary software, it is reasonable to assume that software companies are more likely to expand and update previous versions of their existing computer programs rather than start from scratch. For example, when creating operating systems for personal computers (“PCs”), software companies tend to update and modernize their old operating systems rather than create a completely new product; thus, software companies develop programming styles and strategies unique to their own company as they build upon their existing work and develop new products. The same could likely be said for the vendor the FBI has redacted in the responsive documents at issue. Revealing the vendor’s identity immediately provides those wishing to circumvent the iPhone unlocking technology with a body of work from the company (any existing public technology created by the company) to review and probe for possible weaknesses. They may then apply any knowledge gained through such a review to develop exploits for the vendor’s unique product. This could allow them to create better encryption technology, thwart the iPhone unlocking technology currently available to the FBI, and deprive the FBI of a critical classified intelligence source and method.

(9) Additionally, revealing the vendor’s identity immediately exposes the vendor to attacks and infiltration by hostile entities wishing to exploit the technology they provided to the FBI. While FBI computer networks are protected by sophisticated cyber-security measures and FBI facilities are protected by armed guards and/or sophisticated physical security measures, the vendor likely does not have the same resources to devote to its own security. With this in mind, the FBI would be taking a substantial risk to the continued viability of this technology by acknowledging the vendor. Since the same proprietary technology now owned by the FBI is also

stored within the vendor's facilities and computer systems, the security of this technology would only be as good as the vendor's own security measures. It is reasonable to conclude that they would not be able to thwart the same types of attacks and infiltration attempts the FBI is currently able to defend against; thus, revealing the vendor's identity may provide hostile enemies with a softer target for attack and infiltration, and risks disclosure, exploitation, and circumvention of a classified intelligence source and method. Considering E.O. 13,526, § 1.4(c), and 50 U.S.C. § 3024 (i)(1) prohibit the release of information that risks the harms enumerated above, it is absolutely necessary for the FBI to continue to protect the vendor's identity pursuant to FOIA Exemptions 1 and 3.

(10) Furthermore, considering the FBI is both a law enforcement and intelligence agency (*See Hardy Declaration*, ¶ 48), some of its intelligence gathering methods are also used to enforce federal laws. The FBI could potentially utilize the iPhone unlocking technology at issue in Plaintiffs' requests to pursue its law enforcement mission; thus, this technology must also be considered a law enforcement technique. As described above, releasing the vendor's identity risks circumvention of this technique. Providing criminals with the means to circumvent this technique could potentially enable them to deprive the FBI of information stored in criminals' personal cellular telephones, which in some situations could deprive the FBI of information needed to detect and/or disrupt criminal activities. Thus, the risks described above should also be considered law enforcement circumvention risks.

(11) While the identity of the vendor is not a law enforcement technique in and of itself, the vendor's identity is inexorably tied to the continued viability of the iPhone unlocking law enforcement technique, as described *supra*. Exemption 7E allows for protection of information if 1) the information consists of law enforcement records which would disclose

techniques and procedures for law enforcement investigations; and 2) such disclosure could reasonably be expected to circumvent the law. The existence of the law enforcement technique at issue has already been disclosed—the FBI has acknowledged it used a third party vendor’s technology to unlock Syed Rizwan Farook’s iPhone. However, the FBI has not publically explained how the technology works. As detailed above, disclosing the vendor’s identity provides criminals and hostile entities avenues to discover the “how” and then to create ways to circumvent the technology. Consequently, disclosure of the vendor’s identity risks circumvention of the law.

(12) The identity of the vendor pertains to the FBI’s law enforcement techniques and methods. Release of this information would constitute a reasonable expectation of the circumvention of the law if this information is released. Releasing the vendor’s identity could potentially lead to criminals obtaining all publically available technology developments from this vendor, and potentially exploiting this information to locate potential leads on the investigative tool created for the FBI. Any leads obtained by adversaries through these exploits will reveal the vendor’s capabilities and program sophistication by using small mosaic building blocks, and lead to understanding the scope and direction of FBI’s investigatory developments. Finally, because the vendor has developed unique capabilities, identifying the vendor would reveal knowledge about the FBI’s capabilities, including the specific investigatory tools and equipment used by the FBI, along with its capabilities and potential limitations.

***Protection of the Total Amount Paid to the Vendor***

(13) The FBI asserted FOIA Exemptions 1, 3, 4, and 7E, 5 U.S.C. §§ 552 (b)(1), (b)(3), (b)(4) and (b)(7)(E), to protect the total amount the FBI paid to the third party vendor because release would reveal classified intelligence activities (including covert action),

intelligence sources, or methods (E.O. 13,526, § 1.4(c)); reveal intelligence sources and methods requiring withholding per the National Security Act of 1947 (50 U.S.C. § 3024 (i)(1)); cause substantial harm to the competitive position of the person/company from whom the information was obtained; and/or disclose techniques and procedures for law enforcement investigations, the release of which would allow for circumvention of the law.

Applicability of Exemption 4 to Protect the Total Amount Paid to the Vendor

(14) Plaintiffs argue the FBI “offers no factual support for its contention that release” of the total amount paid to the vendor “would cause substantial competitive harm.” (*See* Docket No. 16, page 24.) As asserted in the original Declaration filed in this case, release of this information could reasonably be assumed to enable potential government contractors with similar technology/methods the opportunity to judge how they might underbid the third party vendor who unlocked Farook’s iPhone when bidding for similar contracts in the future. (*See* Hardy Declaration, ¶ 45.) Although the contract in this instance was sought from a single source, there is no reason to believe that future contracts will be similarly limited. Should the FBI require similar technology in the future, other vendors could use this information to judge how they might underbid the vendor in question, depriving the vendor of the benefits of future contracts with the FBI. Also, considering the vendor proved unlocking these types of encrypted devices is possible, and the vendor was paid for its efforts, it is reasonable to assume that their success will spur competition. The FBI judged that in light of such a competitive threat, it could not release this information without risking competitive harm to the vendor.

(15) Protecting the vendor’s proprietary and confidential data encourages all future submitters to furnish useful commercial or financial information to the government without hesitation, and it also provides the government with an assurance that required submissions will

be reliable. Moreover, release of such proprietary financial information would have a devastating impact on the government's ability to obtain similar types of proposals for state of the art technologies contemplated for law enforcement use in the future.

Applicability of Exemptions 1, 3, and 7E to Protect the Total Amount Paid to the Vendor

(16) The cost of the contract is properly classified as it pertains to intelligence sources and methods. The FBI has not disclosed the specific amount it paid to the third party for the iPhone unlocking technology. Revealing the actual amount paid for this product would designate a finite value for this technology, and would allow the FBI's adversaries to reasonably determine its usefulness to the FBI—whether or not the FBI can broadly utilize this technology to access their encrypted devices. Plaintiffs contend the total purchase price is not a law enforcement technique or procedure, nor is there any foreseeable harm to national security and intelligence sources and methods should this information be released. The given cost of a contract, taken in isolation, may not be exempt pursuant to Exemptions 1, 3, and 7E; however, in this specific instance, this particular price must be considered in conjunction with the intelligence source/method and law enforcement technique to which it relates, the iPhone unlocking technology. Although the cost itself may seem innocuous, it could reveal broader FBI priorities and the source and methods of certain intelligence collection when considered in the larger context of other publicly-available information.

(17) The FBI has never revealed the full scope of intended uses for this technology, and to reveal the total price paid for the technology would allow the FBI's adversaries to assess the nature of the tool. In addition, there are a limited number of vendors offering these types of products, and so with this piece of information (the cost of the contract), adversaries could



extrapolate to identify the maturity of the vendor, the vendor itself, and the likely capabilities of the classified technology.

(18) Revealing the specific financial allotments for technology acquisition shows where the FBI concentrates its resources for national security and criminal investigations. This information would allow these criminal entities and adversaries to judge whether they should continue to utilize their current technological security measures or dedicate further time and resources to obtaining/developing different encryption technology. The FBI is gravely concerned with the mosaic effect of releasing any of these non-public details concerning unique investigatory and intelligence gathering tools as such information would enable potential targets to carefully put together building blocks of information that would result in the degradation of the effectiveness of these tools. Thus, releasing the non-public price in conjunction with the publically acknowledged technique would alert the FBI's adversaries as to its technological capabilities and limitations, enabling them to proactively develop countermeasures to circumvent this technology.

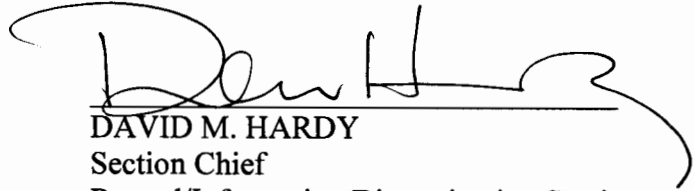
(19) I have determined that since the release of this information would reduce the effectiveness of a critical classified source and method, resulting in serious damage to the national security of the United States, this information is exempt from disclosure pursuant to Exemption 1 (E.O. 13,526, § 1.4(c)) and Exemption 3 (50 U.S.C. § 3024 (i)(1)). Additionally, since release would reduce the effectiveness of this technique in law enforcement investigations and may result in circumvention of the law, this information is also exempt pursuant to FOIA Exemption 7E.

**CONCLUSION**

(20) The FBI carefully examined its redaction of the identity of and the amount of money paid to the party that, the FBI has openly acknowledged, sold to the FBI a tool to break the security protections of at least one model of iPhone. The FBI determined this information remains exempt from disclosure pursuant to FOIA Exemptions 1, 3, 4, and 7E because if disclosed, it would: reveal classified and statutorily protected information; would reveal trade secret information; and/or would disclose techniques and procedures for law enforcement investigations. After extensive review of the documents at issue, I have determined that there is no further non-exempt information that can be reasonably segregated and released without revealing exempt information.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed this 9<sup>th</sup> day of March, 2017.



DAVID M. HARDY  
Section Chief  
Record/Information Dissemination Section  
Records Management Division  
Federal Bureau of Investigation  
Winchester, Virginia

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

THE ASSOCIATED PRESS; GANNETT  
SATELLITE INFORMATION NETWORK  
LLC d/b/a USA TODAY; and VICE MEDIA  
LLC,

Plaintiffs,

v.

FEDERAL BUREAU OF INVESTIGATION,

Defendant.

Civil Docket No. 16-1850 (TSC)

**DEFENDANT'S REPLY IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT  
AND OPPOSITION TO PLAINTIFF'S CROSS-MOTION  
FOR SUMMARY JUDGMENT**

**TABLE OF CONTENTS**

INTRODUCTION ..... 1

ARGUMENT ..... 2

I. The FBI properly withheld information pursuant to Exemption 1 ..... 2

II. The FBI properly withheld information pursuant to Exemption 3 ..... 10

III. The FBI properly withheld information pursuant to Exemption 7(E) ..... 13

IV. The FBI properly withheld information on the purchase price pursuant to Exemption 4 ..... 19

CONCLUSION ..... 23

**TABLE OF AUTHORITIES**

**CASES**

*ACLU v. Dep’t of Def.*,  
628 F.3d 612 (D.C. Cir. 2011) ..... 4

*Aftergood v. CIA*,  
355 F. Supp. 2d 557 (D.D.C. 2005) ..... 11, 18

*Am. Immigration Council v. U.S. Dep’t of Homeland Sec.*,  
950 F. Supp. 2d 221, 229 (D.D.C. 2013) ..... 5

*Blackwell v. FBI*,  
646 F.3d 37 (D.C. Cir. 2011) ..... 16, 17, 18, 19

*Canadian Commercial Corp. v. Dep’t of the Air Force*,  
514 F.3d 37 (D.C. Cir. 2008) ..... 21, 22

*Canadian Commercial Corp. v. Dep’t of the Air Force*,  
442 F. Supp. 2d 15 (D.D.C. 2006) ..... 21

*CIA v. Sims*,  
471 U.S. 159 (1985) ..... 11

*\*Citizens for Responsibility & Ethics in Wash. v. Dep’t of Justice*,  
160 F. Supp. 3d 226 (D.D.C. 2016) ..... 3, 14, 15, 18

*Citizens for Responsibility & Ethics in Wash. v. U.S. Dep’t of Veterans Affairs*,  
828 F. Supp. 2d 325 (D.D.C. 2011) ..... 5

*Concepcion v. FBI*,  
606 F. Supp. 2d 14 (D.D.C. 2009) ..... 16

*Critical Mass Energy Project v. N.R.C.*,  
975 F.2d 871 (D.C. Cir. 1992) ..... 20

*Ctr. for Nat. Sec. Studies v. Dep’t of Justice*,  
331 F.3d 918 (D.C. Cir. 2003) ..... 4, 6, 13

*DeSilva v. U.S. Dep’t of Housing & Urban Dev.*,  
36 F. Supp. 3d 65 (D.D.C. 2014) ..... 5

*Durrani v. DOJ*,  
607 F. Supp. 2d 77 (D.D.C. 2009) ..... 16

*Elec. Privacy Info. Ctr. v. Customs & Border Prot.*,  
160 F. Supp. 3d 354 (D.D.C. 2016) ..... 14

\**Fitzgibbon v. CIA*,  
911 F.2d 755 (D.C. Cir. 1990) ..... 4, 6, 7

*Frankenberry v. FBI*,  
567 F. App'x 120 (3d Cir. 2014)..... 15, 18

\**Gardels v. CIA*,  
689 F.2d 1100 (D.C. Cir. 1982) ..... 4, 9

*Gen. Elec. Co. v. Dep't of Air Force*,  
648 F. Supp. 2d 95 (D.D.C. 2009) ..... 20, 21

\**Halperin v. CIA*,  
629 F.2d 144 (D.C. Cir. 1980) ..... 10, 18

*Judicial Watch, Inc. v. Dep't of Commerce*,  
337 F. Supp. 2d 146 (D.D.C. 2004) ..... 2

*Judicial Watch, Inc. v. Dep't of Def.*,  
715 F.3d 937 (D.C. Cir. 2013) ..... 3, 13

*Judicial Watch, Inc. v. U.S. Food & Drug Admin.*,  
514 F. Supp. 2d 84 (D.D.C. 2007) ..... 5

*Jurewicz v. U.S. Dep't of Agric.*,  
741 F.3d 1326 (D.C. Cir. 2014) ..... 19, 22

*Lardner v. DOJ*,  
638 F. Supp. 2d 14 (D.D.C. 2009) ..... 18

*Larson v. Dep't of State*,  
565 F.3d 857 (D.C. Cir. 2009) ..... passim

\**Leopold v. CIA*,  
106 F. Supp. 3d 51 (D.D.C. 2015) ..... passim

*Long v. Immigration & Customs Enf.*,  
149 F. Supp. 3d 39 (D.D.C. 2015) ..... 18, 19

*Mayer Brown LLP v. IRS*,  
562 F.3d 1190 (D.C. Cir. 2009) ..... 16

*McDonnell Douglass Corp. v. NASA*,  
180 F.3d 303 (D.C. Cir. 1999) ..... 21

*McDonnell Douglas Corp. v. Dep’t of the Air Force*,  
375 F.3d 1182 (D.C. Cir. 2004) ..... 21, 22

*Military Audit Project v. Casey*,  
656 F.2d 724, 749-50 (D.C. Cir. 1981)..... 4

*Miller v. Dep’t of Justice*,  
872 F. Supp. 2d 12 (D.D.C. 2012) ..... 14

*Morley v. CIA*,  
508 F.3d 1109 (D.C. Cir. 2007) ..... 4, 14

*Murphy v. Exec. Office for U.S. Att’ys*,  
789 F.3d 204 (D.C. Cir. 2015) ..... 11

*Physicians for Human Rights v. Dep’t of Defense*,  
675 F. Supp. 2d 149 (D.D.C. 2009) ..... 5

*Pub. Emps. For Env’tl. Responsibility v. Int’l Boundary & Water Comm’n*,  
740 F.3d 195 (D.C. Cir. 2014) ..... 13, 16, 17

*Rosenberg v. Dep’t of Def.*,  
67 F. Supp. 3d 219 (D.D.C. 2014) ..... 3

*Schoenman v. F.B.I.*,  
573 F. Supp. 2d 119 (D.D.C. 2008) ..... 5

*Skinner v. Bureau of Alcohol, Tobacco, Firearms & Explosives*,  
No. 12-5319, 2013 WL 3367431 (D.C. Cir. May 31, 2013)..... 19

*Skinner v. U.S. Dep’t of Justice*,  
893 F. Supp. 2d 109 (D.D.C. 2012) ..... 19

*Tax Analysts v. IRS*,  
294 F.3d 71 (D.C. Cir. 2002) ..... 14

*United Techs. Corp. v. Dep’t of Def.*,  
601 F.3d 557 (D.C. Cir. 2010) ..... 20

*Vest v. Dep’t of Air Force*,  
793 F. Supp. 2d 103 (D.D.C. 2011) ..... 5



*Whitaker v. CIA*,  
31 F. Supp. 3d 23 (D.D.C. 2014) ..... 5

*Wolf v. CIA*,  
473 F.3d 370 (D.C. Cir. 2007) ..... 7, 18

**STATUTES**

5 U.S.C. § 552(b)(7) ..... 13, 15

50 U.S.C. § 3024(i)(1) ..... 10

**ADMINISTRATIVE AND EXECUTIVE MATERIALS**

Exec. Order No. 13,526 § 1.4(c)..... 2

## INTRODUCTION

As part of its federal terrorism investigation into the December 2015 San Bernardino attack, the FBI sought access to an iPhone that was operated by one of the perpetrators, Syed Rizwan Farook. After initially failing to access the contents of that device, the FBI contracted with a third-party vendor, which provided a tool that enabled the agency to circumvent the security protections of Farook's iPhone. Plaintiffs, three news organizations, seek information about that tool. That information is exempt from disclosure pursuant to the FOIA.

Plaintiffs' opposition and cross-motion for summary judgment has substantially narrowed the items in dispute. Plaintiffs are not challenging the vast majority of the FBI's redactions, the adequacy of the FBI's search, or its segregability determination. Mem. Supp. Pls.' Cross-Mot Summ. J. & Opp'n Def.'s Mot. Summ. J. ("Opp'n"), at 1 n.1, 9, ECF No. 15. Instead, they seek only two pieces of information: the identity of the tool's vendor, and the total amount of money paid to that entity. *Id.* at 1. Both, however, are properly and independently protected from disclosure pursuant to FOIA Exemptions 1, 3, and 7(E). The tool's price is also independently protected from disclosure pursuant to Exemption 4. And Plaintiffs' opposition does not call those conclusions into question. Instead, it merely offers armchair intelligence speculation. That speculation, however, is divorced from decades of D.C. Circuit case law that establishes that the information in question, if released, would reveal intelligence sources and methods and law enforcement techniques, and that revealing the hereto unknown price of a vendor's contract can cause substantial competitive harm, by allowing competitors to underbid the vendor in future contracts. For these reasons, as further explained below, this Court should deny Plaintiffs' cross-motion for summary judgment and grant Defendant's motion for summary judgment.

## ARGUMENT

### **A. The FBI Properly Withheld Information Pursuant to Exemption 1**

The FBI properly classified the vendor identity and cost of the technology used to access Farook's iPhone pursuant to Executive Order 13,526, and these two pieces of information are exempt from disclosure pursuant to Exemption 1. In their opposition, Plaintiffs claim that it is not logical or plausible that information about the creator and cost of an intelligence tool "pertains" to "intelligence activities . . . [or] intelligence sources or methods," such that the release of that information could harm national security. *See* Opp'n at 12 (citing Exec. Order No. 13,526 § 1.4(c)). But such a conclusion flies in the face of well-established D.C. Circuit precedent. Moreover, in support of their claim, Plaintiffs offer only armchair intelligence analysis, putting forward their own speculation about how the release of such information will or will not threaten national security. But as this Circuit has made clear, such speculation by a plaintiff simply cannot supersede an agency's logical or plausible claim that the information is classified. *See, e.g., Larson v. Dep't of State*, 565 F.3d 857, 865 (D.C. Cir. 2009) ("If an agency's statements supporting exemption contain reasonable specificity of detail as to demonstrate that the withheld information logically falls within the claimed exemption and evidence in the record does not suggest otherwise . . . the court should not conduct a more detailed inquiry to test the agency's judgment and expertise or to evaluate whether the court agrees with the agency's opinions."); *see also Judicial Watch, Inc. v. Dep't of Commerce*, 337 F. Supp. 2d 146, 162 (D.D.C. 2004) ("In light of courts' presumed lack of expertise in the area of national security and related disclosure interests, a reviewing court is prohibited from conducting a detailed analysis of the agency's invocation of Exemption 1.").

Plaintiffs launch only a limited attack on the FBI's Exemption 1 assertion. They do not dispute the fact that the agency complied with the procedural requirements of Executive Order 13,526, nor do they dispute that the information is under the control of the United States Government. See Defs.'s Mot. Summ. J. ("FBI Mem. "), at 10, ECF No. 14; Opp'n at 12-18. Nor do they appear to challenge the fact that information identifying the vendor and cost of an intelligence tool "pertains" to intelligence activities or intelligence sources and methods. See Opp'n at 14-17. They could not, in any event. "This Circuit has noted that 'pertains' is not a very demanding verb." *Leopold v. CIA*, 106 F. Supp. 3d 51, 62 (D.D.C. 2015) (quoting *Judicial Watch, Inc. v. Dep't of Def.*, 715 F.3d 937, 941 (D.C. Cir. 2013)). And it is certainly reasonable to conclude that core information about an intelligence activity, source, or method – how much it cost and who created it – "pertains" to such an intelligence activity, source, or method. See, e.g., *id.* (budgetary information about costs of intelligence methods "pertains" to intelligence sources and methods); *Citizens for Responsibility & Ethics in Wash ("CREW") v. Dep't of Justice*, 160 F. Supp. 3d.226, 234-35 (D.D.C. 2016) (information about identity of intelligence sources, methods and methodology "pertains" to intelligence activities or intelligence sources and methods); *Rosenberg v. Dep't of Def.*, 67 F. Supp. 3d 219, 221, 225-26 (D.D.C. 2014) (information on the cost of building a detention facility at Guantánamo Bay, and the firm responsible for the construction of that facility, is properly classified need not be disclosed pursuant to Exemption 1).

Instead, Plaintiffs claim that it is not "logical or plausible," *Judicial Watch*, 715 F.3d at 943, that information about the iPhone tool's vendor or cost falls within Exemption 1's ambit, such that its release could harm national security. See Opp'n at 12-17. But as Plaintiffs correctly recognize, this is not a high bar: "the text of Exemption 1 itself suggest that little proof or

explanation is required beyond a plausible assertion that information is properly classified.” *Morley v. CIA*, 508 F.3d 1108, 1124 (D.C. Cir. 2007). Indeed, “the government’s burden [here] is a light one,” *ACLU v. Dep’t of Def.*, 628 F.3d 612, 624 (D.C. Cir. 2011), as “[t]his is necessarily a region for forecasts in which informed judgments as to potential future harm should be respected,” *Gardels v. CIA*, 689 F.2d 1100, 1106 (D.C. Cir. 1982). Moreover, when considering harm, this Circuit teaches that a reviewing court does not consider the release of the classified records in isolation, but rather must consider the effect of their release in conjunction with other pieces of information that might be available to an adversary. *See Fitzgibbon v. CIA*, 911 F.2d 755, 763 (D.C. Cir. 1990) (“This court has established that in considering the potential harm arising from disclosure of [an intelligence] source of method, we must take into account that each individual piece of intelligence information, much like a piece of jigsaw puzzle, may aid in piecing together other bits of information even when the individual piece is not of obvious importance itself.”) (quoting *Gardels*, 689 F.2d at 1106) (internal ellipses, quotation marks, and brackets omitted); *see also Ctr. for Nat. Sec. Studies v. Dep’t of Justice*, 331 F.3d 918, 928 (D.C. Cir. 2003) (adopting a “mosaic argument[] in the context of national security”); *Gardels*, 689 F.2d at 1106 (“The CIA has the right to assume that foreign intelligence agencies are zealous ferrets.”). The FBI has met its burden of showing logical or plausible harm, and the Plaintiffs do not adequately establish otherwise.

Turning first to the price of the tool, it is well-established that information concerning expenditures for intelligence activities are protected from disclosure because such release could harmfully reveal intelligence priorities. *See, e.g. Leopold*, 106 F. Supp. 3d at 59, 64; *see also Military Audit Project v. Casey*, 656 F.2d 724, 749-50 (D.C. Cir. 1981) (affirming Exemption 1 claim when agency stated that “[r]elease of this [expenditure] information would be a valuable

benefit to an intelligence service of a foreign country in that it would permit deductions to be made concerning the state of the art of intelligence collection in a certain area and the importance the United States attributed to particular collection activities”). The FBI has demonstrated that releasing the pricing information of the iPhone tool would identify intelligence priorities and capabilities, and has articulated how it could do so in a way that can harm national security.

Mr. Hardy’s supplemental declaration provides multiple reasons why this is so. First, “[r]evealing the actual amount paid for this product,” which the FBI has not disclosed, “would designate a finite value for this technology, and would allow the FBI’s adversaries to reasonably determine its usefulness to the FBI – whether or not the FBI can broadly utilize this technology to access their encrypted devices.” Second Hardy Decl. ¶ 16 [attached hereto].<sup>1</sup> Second, “[t]he FBI has never revealed the full scope of intended uses for this technology, and to reveal the total price paid for the technology would allow the FBI’s adversaries to assess the nature of the tool. In addition, there are a limited number of vendors offering these types of products, and so with this piece of information (the cost of the contract), adversaries could extrapolate to identify the maturity of the vendor, the vendor itself, and the likely capabilities of the classified technology.” *Id.* ¶ 17. Finally, “[r]evealing the specific financial allotments for technology acquisition shows where the FBI concentrates its resources for national security and criminal investigations. This

---

<sup>1</sup> Courts in this Circuit regularly accept supplemental declarations filed alongside FOIA reply briefs, particularly after the Plaintiffs have focused the issues in dispute. *See, e.g., DeSilva v. U.S. Dep’t of Housing & Urban Dev.*, 36 F. Supp. 3d 65, 72 (D.D.C. 2014); *Whitaker v. CIA*, 31 F. Supp. 3d 23, 36 (D.D.C. 2014), appeal filed, No. 14-5275 (D.C. Cir. Nov. 12, 2014); *Am. Immigration Council v. U.S. Dep’t of Homeland Sec.*, 950 F. Supp. 2d 221, 229 (D.D.C. 2013); *Citizens for Responsibility & Ethics in Wash. v. U.S. Dep’t of Veterans Affairs*, 828 F. Supp. 2d 325, 328 (D.D.C. 2011); *Vest v. Dep’t of Air Force*, 793 F. Supp. 2d 103, 121 (D.D.C. 2011); *Physicians for Human Rights v. Skinner Dep’t of Defense*, 675 F. Supp. 2d 149, 158 (D.D.C. 2009); *Schoenman v. F.B.I.*, 573 F. Supp. 2d 119, 125 n.2 (D.D.C. 2008); *Judicial Watch, Inc. v. U.S. Food & Drug Admin.*, 514 F. Supp. 2d 84, 89 (D.D.C. 2007).

information would allow these criminal entities and adversaries to judge whether they should continue to utilize their current technological security measures or dedicate further time and resources to obtaining/developing different encryption technology.” *Id.* ¶ 18. If the non-public price was released in conjunction with the existence of the publically acknowledged technique, the FBI’s adversaries would be alerted to its technological capabilities and limitations, allowing them to develop countermeasures. *Id.*; *see also Fitzgibbon*, 911 F.2d at 763 (potential harm of release of information must be judged considering other available pieces of information); *Ctr. for Nat. Sec. Studies*, 331 F.3d at 928-29 (adopting mosaic theory).

Indeed, in response, Plaintiffs essentially concede that the cost of an intelligence tool reveals valuable information. They assert that “the FBI’s Director has already revealed the only possible useful bit of information about the tool’s price, namely that it was very high, and that the tool therefore is likely to be somewhat sophisticated or novel. If it were at all plausible that this nation’s enemies could develop disruptive countermeasures by knowing that the government invested heavily in the tool, then the damage has already been done by [Director] Comey’s confirmation that the tool cost ‘a lot of money.’” *Opp’n* at 15 (emphasis omitted). But this argument recognizes – as this Circuit has as well – that knowing the cost of an intelligence source or method reveals information about the source or method’s capabilities and the priority the agency assigned to it. Moreover, it is reasonable that an adversary’s decision about whether and how to invest in countermeasures would be influenced by knowledge about the relative priority the agency has placed in an intelligence tool, as well as the potential sophistication of that tool, information reflected in that tool’s price – a point the Plaintiffs also seem to recognize. *See id.* The Plaintiffs, however, argue that price is only relevant in a binary sense: an intelligence tool’s price is either “high” or “low,” and that no other information can be relevant

to an assessment of its capabilities (or the harm coming from the revelation thereof). This statement is simply wrong: the specific dollar amount of the tool conveys far more information, and reasonably allows for far more granular assessments of the tool's capabilities by an adversary than merely knowing that the cost is "high." Such an attempt to impose artificial (and illogical) limitations on the FBI's invocation of harm is inconsistent with this Circuit's caselaw.

Plaintiff also claims that the FBI Director has "suggest[ed] that the government's true motive for withholding the contract price is prohibited under EO 13526," in that the FBI was solely focused on "artificially alter[ing] the competitive landscape for technology contracting." Opp'n at 16. But Plaintiffs put forward no evidence that the FBI has officially stated that this is the reason for limiting disclosure. Nor could they. In order for agency statements to have been "officially acknowledged," the information must meet three criteria: "First, the information requested must be as specific as the information previously released. Second, the information requested must match the information previously disclosed. Third, the information requested must already have been made public through an official and documented disclosure." *Wolf v. CIA*, 473 F.3d 370, 379 (D.C. Cir. 2007) (alteration in original) (quoting *Fitzgibbon*, 911 F.2d at 765). None of Director Comey's statements leads to an official acknowledgment that the reason for non-disclosure was for improper reasons. Moreover, the information at issue has been properly classified. *See* First Hardy Decl. ¶¶ 33-37; Second Hardy Decl. ¶¶ 7-9.

The FBI also properly classified the name of the vendor of the iPhone tool. The FBI stated that "identifying the specific vendor could reveal/allow for circumvention of the intelligence activities or methods utilized," First Hardy Decl. ¶ 35, ECF No. 14-2, because adversaries could use that classified information to learn more about the vendor and its products, *see Fitzgibbon*, 911 F.2d at 763. The company that created this tool has not been publically



linked to the tool itself; if that classified information was released and combined with other information about that company, it is logical or plausible that adversaries could learn more about the technical capabilities of that tool, be that from studying other products created by that company, the background of its employees, etc. In its supplemental declaration, the FBI expanded upon these potential harms. First, Mr. Hardy stated that because technology vendors “are more likely to expand and update previous versions of their existing computer programs rather than start from scratch . . . ,” “[r]evealing the vendor’s identity immediately provides those wishing to circumvent the iPhone unlocking technology with a body of work from the company (any existing public technology created by the company) to review and probe for possible weaknesses. [Adversaries] may then apply any knowledge gained through such a review to develop exploits for the vendor’s unique product.” Second Hardy Decl. ¶ 8. This, in turn, could allow adversaries to “thwart the iPhone unlocking technology currently available to the FBI, and deprive the FBI of a critical classified intelligence source and method.” *Id.*

Revealing the vendor’s identity also threatens the continued security of the intelligence tool itself. The exposure of such information “immediately exposes the vendor to attacks and infiltration by hostile entities wishing to exploit the technology they provided to the FBI.” *Id.* ¶ 9. “Since the same proprietary technology now owned by the FBI is also stored within the vendor’s facilities and computer systems, the security of this technology would only be as good as the vendor’s own security measures. It is reasonable to conclude that they would not be able to thwart the same types of attacks and infiltration attempts the FBI is currently able to defend against; thus, revealing the vendor’s identity may provide hostile enemies with a softer target for attack and infiltration, and risks disclosure, exploitation, and circumvention of a classified intelligence source and method.” *Id.*

In response, Plaintiffs advance an inapt analogy, rejecting the proposition that simply “stating that knowing that Lockheed Martin is building F-35 fighter jets inherently reveals the specific capabilities of the jets themselves.” Opp’n at 17. This analogy misconstrues the inquiry. It is not whether the vendor name *inherently reveals* the specific capabilities of an intelligence tool, but whether it is logical or plausible to suppose that releasing that name, when combined with other available information about the vendor, could reveal the capabilities about the tool the vendor created. *See, e.g., Larson*, 565 F.3d at 864-65 (the harm from releasing information must be considered in context); *Gardels*, 689 F.2d at 1106 (same). To use Plaintiffs’ analogy correctly: the name “Lockheed Martin” may not singlehandedly reveal the capability of its jets, but knowing that the company produces those fighters, when combined with other available information about Lockheed’s history, business model, the expertise of its engineers, other similar contracts which it may have, etc., certainly could allow a dedicated adversary to make reasonable assessments about the company’s product, thus harming national security. Accordingly, in that hypothetical situation, even the name of an otherwise well-known company (Lockheed) could be properly classified if the name could be used to extrapolate information about the classified contracted-for technology.

Plaintiffs remaining objection is unavailing. They claim that the iPhone tool itself is of no current value. *See* Opp’n at 15-16 (“Acceptance of the FBI’s argument would also require this Court to ignore that the FBI has been exceedingly public about the fact that the tool applies only to a specific model of phone (the iPhone 5c) running a specific, and already outdated, operating system (iOS9). Were adversaries on the hunt for actually effective countermeasures, they need only to heed [Director] Comey’s public statement and simply use a different kind of phone, or a different operating system.”) (citation omitted). But this argument is unvarnished

speculation about the efficacy of this intelligence tool – and this Circuit has made exceedingly clear that such speculation cannot defeat an agency’s summary judgment claim. *See, e.g., Leopold*, 106 F. Supp. 3d at 59 (“In essence, [Plaintiff] asks the Court to credit his judgments about the effects of disclosure over those of the agency. This is something it clearly cannot do.”) (citing *Larson*, 565 F.3d at 865).

Because Exemption 1 applies, the FBI properly withheld this information.

**B. The FBI Properly Withheld Information Pursuant to Exemption 3**

The FBI also properly withheld the iPhone tool vendor identity and pricing information pursuant to Exemption 3. The FBI relied upon section 102A(i)(1) of the National Security Act of 1947, 50 U.S.C. § 3024(i)(1), which “protect[s] intelligence sources and methods from unauthorized disclosure.” The Plaintiffs concede that this statute is an exempting statute and applies to the FBI. Opp’n at 18. The FBI has demonstrated that both the price and vendor of the iPhone tool “relate[] to intelligence sources and methods or can reasonably be expected to lead to unauthorized disclosure of intelligence sources and methods,” *Leopold*, 106 F. Supp. 3d at 57 (citations omitted), and so these records are exempt from disclosure.

Turning first to the price of the tool, it is well established that expenditures on intelligence activities, like spending on the tool here, can reveal information about intelligence methods, sources, and priorities funded by those monies, and that these monetary values are protected from disclosure pursuant to Exemption 3 and section 102A(i)(1). *See, e.g., Leopold*, 106 F. Supp. 3d at 58 (money spent by CIA related to its former detention and interrogation program are exempt from disclosure because they could reveal resources and priorities of agency); *Halperin v. CIA*, 629 F.2d 144, 150 (D.C. Cir. 1980) (information on attorneys fees is exempt because “[w]hen combined with other small leads,” it could reveal information on the

“size and nature of the operation”); *Aftergood v. CIA*, 355 F. Supp. 2d 557, 562 (D.D.C. 2005) (intelligence budget information is exempt from release because it “relates to intelligence methods, namely the allocation, transfer and funding of intelligence programs”).

The reasoning of these decisions accord precisely with the Supreme Court’s seminal opinion in *CIA v. Sims*, 471 U.S. 159 (1985). There, the Supreme Court interpreted the “sources and methods” statutory provision and recognized the statute protects information which reveals the relative priorities of the intelligence agency. It held that “[d]isclosure of the subject matter of the Agency’s research efforts and inquiries may compromise the Agency’s ability to gather intelligence as much as disclosure of the identities of intelligence sources. . . . The inquiries pursued by the Agency can often tell our adversaries something that is of value to them.” *Id.* at 176-77; *id.* at 178 (“Foreign intelligence services have both the capacity to gather and analyze any information that is in the public domain and the substantial expertise in deducing the identities of intelligence sources from seemingly unimportant details.”). The FBI found that the release of the price of the iPhone tool would also convey useful information to adversaries. Second Hardy Decl. ¶¶ 16-18. Accordingly, it is exempt from disclosure.

Plaintiffs’ objections fail. The bulk of its opposition claims that the First Hardy Declaration is conclusory. Opp’n at 19-20. It was not. Nevertheless, the FBI has since supplemented its declaration. *See* Second Hardy Decl. Plaintiffs also state that the FBI has “fail[ed] to adduce any such evidence” of a connection between the withheld information and the intelligence source. Opp’n at 20. But the standard is not whether the agency has put forward an adequate evidentiary showing, but that “the basis for invoking exemption 3 need only be ‘logical or plausible.’” *Murphy v. Exec. Office for U.S. Att’ys*, 789 F.3d 204, 211 (D.C. Cir. 2015) (quoting *Larson*, 565 F.3d at 862) (internal citation omitted). Accordingly, “[a] risk of harm is

plausible even if the anticipated harm has not yet materialized. Likewise, an explanation is no less plausible because it posits persuasive hypotheticals rather than real-world examples.” *Id.* (internal citations omitted). Finally, Plaintiffs state that it is “not credible” “that knowing the exact dollar amount of the price will permit the development of countermeasures.” *Opp’n* at 20. For the reasons stated in the context of Exemption 1, this speculation is unavailing.

The identity of the tool’s vendor is similarly protected because it “relates to intelligence sources and methods.” *Larson*, 565 F.3d at 865. The iPhone tool itself is an intelligence source and method. *Second Hardy Decl.* ¶ 8. As the FBI has articulated, revealing the identity of the vendor reveals information about the vendor’s other body of works and its technical capacities, which can allow an inquisitive adversary to learn about the capabilities and weaknesses about the iPhone intelligence tool itself. *See id.* (“Revealing the vendor’s identity immediately provides those wishing to circumvent the iPhone unlocking technology with a body of work from the company (any existing public technology created by the company) to review and probe for possible weaknesses. [Adversaries] may then apply any knowledge gained through such a review to develop exploits for the vendor’s unique product.”). Moreover, acknowledging the identity of the vendor would “expose[] the vendor to attacks and infiltration by hostile entities wishing to exploit the technology they provided to the FBI.” *Id.* ¶ 9; *see also id.* (“[R]evealing the vendor’s identity may provide hostile enemies with a softer target for attack and infiltration, and risks disclosure, exploitation, and circumvention of a classified intelligence source and method.”).

Exemption 3 only requires that information “relate[] to” or be “reasonably be expected to lead to unauthorized disclosure of” intelligence sources and methods. *Leopold*, 106 F. Supp. 3d at 57. Plaintiffs do not question that the identity of the creator of an intelligence tool is related to

“intelligence sources and methods,” Opp’n at 18, and the FBI has explained how disclosing information about the vendor’s identity could reveal information about the intelligence source and method that the vendor created. Thus, while the identity of the vendor may not itself be an intelligence source or method, *see* Opp’n at 18, releasing that information leads “logically or plausibly” to information about the intelligence source or method, *see Judicial Watch*, 715 F.3d at 941, and is thus exempt from disclosure under Exemption 3. That is particularly true in light of the “considerable deference” owed to the FBI in this context. *Leopold*, 106 F. Supp. 3d at 58; *see also Ctr. for Nat’l Sec. Studies v. Dep’t of Justice*, 331 F.3d 918, 927 (D.C. Cir. 2003) (“[W]e have consistently deferred to executive affidavits predicting harm to the national security, and have found it unwise to undertake searching judicial review.”). Accordingly, the FBI has appropriately applied Exemption 3 to these two pieces of information.

### **C. The FBI Properly Withheld Information Pursuant to Exemption 7(E)**

The FBI has properly withheld information about the iPhone unlocking tool’s vendor and price pursuant to Exemption 7(E), as release of this information “would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosures could reasonably be expected to risk circumvention of the law.” 5 U.S.C. § 552(b)(7)(E).<sup>2</sup>

As an initial note, Plaintiffs assert that “the FBI does not explain how the total purchase price for the iPhone access tool or the identity of the vendor are law enforcement ‘techniques’ or

---

<sup>2</sup> Plaintiffs concede that “the purchase price for the iPhone access tool and the identity of the third party vendor were ‘compiled for law enforcement purposes.’” Opp’n at 29; *see also Pubc. Emps. For Env’tl. Responsibility v. Int’l Boundary & Water Comm’n (“PEER”)*, 740 F.3d 195, 202 (D.C. Cir. 2014) (“To fall within any of the exemptions under the umbrella of Exemption 7, a record must have been ‘compiled for law enforcement purposes.’”) (quoting 5 U.S.C. § 552(b)(7)).

‘procedures.’” Opp’n at 29. But that is not the test. Instead, Exemption 7(E) asks whether the “information, if disclosed, *would reveal* law enforcement techniques and procedures which . . . could reasonably be expected to risk circumvention of the law.” *CREW*, 160 F. Supp. 3d at 243 (emphasis added); *see also Elec. Privacy Info. Ctr. v. Customs & Border Prot.*, 160 F. Supp. 3d 354, 359 (D.D.C. 2016) (agency must demonstrate that the materials withheld “would reveal techniques and procedures for law enforcement investigations or prosecutions”); *Miller v. U.S. Dep’t of Justice*, 872 F. Supp. 2d 12, 29 (D.D.C. 2012) (“Because the [records] were created for a law enforcement purpose and their disclosure may disclose techniques and procedures for law enforcement investigation, this Court finds that they are properly withheld under Exemption 7(E).”). This Circuit has also applied Exemption 7(E) to protect materials “relating to” law enforcement techniques and procedures. *Morley v. CIA*, 508 F.3d 1109, 1129 (D.C. Cir. 2007) (“An agency may seek to block the disclosure of internal agency materials *relating to* guidelines, techniques, sources, and procedures for law enforcement investigations and prosecutions [under Exemption 7(E)] . . .”) (quoting *Tax Analysts v. IRS*, 294 F.3d 71, 79 (D.C. Cir. 2002) (emphasis added)).

While the identity of the iPhone tool vendor and the total amount paid are not in and of themselves law enforcement techniques, these pieces of information *relate* to and could *reveal* law enforcement techniques, and are accordingly protected from release pursuant to Exemption 7(E). *See* Second Hardy Decl. ¶ 11. As the FBI explains: “The existence of the law enforcement technique at issue has already been disclosed – the FBI has acknowledged it used a third party vendor’s technology to unlock Syed Rizwan Farook’s iPhone. However, the FBI has not publically explained how the technology works.” *Id.* “[D]isclosing the vendor’s identity provides criminals and hostile entities avenues to discover the ‘how’ and then to create ways to

circumvent the technology.” *Id.* As discussed in more detail above, revealing the identity of the vendor would provide insight into the unique “programming styles and strategies” of the vendor, as well as the vendor’s previous body of work. *Id.* ¶ 9. It would also “reveal knowledge about the FBI’s capabilities, including the specific investigatory tools and equipment used by the FBI, along with its capabilities and potential limitations.” *Id.* ¶ 12; *see also id.* (“Releasing the vendor’s identity could potential lead to criminals obtaining all publically available technology developments from this vendor, and potentially exploiting this information to locate potential leads on the investigative tool created for the FBI.”).

The price relates to and would reveal law enforcement techniques as well. “The FBI has never revealed the full scope of intended uses for this technology, and to reveal the total price paid for this technology would allow the FBI’s adversaries to assess the nature of the tool.” *Id.* ¶ 17. These facts accord with those of other courts that have recognized that the vendor and supplier identities and funding/expenditure information reveals law enforcement information protected by Exemption 7(E). *See, e.g., CREW*, 160 F. Supp. 3d at 243 (rejecting the claim that “vendor and supplier identities are not law enforcement techniques within the meaning of Exemption 7(E)” because revealing the vendor identity would reveal information about the FBI’s law enforcement capabilities and limitations); *id.* at 243-44 (holding that funding information, including “product pricing” and “funding allocation and budgeting details” was protected pursuant to Exemption 7(E) because it would provide information about the law enforcement capabilities of the services FBI was procuring); *Frankenberry v. FBI*, 567 F. App’x 120, 125 n.2 (3d Cir. 2014) (concluding that “the FBI had properly withheld documents that contain information relating to money expenditures in the FBI investigation. This information relates to ‘procedures for law enforcement investigations’ because it shows where the FBI concentrates its



resources in an investigation,” and was exempt under Exemption 7(E).”) (citing 5 U.S.C. § 552(b)(7)(E)); *Concepcion v. FBI*, 606 F. Supp. 2d 14, 43-44 (D.D.C. 2009) (holding that “the amount of money used to purchase evidence” by the FBI was protected from disclosure under Exemption 7(E)).

Moreover, the release of this information would risk circumvention of the law.<sup>3</sup> As Plaintiffs concede, this is a “low bar.” *Pub. Emps. for Envtl. Responsibility v. Int’l Boundary & Water Comm’n (“PEER”)*, 740 F.3d 195, 204 n.4 (D.C. Cir. 2014); *see also Mayer Brown LLP v. IRS*, 562 F.3d 1190, 1194 (D.C. Cir. 2009) (“[T]he text of exemption 7(E) is much broader” than other exemptions that “set a high standard”); *Mayer Brown*, 562 F.3d at 1193 (Exemption 7(E) “exempts from disclosure information that could *increase the risks* that a law will be violated or that past violators will escape legal consequence.”). And it is a bar that the FBI has met, as it has “logically shown how a risk of circumvention might result.” *Mayer Brown*, 562 F.3d at 1194. Turning first to vendor identity, the FBI has explained how revealing that information would allow adversaries to learn about the vendor’s past body of work and unique programming style, so they may be able to “develop exploits for the vendor’s unique product” and compromise the tool’s efficacy. Second Hardy Decl. ¶ 8. Revealing the name of the vendor would also expose that company to attacks and potential infiltration, potentially compromising the security of the software and allowing for its circumvention. *Id.* ¶ 9. It would also reveal information about the FBI’s specific investigatory tools and equipment, along with the capabilities and potential

---

<sup>3</sup> Defendant’s opening memorandum acknowledged that courts disagree as to whether “techniques and procedures for law enforcement investigations” receive categorical protection under Exemption 7(E), and submits that the D.C. Circuit’s pronouncements on this issue are better viewed as *dicta*. *See, e.g., PEER*, 740 F.3d at 204 n.4; *Blackwell v. FBI*, 646 F.3d 37, 41-42 (D.C. Cir. 2011); *Mayer Brown LLP v. IRS*, 562 F.3d 1190, 1194 (D.C. Cir. 2009); *see also, e.g., Durrani v. DOJ*, 607 F. Supp. 2d 77, 91 (D.D.C. 2009) (techniques and procedures entitled to categorical protection under (7)(E)). In any event, Defendant prevails under either standard.

limitations of those tools. *Id.* ¶ 12. These explanations more than comply with this Circuit’s low bar to establish risk of circumvention. *See, e.g., Blackwell v. FBI*, 646 F.3d 37, 42 (D.C. Cir. 2011) (information that could “expose computer . . . vulnerabilities to potential criminals” is protected under Exemption 7(E)); *id.* (information that could “enable criminals to employ countermeasures to avoid detection” is protected under Exemption 7(E)).

Furthermore, because the iPhone unlocking technique can also be used pursuant to the FBI’s law enforcement mission, “[p]roviding criminals with the means to circumvent this technique could potentially enable them to deprive the FBI of information stored in criminals’ personal cellular telephones, which in some situations could deprive the FBI of information needed to detect and/or disrupt criminal activities.” Second Hardy Decl. ¶ 10. Revealing the total price paid for the tool, combined with the fact that “[t]he FBI has never revealed the full scope of intended uses for this technology,” *id.* ¶ 17, would allow the FBI’s adversaries to assess the nature of the tool, and to “judge whether they should continue to utilize their current technological security measures or dedicate further time and resources to obtaining/developing different encryption technology.” *Id.* ¶ 18; *see also id.* ¶ 17 (“In addition, there are a limited number of vendors offering these types of products, and so with this piece of information (the cost of the contract), adversaries could extrapolate to identify the maturity of the vendor, the vendor itself, and the likely capabilities of the classified technology.”). This explanation comports with the “relatively low bar” that this Circuit requires for Exemption 7(E). *See, e.g., PEER*, 740 F.3d at 71 (information that can help “[t]errorists or criminals . . . to obstruct attempts to investigate” a criminal act are protected from disclosure).

Plaintiffs’ remaining arguments fail. They baldly state that it is “incredible” and “implausible” that revealing the price of the iPhone tool could allow adversaries to assess the

nature of the law enforcement tool and judge the possibility for employing countermeasures. Opp'n at 29-30. But, as discussed above, it is well-established that revealing the amount of money an investigatory agency spends on intelligence and law enforcement tools reveals information about the priorities and capabilities of that agency. *See, e.g., CREW*, 160 F. Supp. 3d at 243-44; *Frankenberry*, 567 F. App'x at 125 n.2; *see also Leopold*, 106 F. Supp. 3d at 58; *Halperin*, 629 F.2d at 150; *Aftergood*, 355 F. Supp. 2d at 562. Given Exemption 7(E)'s "low bar," and the fact that a law enforcement agency's "decision to invoke Exemption 7 is entitled to deference," *Long v. Immigration & Customs Enf.*, 149 F. Supp. 3d 39, 48 (D.D.C. 2015) (quoting *Lardner v. DOJ*, 638 F. Supp. 2d 14, 31 (D.D.C. 2009)), the FBI's explanation is more than sufficient. Any statement made by Director Comey does not undermine the FBI's explanation. Plaintiffs cite to a press conference where Director Comey made general statements that he hoped the tool would be useful in other, undefined future cases. Opp'n at 30. These statements do not define how the tool works, its technical scope, or how broadly it would be applied (much less in what specific contexts). *See* Second Hardy Decl. ¶¶ 16-18. However, revealing the total price of this tool could, when combined with other information, provide insight into these questions and risk circumvention of the law. In any event, these statements do not constitute an "official acknowledgment" of the price of the tool or its vendor, *Wolf*, 473 F.3d at 37, and Plaintiffs do not argue that it would.

Plaintiffs' challenge to vendor identity is on even shakier ground. They criticize the FBI for not precisely defining the "countermeasures" that potential criminals who know the identity of the tool's vendor (and thus its past body of work and potential repository of the tool itself) might use. Opp'n at 31. But this Circuit does not require identification of particular countermeasures. *See, e.g., Blackwell*, 646 F.3d at 42 (FBI's assertion that disclosure of

information “could enable criminals to employ countermeasures to avoid detection” is sufficient); *Skinner v. U.S. Dep’t of Justice*, 893 F. Supp. 2d 109, 113 (D.D.C. 2012) *aff’d sub nom. Skinner v. Bureau of Alcohol, Tobacco, Firearms & Explosives*, No. 12-5319, 2013 WL 3367431 (D.C. Cir. May 31, 2013) (statement that release of information could allow criminals to “effectuat[e] other countermeasures” is sufficient). Nor should it: such a requirement would subvert the integrity of the very information Exemption 7(E) is designed to protect. Indeed, Plaintiffs go further and suggest that the *only possible countermeasure* is “[d]o not use an iPhone 5c and do not use iOS9.” Opp’n at 31. These judgments about the viability of potential countermeasures are not the Plaintiffs’ to make, *see Long*, 149 F. Supp 3d. at 51, and in any event, none of the materials cited by the Plaintiffs indicate that iPhone unlocking tool is no longer of intelligence or law enforcement value, or that knowing the identity of the vendor would not be useful to potential adversaries. That is, again, especially true considering the “low bar” that the “circumvention of the law” requirement imposes. *Blackwell*, 646 F.3d at 42.<sup>4</sup>

Accordingly, the FBI properly withheld this information under Exemption 7(E).

**D. The FBI Properly Withheld Information on the Purchase Price Pursuant to Exemption 4**

Finally, the FBI also properly withheld information about the iPhone unlocking tool’s purchase price pursuant to Exemption 4. The FBI determined that such information was confidential, because disclosure would likely “cause substantial harm to the competitive position of the [vendor] from whom the information was obtained.” *Jurewicz v. U.S. Dep’t of Agric.*, 741

---

<sup>4</sup> Plaintiffs also suggest that “the FBI has offered no support for the contention that the vendor’s past work or capabilities would be evident from disclosure of the vendor’s name.” Opp’n at 31. Even if that were true, which it is not, the Second Hardy Declaration provides ample support. *See* Second Hardy Decl. ¶ 8.

F.3d 1326, 1331 (D.C. Cir. 2014) (quoting *Critical Mass Energy Project v. N.R.C.*, 975 F.2d 871, 878 (D.C. Cir. 1992)).<sup>5</sup> “This requires a showing of both actual competition and a likelihood of substantial competitive injury.” *Id.* “The court will ‘generally defer to the agency’s predictive judgments as to the repercussions of disclosure.’” *Id.* (quoting *United Techs. Corp. v. U.S. Dep’t of Def.*, 601 F.3d 557, 563 (D.C. Cir. 2010)). The FBI has satisfied both metrics.

First, the FBI has shown that there was actual competition at the time and that there would reasonably be competition in the future. As Plaintiffs themselves recognize, Opp’n at 25, there were multiple companies interested in bidding for the iPhone intelligence tool, and thus multiple competitors to the vendor, although only the awarded vendor could actually produce the tool in sufficient time. *See* Justification For Other Than Full & Open Competition, AP-22, ECF No. 15-2, at 72 (“The FBI received at least three inquiries from companies indicating an interest in developing a product for the FBI to access Farook’s iPhone. However, none of these companies had begun to develop or test a solution at the time of the inquiry, and thus would not be able to produce a solution quickly enough to meet the FBI’s investigative requirements.”). The FBI also concluded that the vendor would face actual competition in the future. *See* Second Hardy Decl. ¶ 14 (“[C]onsidering the vendor proved unlocking these types of encrypted devices is possible, and the vendor was paid for its efforts, it is reasonable to assume that their success will spur competition.”). Such future competition is more than sufficient for the actual competition prong. *See, e.g., Gen. Elec. Co. v. Dep’t of Air Force*, 648 F. Supp. 2d 95, 103 (D.D.C. 2009) (“While there was technically no competition for these two contracts – since GE

---

<sup>5</sup> Plaintiffs concede that the FBI has satisfied the other elements of Exemption. Opp’n at 21-22.

was awarded them on a sole source basis – GE has demonstrated that there remains actual competition over both future contracts with the Air Force and contracts with other countries’ air forces . . . .”); *cf. McDonnell Douglas Corp. v. NASA*, 180 F.3d 303, 304-07 (D.C. Cir. 1999) (withholding contract’s pricing information under FOIA Exemption 4 on competitive harm grounds in case where no other contractors submitted proposals for the contract at issue). While Plaintiffs correctly note that the procurement in question was awarded on a sole source basis, Opp’n at 25-26, as the above cases indicate, a sole source contract does not preclude finding actual competition in the future.

Second, the FBI has shown that there is a likelihood of substantial competitive injury to the vendor caused by competitors underbidding future contracts. The FBI concluded that release of the total amount paid to the vendor “could reasonably be assumed to enable potential government contractors with similar technology/methods the opportunity to judge how they might underbid the third party vendor who unlocked Farook’s iPhone when bidding for similar contracts in the future.” Second Hardy Decl. ¶ 14; *see also* First Hardy Decl. ¶ 45; Second Hardy Decl. ¶ 14 (“Should the FBI require similar technology in the future, other vendors could use this information to judge how they might underbid the vendor in question, depriving the vendor of the benefit of future contracts with the FBI.”). It is well established that disclosing pricing information can cause substantial competitive harm by allowing competitors to submit lower bids (or underbid) the submitter. *See, e.g., Canadian Commercial Corp. v. Dep’t of the Air Force*, 442 F. Supp. 2d 15, 36 (D.D.C. 2006), *aff’d* 514 F.3d 37 (D.C. Cir. 2008) (disclosure of prices would likely cause plaintiffs “substantial competitive harm by *informing the bids of its rivals* in the event the contract is rebid”) (quoting *McDonnell Douglas Corp. v. Dep’t of the Air Force*, 375 F.3d 1182, 1190 (D.C. Cir. 2004); *Gen. Elec., Co.*, 648 F. Supp. 2d at 103 (pricing

information is protected from disclosure if it would increase the probability that competitors would underbid contractor in the future). The FBI determined that there was substantial chance of competitive injury in this case, and properly withheld that information on this basis. Second Hardy Decl. ¶ 14. It reasonably did so, and its judgment is entitled to deference. *Jurewicz v. U.S. Dep't of Agric.*, 741 F.3d at 1331 (“The court will generally defer to the agency’s predictive judgments as to the repercussions of disclosure.”).

Plaintiffs remaining objections are unavailing. First, they claim that, while “courts have sanctioned in particular factual scenarios the withholding of line-item pricing data, this is only permitted where the information ‘reveals the inner workings of the contractor, not those of the Government.’” Opp’n at 24 (quoting *McDonnell Douglas Corp.*, 375 F.3d at 1193). But that is not the test. Rather, as the D.C. Circuit has made clear in its more recent decisions, prices are evaluated “as we would any other commercial or financial information,” such that it is exempt if its release would “cause substantial harm to the competitive position of the person from whom the information was obtained.” *Canadian Commercial Corp.*, 514 F.3d at 41. Second, Plaintiffs refer to a routine provision in the contracting documents, Opp’n at 27, which states that “[i]f a request for information contained in a proposal is requested under the FOIA, the Government shall have the right to disclose any information or data contained in a proposal that results in a contract to the extent provided under the FOIA.” See Contract § H.1, Disclosure of Data Under the Freedom of Information Act, AP-38, ECF No. 15-2, at 87. But this provision merely explains the unobjectionable and uncontroversial position that the contract itself is subject to FOIA, something that the FBI does not dispute. It says nothing at all about disclaiming confidentiality over these documents.

The price of the iPhone unlocking tool was properly withheld under Exemption 4.

**CONCLUSION**

For the foregoing reasons, as well as those set out in Defendant's opening brief, this Court should grant Defendant's motion for summary judgment and deny Plaintiffs' cross-motion for summary judgment.

Dated: March 13, 2017

Respectfully submitted,

CHAD A. READLER  
Acting Assistant Attorney General

CHANNING D. PHILLIPS  
United States Attorney for the District of Columbia

ELIZABETH J. SHAPIRO  
Deputy Director

/s/ Joseph E. Borson  
JOSEPH E. BORSON  
Trial Attorney (Virginia Bar No. 85519)  
U.S. Department of Justice,  
Civil Division, Federal Programs Branch  
20 Massachusetts Avenue, NW  
Washington, D.C. 20530  
Telephone: (202) 514-1944  
Facsimile: (202) 616-8460  
E-mail: joseph.borson@usdoj.gov

*Counsel for the Defendant*



**CERTIFICATE OF SERVICE**

I HEREBY CERTIFY that on March 13, 2017, I have electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of electronic filing to the parties.

/s/ Joseph E. Borson