

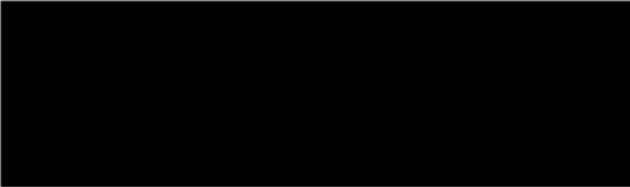


U.S. Department of Justice
Office of Information Policy
441 G Street, NW
Sixth Floor
Washington, DC 20530

Telephone: (202) 514-3642

November 2, 2020

Jason Leopold
Senior Investigative Reporter
BuzzFeed News



Re: DOJ-2019-003097
No. 19-cv-957 (D.D.C.)
VRB:JMB:BRV

Dear Jason Leopold:

This letter is in further response to your Freedom of Information Act (FOIA) request, dated and received in this Office on November 5, 2018, for various records pertaining to Special Counsel Robert S. Mueller III's investigation into Russian interference with the 2016 U.S. presidential election and other related matters.

An updated version of the "Report On The Investigation Into Russian Inference In The 2016 Presidential Election" ("the Report") is enclosed. This updated version will also soon be made available in OIP's online FOIA Library, at <https://www.justice.gov/oip/available-documents-oip> (under the "FOIA-Processed Documents" heading). In this updated version of the Report, certain withholdings that were originally made pursuant to Exemptions 5, 7(A), and 7(E) of the FOIA, 5 U.S.C. § 552(b)(5), (b)(7)(A), and (b)(7)(E) have now been removed.

If you have any questions regarding this letter, please contact Courtney D. Enlow of the Department's Civil Division, Federal Programs Branch at 202-616-8467.

Sincerely,

Vanessa R. Brinkmann
Senior Counsel

Enclosure

B. Russian Hacking and Dumping Operations	175	
1. Section 1030 Computer-Intrusion Conspiracy.....	175	
a. Background	175	
b. Charging Decision As to WikiLeaks, Julian Assange, and Roger Stone.....	176	
2. Potential Section 1030 Violation By (b) (6), (b) (7)(C)	179	(b)(6)/ (b)(7)(C)-2
C. Russian Government Outreach and Contacts.....	180	
1. Potential Coordination: Conspiracy and Collusion.....	180	
2. Potential Coordination: Foreign Agent Statutes (FARA and 18 U.S.C. § 951) .	181	
a. Governing Law.....	181	
b. Application.....	182	
3. Campaign Finance	183	
a. Overview Of Governing Law.....	184	
b. Application to June 9 Trump Tower Meeting.....	185	
i. Thing-of-Value Element	186	
ii. Willfulness	187	
iii. Difficulties in Valuing Promised Information	188	
c. Application to WikiLeaks and Roger Stone.....	188	
i. Questions Over Whether WikiLeaks's Activities Are Covered by the Campaign-Finance Laws.....	189	
ii. Willfulness	190	
iii. Constitutional Considerations	190	
iv. Analysis as to Roger Stone.....	190	
4. False Statements and Obstruction of the Investigation.....	191	
a. Overview Of Governing Law.....	191	
b. Application to Certain Individuals.....	192	
i. George Papadopoulos.....	192	
ii. (b)(6), (b)(7)(C)	194	(b)(6)/ (b)(7)(C)-2
iii. Michael Flynn	194	
iv. Michael Cohen	195	
v. Roger Stone	196	
vi. Jeff Sessions	197	
vii. Others Interviewed During the Investigation.....	198	

and whether prosecution would serve a substantial federal interest that could not be adequately served by prosecution elsewhere or through non-criminal alternatives. *See* Justice Manual § 9-27.220.

Section V of the report provides detailed explanations of the Office's charging decisions, which contain three main components.

First, the Office determined that Russia's two principal interference operations in the 2016 U.S. presidential election—the social media campaign and the hacking-and-dumping operations—violated U.S. criminal law. Many of the individuals and entities involved in the social media campaign have been charged with participating in a conspiracy to defraud the United States by undermining through deceptive acts the work of federal agencies charged with regulating foreign influence in U.S. elections, as well as related counts of identity theft. *See United States v. Internet Research Agency, et al.*, No. 18-cr-32 (D.D.C.). Separately, Russian intelligence officers who carried out the hacking into Democratic Party computers and the personal email accounts of individuals affiliated with the Clinton Campaign conspired to violate, among other federal laws, the federal computer-intrusion statute, and they have been so charged. *See United States v. Netyksho, et al.*, No. 18-cr-215 (D.D.C.). The evidence was not sufficient to charge that former Trump Campaign member Roger Stone joined or participated in the hacking conspiracy. Applying the Principles of Federal Prosecution, the Office also determined not to charge (b) (6), (b) (7)(C) with a misdemeanor computer-intrusion offense (b) (6), (b) (7)(C)

[REDACTED]

(b)(6)/
(b)(7)(C)-2

Second, while the investigation identified numerous links between individuals with ties to the Russian government and individuals associated with the Trump Campaign, the evidence was not sufficient to support criminal charges. Among other things, the evidence was not sufficient to charge any Campaign official as an unregistered agent of the Russian government or other Russian principal. And our evidence about the June 9, 2016 meeting and WikiLeaks's releases of hacked materials was not sufficient to charge a criminal campaign-finance violation. Further, the evidence was not sufficient to charge that any member of the Trump Campaign conspired with representatives of the Russian government to interfere in the 2016 election.

Third, the investigation established that several individuals affiliated with the Trump Campaign lied to the Office, and to Congress, about their interactions with Russian-affiliated individuals and related matters. Those lies materially impaired the investigation of Russian election interference. The Office charged some of those lies as violations of the federal false-statements statute. Former National Security Advisor Michael Flynn pleaded guilty to lying about his interactions with Russian Ambassador Kislyak during the transition period. George Papadopoulos, a foreign policy advisor during the campaign period, pleaded guilty to lying to investigators about, *inter alia*, the nature and timing of his interactions with Joseph Mifsud, the professor who told Papadopoulos that the Russians had dirt on candidate Clinton in the form of thousands of emails. Former Trump Organization attorney Michael Cohen pleaded guilty to making false statements to Congress about the Trump Moscow project. Based on evidence of his lies to Congress and efforts to influence witnesses in the various Russia investigations, a grand jury charged Roger Stone with making false statements, obstruction of justice, and witness tampering. And in February 2019, the U.S. District Court for the District of Columbia found that

(b) (7)(A), (b) (7)(E)

(b)(7)(E)-2

Similar (b) (7)(A), (b) (7)(E) for vulnerabilities continued through the election.

Unit 74455 also sent spearphishing emails to public officials involved in election administration and personnel at companies involved in voting technology. In August 2016, GRU officers targeted employees of VR Systems, a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network. Similarly, in November 2016, the GRU sent spearphishing emails to over 120 email accounts used by Florida county officials responsible for administering the 2016 U.S. election.¹⁹¹ The spearphishing emails contained an attached Word document coded with malicious software (commonly referred to as a Trojan) that permitted the GRU to access the infected computer.¹⁹² The FBI was separately responsible for this investigation. We understand the FBI believes that this operation enabled the GRU to gain access to the network of at least one Florida county government. The Office did not independently verify that belief and, as explained above, did not undertake the investigative steps that would have been necessary to do so.

D. Trump Campaign and the Dissemination of Hacked Materials

The Trump Campaign showed interest in WikiLeaks's releases of hacked materials throughout the summer and fall of 2016. Trump associate Roger Stone made several attempts to contact WikiLeaks founder Assange, boasted of his access to Assange, and was in regular contact with Campaign officials about the releases that Assange made and was believed to be planning. The investigation was unable to resolve whether Stone played a role in WikiLeaks's release of the stolen Podesta emails on October 7, 2016, the same day a video was published of candidate Trump using graphic language about women years earlier.

1. Role of Roger Stone

a. Background

Roger Stone has known President Trump for many years and was an advisor to the Trump Campaign from close to its inception until approximately August 2015. After leaving the Campaign in August 2015, Stone continued to promote the Campaign and maintained regular contact with Trump Campaign members, including candidate Trump and, when they joined the Campaign, with campaign officials Paul Manafort, Steve Bannon, and Rick Gates. According to multiple witnesses involved with the Campaign, beginning in June 2016 and continuing through October 2016, Stone spoke about WikiLeaks with senior Campaign officials, including candidate Trump.

¹⁹¹ *Netyksho* Indictment ¶ 76; (b) (7)(A), (b) (7)(E)

(b) (7)(E), (b) (3), (b) (7)(A), (b) (7)(E)

(b)(7)(E)-2

¹⁹² (b) (7)(A), (b) (7)(E)

(b) (7)(E), (b) (3)

email claimed that WikiLeaks would release “All 33k deleted Emails” by “November 1st.” No emails obtained from Clinton’s server were subsequently released.

Smith drafted multiple emails stating or intimating that he was in contact with Russian hackers. For example, in one such email, Smith claimed that, in August 2016, KLS Research had organized meetings with parties who had access to the deleted Clinton emails, including parties with “ties and affiliations to Russia.”²⁸⁶ The investigation did not identify evidence that any such meetings occurred. Associates and security experts who worked with Smith on the initiative did not believe that Smith was in contact with Russian hackers and were aware of no such connection.²⁸⁷ The investigation did not establish that Smith was in contact with Russian hackers or that Smith, Ledeen, or other individuals in touch with the Trump Campaign ultimately obtained the deleted Clinton emails.

* * *

In sum, the investigation established that the GRU hacked into email accounts of persons affiliated with the Clinton Campaign, as well as the computers of the DNC and DCCC. The GRU then exfiltrated data related to the 2016 election from these accounts and computers, and disseminated that data through fictitious online personas (DCLeaks and Guccifer 2.0) and later through WikiLeaks. The investigation also established that the Trump Campaign displayed interest in the WikiLeaks releases, and that former Campaign member Roger Stone was in contact with the Campaign about those releases, claiming advance knowledge of more to come. As explained in Volume I, Section V.B, *infra*, the evidence was sufficient to support computer-intrusion (and other) charges against GRU officers for their role in election-related hacking. The evidence, however, was not sufficient to charge WikiLeaks, its founder (Assange), or Stone for participating in the hacking conspiracy with those GRU officers.

²⁸⁶ 8/31/16 Email, Smith to Smith.

²⁸⁷ Safron 3/20/18 302, at 3; Szobocsan 3/29/18 302, at 6.

V. PROSECUTION AND DECLINATION DECISIONS

The Appointment Order authorized the Special Counsel’s Office “to prosecute federal crimes arising from [its] investigation” of the matters assigned to it. In deciding whether to exercise this prosecutorial authority, the Office has been guided by the Principles of Federal Prosecution set forth in the Justice (formerly U.S. Attorney’s) Manual. In particular, the Office has evaluated whether the conduct of the individuals considered for prosecution constituted a federal offense and whether admissible evidence would probably be sufficient to obtain and sustain a conviction for such an offense. Justice Manual § 9-27.220 (2018). Where the answer to those questions was yes, the Office further considered whether the prosecution would serve a substantial federal interest, the individuals were subject to effective prosecution in another jurisdiction, and there existed an adequate non-criminal alternative to prosecution. *Id.*

As explained below, those considerations led the Office to seek charges against two sets of Russian nationals for their roles in perpetrating the active-measures social media campaign and computer-intrusion operations. The Office concluded, however, that it did not have sufficient evidence to obtain or sustain a conviction of WikiLeaks or one U.S. national connected to the Campaign (Roger Stone) for participating in the computer-intrusion conspiracy. The Office similarly determined that the contacts between Campaign officials and Russia-linked individuals either did not involve the commission of a federal crime or, in the case of campaign-finance offenses, that our evidence was not sufficient to obtain and sustain a criminal conviction. At the same time, the Office concluded that the Principles of Federal Prosecution supported charging certain individuals connected to the Campaign with making false statements or otherwise obstructing this investigation or parallel congressional investigations.

A. Russian “Active Measures” Social Media Campaign

On February 16, 2018, a federal grand jury in the District of Columbia returned an indictment charging 13 Russian nationals and three Russian entities—including the Internet Research Agency (IRA) and Concord Management and Consulting LLC (Concord)—with violating U.S. criminal laws in order to interfere with U.S. elections and political processes.¹²⁷⁶ The indictment charges all of the defendants with conspiracy to defraud the United States (Count One), three defendants with conspiracy to commit wire fraud and bank fraud (Count Two), and five defendants with aggravated identity theft (Counts Three through Eight). *Internet Research Agency* Indictment. Concord, which is one of the entities charged in the Count One conspiracy, entered an appearance through U.S. counsel and moved to dismiss the charge on multiple grounds. In orders and memorandum opinions issued on August 13 and November 15, 2018, the district court denied Concord’s motions to dismiss. *United States v. Concord Management & Consulting LLC*, 347 F. Supp. 3d 38 (D.D.C. 2018). *United States v. Concord Management & Consulting LLC*, 317 F. Supp. 3d 598 (D.D.C. 2018). As of this writing, the prosecution of Concord remains ongoing before the U.S. District Court for the District of Columbia. The other defendants remain at large.

¹²⁷⁶ A more detailed explanation of the charging decision in this case is set forth in a separate memorandum provided to the Acting Attorney General before the indictment.

the releases, the defendants used the Guccifer 2.0 persona to disseminate documents through WikiLeaks. On July 22, 2016, WikiLeaks released over 20,000 emails and other documents that the hacking conspirators had stolen from the DNC. *Netyksho* Indictment ¶ 48. In addition, on October 7, 2016, WikiLeaks began releasing emails that some conspirators had stolen from Clinton Campaign chairman John Podesta after a successful spearphishing operation. *Netyksho* Indictment ¶ 49.

One witness told the Office at one point that the initial release of Podesta emails on October 7 may have come at the behest of, or in coordination with, Roger Stone, an associate of candidate Trump. As explained in Volume I, Section III.D.1.d, *supra*, phone records show that Stone called Jerome Corsi on October 7, after Stone received a call from the Washington Post. The Washington Post broke a story later that day about a video recording of Trump speaking about women in graphic terms. According to some of Corsi's statements to the Office (b) (3) Stone said that he had learned about the imminent release of that tape recording, and it was expected to generate significant negative media attention for the Campaign. Corsi told investigators that Stone may have believed from their prior dealings that Corsi had connections to Julian Assange, WikiLeaks's founder, and that Stone therefore asked Corsi to tell Assange to start releasing the Podesta emails immediately to shift the news cycle away from the damaging Trump recording. Although Corsi denies that he actually had access to Assange, he told the Office at one point that he tried to bring the request to Assange's attention via public Twitter posts and by asking other contacts to get in touch with Assange. The investigation did not establish that Corsi actually took those steps, but WikiLeaks did release the first batch of Podesta emails later on the afternoon of October 7, within an hour of the publication of the Washington Post's story on the Trump tape.

(b)(3)-1

b. Charging Decision As to WikiLeaks, Julian Assange, and Roger Stone

Given WikiLeaks's role in disseminating the hacked materials, and the existence of some evidence that Stone played a role in coordinating the October 7 release of the Podesta materials, this Office considered whether to charge WikiLeaks, Assange, or Stone as conspirators in the computer-intrusion conspiracy under Sections 1030 and 371.¹²⁷⁸ The theory of prosecution would be that these actors were liable as late joiners in an already existing conspiracy. *See United States v. Bridgeman*, 523 F.2d 1099, 1107 (D.C. Cir. 1975) ("A defendant can join a conspiracy at any

¹²⁷⁸ The Office also considered, but ruled out, charges on the theory that the post-hacking sharing and dissemination of emails could constitute trafficking in or receipt of stolen property under the National Stolen Property Act (NSPA), 18 U.S.C. §§ 2314 and 2315. The statutes comprising the NSPA cover "goods, wares, or merchandise," and lower courts have largely understood that phrase to be limited to tangible items since the Supreme Court's decision in *Dowling v. United States*, 473 U.S. 207 (1985). *See United States v. Yijia Zhang*, 995 F. Supp. 2d 340, 344-48 (E.D. Pa. 2014) (collecting cases). One of those post-*Dowling* decisions—*United States v. Brown*, 925 F.2d 1301 (10th Cir. 1991)—specifically held that the NSPA does not reach "a computer program in source code form," even though that code was stored in tangible items (*i.e.*, a hard disk and in a three-ring notebook). *Id.* at 1302-03. Congress, in turn, cited the *Brown* opinion in explaining the need for amendments to 18 U.S.C. § 1030(a)(2) that "would ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items [is] protected." S. Rep. 104-357, at 7 (1996). That sequence of events would make it difficult to argue that hacked emails in electronic form, which are the relevant stolen items here, constitute "goods, wares, or merchandise" within the meaning of the NSPA.

time, and can properly be convicted though he was not in the conspiracy at its inception.”); *see also United States v. Scott*, 64 F.3d 377, 381 (8th Cir. 1995) (“[E]ven if defendant joined the conspiracy relatively late, played only a minor role, and was unaware of some aspects of the conspiracy, he was legally responsible as a co-conspirator for all acts carried out in furtherance of the conspiracy.”). In particular, although it did not participate in the hacking itself, WikiLeaks would be liable for ensuring a market for and maximizing the value of the stolen materials—much as someone who holds himself out as a “fence” may be found to have joined a conspiracy to traffic in stolen goods, *see United States v. Hess*, 691 F.2d 984, 988 (11th Cir. 1982), and an individual who launders drug money can be a member of a drug-trafficking conspiracy when such laundering activities are “integral to the success” of the overall trafficking venture, *see United States v. Orozco-Prada*, 732 F.2d 1076, 1080 (2d Cir. 1984). *See also, e.g., United States v. Tarantino*, 846 F.2d 1384, 1396-97 (D.C. Cir. 1988); *United States v. Dela Espriella*, 781 F.2d 1432, 1436 (9th Cir. 1986). Stone might similarly be liable under these cases if he too was integral to the computer-intrusion conspiracy’s success by ensuring that the stolen materials had their maximum impact upon dissemination.

The Office determined, however, that it did not have admissible evidence that was probably sufficient to obtain and sustain a Section 1030 conspiracy conviction of WikiLeaks, Assange, or Stone. *See* Justice Manual § 9-27.200. The foregoing theory of conspiracy liability depends on proof of an agreement, *see Iannelli v. United States*, 420 U.S. 770, 777 (1975), whether express or “tacit,” *see United States v. Willson*, 708 F.3d 47, 54 (1st Cir. 2013) (observing that conspiracy may be proved through “a tacit agreement shown from an implicit working relationship”) (internal quotation marks omitted). It would also require evidence of knowledge on the part of the putative conspirator that the criminal objective of the conspiracy has not yet been completed. *Cf. Rosemond v. United States*, 572 U.S. 65, 78-80 (2014). (discussing role of “foreknowledge” in aiding-and-abetting liability). A “fence” who had no advance knowledge of the plan to steal the goods he disposes of, for example, is generally *not* liable for conspiring to steal those goods. *See United States v. Solomon*, 686 F.2d 863, 876 (11th Cir. 1982); *United States v. McGann*, 431 F.2d 1104, 1106-07 (5th Cir. 1970). Here, a late-joiner theory would require that the conspirator knew that the computer intrusions that comprise the Section 1030 violation were ongoing, or expected to continue, at the time that he or she joined the conspiracy.

With respect to WikiLeaks and Assange, this Office determined the admissible evidence to be insufficient on both the agreement and knowledge prongs. As to agreement, many of the communications between the GRU officers and WikiLeaks-affiliated actors occurred via encrypted chats. Although a conspiracy is often inferred from the circumstances, *see Iannelli*, 420 U.S. at 777 n.10, the lack of visibility into the contents of these communications would hinder the Office’s ability to prove that WikiLeaks was aware of and intended to join the criminal venture comprised of the GRU hackers. Similar problems of proof existed as to knowledge. While the investigation developed evidence that the GRU’s hacking efforts in fact were continuing at least at the time of the July 2016 WikiLeaks dissemination, *see Netyksho* Indictment ¶¶ 32, 34, the Office did not develop sufficient admissible evidence that WikiLeaks knew of—or even was willfully blind to—that fact. *Cf. Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 769-70 (2011) (recognizing that willful blindness can be used to prove the knowledge element of an offense). And absent sufficient evidence of such knowledge, the government could not prove that WikiLeaks (or Assange) joined an ongoing hacking conspiracy intending to further or facilitate

additional computer intrusions. *See United States v. Piper*, 35 F.3d 611, 615 (1st Cir. 1994) (conspiracy defendant must have “an intent to effectuate the commission of the substantive offense”); *see also Ingram v. United States*, 360 U.S. 672, 678 (1959) (“Without the knowledge, the intent cannot exist.”) (internal quotation marks and citation omitted).

The Office determined that it could not pursue a Section 1030 conspiracy charge against Stone for some of the same legal reasons. The most fundamental hurdles, though, are factual ones.¹²⁷⁹ As explained in Volume I, Section III.D.1, *supra*, Corsi’s accounts of his interactions with Stone on October 7, 2016 are not fully consistent or corroborated. Even if they were, neither Corsi’s testimony nor other evidence currently available to the Office is sufficient to prove beyond a reasonable doubt that Stone knew or believed that the computer intrusions were ongoing at the time he ostensibly encouraged or coordinated the publication of the Podesta emails. Stone’s actions would thus be consistent with (among other things) a belief that he was aiding in the dissemination of the fruits of an already completed hacking operation perpetrated by a third party, which would be a level of knowledge insufficient to establish conspiracy liability. *See State v. Phillips*, 82 S.E.2d 762, 766 (N.C. 1954) (“In the very nature of things, persons cannot retroactively conspire to commit a previously consummated crime.”) (quoted in Model Penal Code and Commentaries § 5.03, at 442 (1985)).

The Office’s determination that it could not charge WikiLeaks or Stone as part of the Section 1030 conspiracy was also informed by the constitutional issues that such a prosecution would present. Under the Supreme Court’s decision in *Bartnicki v. Vopper*, 532 U.S. 514 (2001), the First Amendment protects a party’s publication of illegally intercepted communications on a matter of public concern, even when the publishing parties knew or had reason to know of the intercepts’ unlawful origin. *Id.* at 517-518. Any effort by WikiLeaks to invoke *Bartnicki* would raise an initial question whether, as a foreign actor, WikiLeaks is entitled to claim the protections of the First Amendment. *Compare DKT Mem’l Fund Ltd. v. Agency for Int’l Dev.*, 887 F.2d 275, 284 (D.C. Cir. 1989) (stating that “aliens beyond the territorial jurisdiction of the United States are generally unable to claim the protections of the First Amendment”), *with Lamont v. Postmaster General*, 381 U.S. 301, 305 (1965) (invalidating a statute based on the First Amendment rights of the addressees to whom the material was directed); *id.* at 308 (Brennan, J., concurring). But assuming that a First Amendment defense is available to WikiLeaks (or that Stone raised one), a court could conclude that *Bartnicki*’s holding applies equally to actors such as WikiLeaks and Stone on the ground that they published or caused the publication of previously hacked materials, without participating directly “in the initial illegality” of the computer intrusions, *see* 532 U.S. at 529.

The government might be able to distinguish *Bartnicki* on the ground that, under the late-joiner principles of conspiracy law described above, WikiLeaks and Stone *were* complicit in the computer intrusions. That contention would succeed only if qualifying as a conspirator under late-joiner principles establishes sufficient participation under *Bartnicki*, a question that the decision itself does not resolve. Regardless, success would also depend upon evidence of WikiLeaks’s and Stone’s knowledge of ongoing or contemplated future computer intrusions—the proof that is

¹²⁷⁹ Some of the factual uncertainties are the subject of ongoing investigations that have been referred by this Office to the D.C. U.S. Attorney’s Office.

currently lacking. The absence of evidence as to knowledge, in short, would both hinder the government's ability to prove conspiracy liability and also potentially provide a First Amendment defense. Therefore, the Office did not seek charges against WikiLeaks, Assange, or Stone for participating in the computer-intrusion conspiracy alleged in Count One of the *Netyksho* indictment.

2. Potential Section 1030 Violation By (b) (6), (b) (7)(C)

(b)(6)/
(b)(7)(C)-2

The Office also considered whether (b) (6), (b) (7)(C) intentionally accessed a protected computer without authorization, in violation of 18 U.S.C. § 1030(a)(2)(C) & (c)(2)(A) (providing penalties for “[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer”). The conduct at issue was (b) (6), (b) (7)(C)

The facts known to the Office likely sufficed to establish each element of a misdemeanor violation of Section 1030(a)(2)(C). (b) (6), (b) (7)(C)

(b) (6), (b) (7)(C) that evidence would support a conclusion (b) (6), (b) (7)(C) “accesse[d] a computer without authorization.” See *United States v. Phillips*, 477 F.3d 215, (b) (6), (b) (7)(C) (5th Cir. 2007) (b) (6), (b) (7)(C)

(b)(6)/
(b)(7)(C)-2

That same course of conduct, and (b) (6), (b) (7)(C) also suggested that (b) (6), (b) (7)(C) acted “intentionally.” See *United States v. Willis*, 476 F.3d 1121, 1125 n.1 (10th Cir. 2007) (explaining that the 1986 amendments to Section 1030 reflect Congress’s desire to reach “‘intentional acts of unauthorized access—rather than mistaken, inadvertent, or careless ones’”) (quoting S. Rep. 99-432, at 5 (1986)). In addition, the computer (b) (6), (b) (7)(C) likely qualifies as a “protected” one under the statute, which reaches “effectively all computers with Internet access.” *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012) (en banc). And (b) (6), (b) (7)(C) likely sufficed to demonstrate (b) (6), (b) (7)(C) “obtained information” from the computer, since the word “obtain” in this provision “includes mere observation of the data,” S. Rep. 99-432, at 6, even without an attempt to copy or download it.

Applying the Principles of Federal Prosecution, however, the Office determined that prosecution of this potential violation was not warranted. Those Principles instruct prosecutors to consider, among other things, the nature and seriousness of the offense, the person’s culpability in connection with the offense, and the probable sentence to be imposed if the prosecution is successful. Justice Manual § 9-27.230. (b) (6), (b) (7)(C)

That fact, among others, would make it difficult to prove that (b) (6), (b) (7)(C) acted to further any crime or tort or (b) (6), (b) (7)(C) obtained information valued at more than \$5,000—which are the kind of circumstances that can trigger felony punishment under the statute. See 18 U.S.C. § 1030(c)(2)(B). (b) (6), (b) (7)(C) the absence of evidence that (b) (6), (b) (7)(C) or obtained valuable information, the

(b)(6)/
(b)(7)(C)-2

did not believe his response to the offer and the June 9 meeting itself violated the law. Given his less direct involvement in arranging the June 9 meeting, Kushner could likely mount a similar defense. And, while Manafort is experienced with political campaigns, the Office has not developed evidence showing that he had relevant knowledge of these legal issues.

iii. Difficulties in Valuing Promised Information

The Office would also encounter difficulty proving beyond a reasonable doubt that the value of the promised documents and information exceeds the \$2,000 threshold for a criminal violation, as well as the \$25,000 threshold for felony punishment. *See* 52 U.S.C. § 30109(d)(1). The type of evidence commonly used to establish the value of non-monetary contributions—such as pricing the contribution on a commercial market or determining the upstream acquisition cost or the cost of distribution—would likely be unavailable or ineffective in this factual setting. Although damaging opposition research is surely valuable to a campaign, it appears that the information ultimately delivered in the meeting was not valuable. And while value in a conspiracy may well be measured by what the participants expected to receive at the time of the agreement, *see, e.g., United States v. Tombrello*, 666 F.2d 485, 489 (11th Cir. 1982), Goldstone’s description of the offered material here was quite general. His suggestion of the information’s value—*i.e.*, that it would “incriminate Hillary” and “would be very useful to [Trump Jr.’s] father”—was non-specific and may have been understood as being of uncertain worth or reliability, given Goldstone’s lack of direct access to the original source. The uncertainty over what would be delivered could be reflected in Trump Jr.’s response (“*if it’s what you say I love it*”) (emphasis added).

Accordingly, taking into account the high burden to establish a culpable mental state in a campaign-finance prosecution and the difficulty in establishing the required valuation, the Office decided not to pursue criminal campaign-finance charges against Trump Jr. or other campaign officials for the events culminating in the June 9 meeting.

c. Application to WikiLeaks and Roger Stone

The Office also considered whether WikiLeaks and anyone connected to the Trump Campaign had liability in connection with WikiLeaks’s months-long releases of stolen emails and other documents, possibly with the aim of influencing the 2016 presidential election, described in Volume I, Section III, *supra*. The Office explored whether WikiLeaks’s actions could constitute a prohibited “expenditure,” 52 U.S.C. § 30121(a)(1)(C), which “includes” “any purchase, payment, distribution, loan, advance, deposit, or gift of money or anything of value, made by any person for the purpose of influencing any election for Federal office,” 52 U.S.C. § 30101(9)(A)(i), but excludes, among other things, “any news story, commentary, or editorial distributed through the facilities of any broadcasting station, newspaper, magazine, or other periodical publication, unless such facilities are owned or controlled by any political party, political committee, or candidate; news stories and non-partisan get-out-the-vote “activities.” 52 U.S.C. § 30101(9)(B)(i) and (ii).

The Office concluded that substantial questions exist about whether the release of emails could be treated as an “expenditure,” whether the government could establish willfulness, and

whether prosecution of this conduct would be subject to a First Amendment defense. In combination, those factors created sufficient doubt that the Office could obtain and sustain a conviction based on WikiLeaks's conduct. There is also insufficient evidence at the present time to establish beyond a reasonable doubt that Roger Stone or any other persons associated with the Campaign coordinated with WikiLeaks on the release of the emails, which alone would preclude prosecution of them for the WikiLeaks-related conduct even if WikiLeaks had violated campaign-finance law. Finally, and in any event, the Office took into consideration several of the legal uncertainties discussed above with respect to June 9.

i. Questions Over Whether WikiLeaks's Activities Are Covered by the Campaign-Finance Laws

Substantial questions exist about whether WikiLeaks's activity in posting documents is covered by the campaign-finance laws. Threshold questions include whether stolen emails constitute "anything of value" as used in the statute defining the term "expenditure," and whether the posting of documents online qualifies as a "gift" or as any of the other types of transactions described in that statute ("purchase, payment, distribution, loan, advance, deposit"). Assuming that they do, two other hurdles would pose challenges.

First, in *Bluman*, a three-judge court held that the ban on foreign-national expenditures (in contrast to contributions or donations) is limited to "expenditures to expressly advocate the election or defeat of a political candidate," i.e., "'express campaign speech' or its 'functional equivalent.'" 800 F. Supp. 2d at 284 (quoting *FEC v. Wisconsin Right to Life, Inc.*, 551 U.S. 449, 456 (2007) (*WRTL*) (opinion of Roberts, C.J.)). That standard would require more than that the posted emails were intended to influence elections and would have that effect. *WRTL*, 551 U.S. at 465-470; see *id.* at 470-475. Rather, they must be "susceptible of no reasonable interpretation other than as an appeal to vote for or against a specific candidate." *Id.* at 469-470; cf. 11 C.F.R. § 100.22 (defining the term "expressly advocating" in the campaign-finance laws as using certain electoral words or phrases or "[w]hen taken as a whole and with limited reference to external events, such as the proximity to the election, could only be interpreted by a reasonable person as containing advocacy of the election or defeat of one or more clearly identified candidate(s)"). If the standard articulated in that decision governs, then it is unlikely that the distribution of emails, divorced from messaging that expressly advocates the election or defeat of a candidate—through particular magic words or the functional equivalent—would satisfy it.

Second, pursuant to its authority to "prescribe rules, regulations, and forms to carry out" the campaign-finance laws, 52 U.S.C. § 30111(a)(8); see *Buckley v. Valeo*, 424 U.S. 1, 110 (1976) (per curiam), the FEC has promulgated regulations that exclude most "internet activity" from the category of expenditures. 11 C.F.R. § 100.155; see also 11 C.F.R. § 100.94 (similar for "contributions"). That regulation generally excludes posting, hosting, blogging, and similar internet activities, where they are "uncompensated." *Id.* That exclusion may well cover WikiLeaks's activities.

ii. Willfulness

As discussed, to establish a criminal campaign-finance violation, the government must prove that the defendant acted “knowingly and willfully.” 52 U.S.C. § 30109(d)(1)(A)(i). That standard requires proof that the defendant knew generally that his conduct was unlawful. *Election Offenses* 123. Given the uncertainties noted above, the “willfulness” requirement would pose a substantial barrier to prosecution.

iii. Constitutional Considerations

Finally, the First Amendment could pose constraints on a prosecution. Even if WikiLeaks, as a non-citizen abroad, could not assert First Amendment rights, *see DKT Mem’l Fund Ltd. v. Agency for Int’l Dev.*, 887 F.2d 275, 284 (D.C. Cir. 1989); *Bahlul v. United States*, 840 F.3d 757, 797 (D.C. Cir. 2016) (en banc) (Millett, J., concurring) (“no governing precedent extends First Amendment protection to speech undertaken by non-citizens on foreign soil”), WikiLeaks could argue that the transmission of information into the United States that did not involve express advocacy implicates the First Amendment rights of American audiences. *See Lamont v. Postmaster General*, 381 U.S. 301, 305 (1965) (treating limits on mailing propaganda into the United States as “a limitation on the unfettered exercise of the addressee’s First Amendment rights”); *see also Bluman*, 800 F. Supp. 2d at 290 (noting that the court’s interpretation of the foreign-expenditure ban “does not restrain foreign nationals from speaking out about issues or spending money to advocate their views about issues”). Assuming that no coordination with the Campaign occurred, a criminal prosecution of overseas actors providing non-express-advocacy information to American listeners would likely be difficult.

iv. Analysis as to Roger Stone

The Office also considered whether Roger Stone could be prosecuted for any direct or indirect contacts with WikiLeaks about its release of hacked emails for the purpose of influencing the presidential election, and whether any coordination between Stone and WikiLeaks would affect WikiLeaks’s criminal exposure. If WikiLeaks’s release of documents were conducted in coordination with Stone (or others associated with the Trump Campaign), the activity would arguably constitute a “contribution,” rather than an “expenditure.” *Cf.* 52 U.S.C. § 30116(a)(7)(B)(i) (“For purposes of this subsection . . . expenditures made by any person in cooperation, consultation, or concert, with, or at the request or suggestion of, a candidate, his authorized political committees, or their agents, shall be considered to be a contribution to such candidate.”). That characterization would potentially render *Bluman*’s express-advocacy limitation inapplicable (because *Bluman* had applied that interpretation only to expenditures made independent of a campaign) and would significantly alleviate the First Amendment concerns identified above (because coordinated election activity would implicate the compelling interest in preventing foreign participation in the U.S. political process and in avoiding quid pro quo corruption or its appearance). *See Citizens United v. FEC*, 558 U.S. 310, 357 (2010); *FEC v. Colorado Republican Fed. Campaign Comm.*, 533 U.S. 431, 444-60 (2001); *Bluman*, 800 F. Supp. 2d at 288.

The Office did not pursue that theory, however, because the investigation did not identify sufficient credible evidence that would establish that Stone coordinated with WikiLeaks or that any contacts with WikiLeaks were attributable to the Campaign. *See* Volume I, Section III.D.1, *supra*. While the Office cannot exclude the possibility of coordination between Stone and WikiLeaks or that additional evidence could come to light on that issue, the investigation did not obtain admissible evidence likely to meet the government’s burden to prove facts establishing such coordination beyond a reasonable doubt.

In any event, even if the Office could establish coordination, arguments premised on a showing of coordination would not address the questions discussed above about whether electronic documents posted on the internet are things of value covered by the campaign-finance laws. Nor would it address the FEC’s regulation providing that uncompensated internet activity is not a contribution, even if done in coordination with a campaign, *see* 11 C.F.R. § 100.94. Those reasons for questioning the applicability of the campaign-finance laws to the facts at issue would similarly make it difficult to establish the general knowledge of illegality necessary to prove a willful violation. *See Election Offenses* 123.

4. False Statements and Obstruction of the Investigation

The Office determined that certain individuals associated with the Campaign lied to investigators about Campaign contacts with Russia and have taken other actions to interfere with the investigation. As explained below, the Office therefore charged some U.S. persons connected to the Campaign with false statements and obstruction offenses.

a. Overview Of Governing Law

False Statements. The principal federal statute criminalizing false statements to government investigators is 18 U.S.C. § 1001. As relevant here, under Section 1001(a)(2), it is a crime to knowingly and willfully “make[] any materially false, fictitious, or fraudulent statement or representation” “in any matter within the jurisdiction of the executive . . . branch of the Government.” An FBI investigation is a matter within the Executive Branch’s jurisdiction. *United States v. Rodgers*, 466 U.S. 475, 479 (1984). The statute also applies to a subset of legislative branch actions—*viz.*, administrative matters and “investigation[s] or review[s]” conducted by a congressional committee or subcommittee. 18 U.S.C. § 1001(c)(1) and (2); *see United States v. Pickett*, 353 F.3d 62, 66 (D.C. Cir. 2004).

Whether the statement was made to law enforcement or congressional investigators, the government must prove beyond a reasonable doubt the same basic non-jurisdictional elements: the statement was false, fictitious, or fraudulent; the defendant knew both that it was false and that it was unlawful to make a false statement; and the false statement was material. *See, e.g., United States v. Smith*, 831 F.3d 1207, 1222 n.27 (9th Cir. 2017) (listing elements); *see also* Ninth Circuit Pattern Instruction 8.73 & cmt. (explaining that the Section 1001 jury instruction was modified in light of the Department of Justice’s position that the phrase “knowingly and willfully” in the statute requires the defendant’s knowledge that his or her conduct was unlawful). In the D.C. Circuit, the government must prove that the statement was actually false; a statement that is misleading but “literally true” does not satisfy Section 1001(a)(2). *See United States v. Milton*, 8 F.3d 39, 45