UNITED STATES DISTRICT COURT
DISTRICT OF COLUMBIA

BUZZFEED, INC. and BEN SMITH,
Plaintiffs,

v.

DEMOCRATIC NATIONAL COMMITTEE,
430 South Capitol Street SE
Washington, DC 20003

Defendant.

MOTION TO COMPEL AND INCORPORATED MEMORANDUM OF LAW

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Federal Cases

State Cases

Constitutional Provisions

Rules

Other Authorities

BuzzFeed, Inc. ("BuzzFeed") and Ben Smith ("Smith") (collectively, "Movants") submit this memorandum of law in support of their motion to compel the Democratic National Committee (the "DNC") to comply with the subpoena issued to them pursuant to Rules 26 and 45 of the Federal Rules of Civil Procedure.[1]

PRELIMINARY STATEMENT

This is a case in which a news organization and its chief editor are being sued for having published information that lies at the heart of one the most important political stories of our day: Russia's efforts to interfere with the 2016 United States presidential election. The underlying Complaint in this action, *Gubarev et al. v. BuzzFeed, Inc.*, No. 17-cv-60426-UU (S.D. Fla.), pending in the Southern District of Florida (the "Florida Litigation"), asserts a claim for defamation based upon an article published by defendant BuzzFeed in January 2017 entitled "These Reports Allege Trump Has Deep Ties to Russia" (the "Article"). The Article includes an embedded document file containing a 35-page collection of memoranda that primarily discuss Russian efforts to influence the 2016 U.S. Presidential election, including alleged ties between Russia and the campaign of President Trump. The collection of reports has since been popularly dubbed "the Trump Dossier" or the "Steele Dossier" (the "Dossier").

The plaintiffs in the Florida Litigation (the "Florida Plaintiffs") assert that they were falsely identified in the penultimate paragraph of the Dossier as having been involved in and/or linked to Russian efforts to hack Democratic political operatives. As part of their defense in this action, Movants are pursuing evidence through discovery that could reasonably lead to admissible evidence that the allegations concerning the Florida Plaintiffs in the Dossier are substantially true: specifically, that "entities linked to" Plaintiff Aleksej Gubarev and Plaintiffs XBT Holdings S.A. ("XBT") and Webzilla, Inc. ("Webzilla") were involved in using "botnets and porn traffic to transmit viruses, plant bugs, steal data, and conduct 'altering operations' against the Democratic Party leadership."

[1] The exhibits supporting this motion are annexed to the Declaration of Katherine M. Bolger, sworn to the 13th day of February 2018 (the "Bolger Decl.").

As part of the discovery process, Movants served a subpoena on the DNC seeking certain technical information that equates to the physical, technical "clues" and "evidence" left behind by the cyber-intruders who breached the DNC's network in 2016, which Movants would use to investigate links between the hackers and the Florida Plaintiffs. The information sought would have been isolated and identified by the DNC and its retained cybersecurity experts CrowdStrike Services Inc. ("CrowdStrike")[2] in the course of their investigation of the 2016 hack.

Movants engaged in numerous discussions with counsel for the DNC, in which Movants repeatedly explained that they are *not* seeking information such as DNC membership lists, donor lists, voter data, strategic plans, or any other substantive content or personally identifiable information created or held by the DNC. Rather, Movants seek information and technical indicators that merely show *how* the hackers breached the DNC's network in 2015 and 2016. In other words, if one analogizes this case to investigating a burglary, Movants are seeking evidence of the fingerprints and tools left behind by the intruders, not a catalogue of the property that they sought or stole from the house. Nevertheless, the DNC ultimately responded with broad objections insisting that (i) Movants were seeking "sensitive political information" such as "membership and donor lists"; (ii) that the requested technical evidence of the hack amounts to commercially sensitive, "First Amendment protected" information; and (iii) that compliance with any of Movants' requests would expose the DNC to further hacking. *See* Bolger Decl. Ex. 4.

The DNC's objections conjure up speculative harms in response to imagined requests that Movants are simply not making. Moreover, the DNC's core objection concerning the sensitivity of the requested information is appropriately addressed by the use of a confidentiality order limiting dissemination of the material – which is already in place in the Florida Litigation[3] – not by allowing them to refuse any production whatsoever. On the other hand, the information sought by Movants is both narrowly tailored and highly relevant to a core issue in the Florida

[2] Movants have also served a companion subpoena *duces tecum* on CrowdStrike, but agreed to toll CrowdStrike's response pending resolution of the instant motion. *See* Bolger Decl. ¶ 6.

[3] *See* Bolger Decl., Ex. 7 (Amended Confidentiality Stipulation and Protective Order in the Florida Litigation), which provides for both "Confidential" and "Attorneys' Eyes Only" designations and specifically contemplates the designation of "highly sensitive technical information" as Attorneys' Eyes Only. *See id.* ¶ 4.

Litigation – the substantial truth or falsity of the allegedly defamatory statements. Accordingly, Movants respectfully request that this Court compel the DNC to comply with their subpoena *duces tecum* pursuant to Rules 26 and 45 of the Federal Rules of Civil Procedure.

FACTUAL BACKGROUND

I. THE HACK OF THE DNC

As most Americans now know, beginning in July 2015 and continuing through much of 2016, known hacking organizations that were closely affiliated with Russian intelligence services launched cyber attacks against the DNC and senior Democratic Party leadership in an effort to influence the 2016 U.S. presidential election and damage the campaign of Democratic presidential candidate Hillary Clinton.[4]

According to the information that has been publicly released to date, the hackers perpetrated these cyber attacks through a technique called "spear phishing," which is an email scam targeted at an individual, organization or business in an attempt to steal information or install malware. In a spear phishing attack, the hackers deploy email messages that are disguised to look like they were sent by a trustworthy source, such as Gmail or another e-mail provider. Bolger Decl. Ex. 5 at 4. The deceptive emails prompt recipients to click on a website link or provide sensitive personal information – for example, by telling the recipient that they need to reset their password. When targets of the attack click on the link and/or provide the requested information, they unwittingly allow the hackers to compromise their computers by, among other things, installing malicious software packages that can be deployed to steal information on the network. The Russian-linked hacking organizations behind the attack on the DNC have been

[4] *See, e.g.*, *Assessing Russian Activities and Intentions in Recent U.S. Elections*, at 2-3, available at https://www.dni.gov/files/documents/ICA_2017_01.pdf (declassified version of classified U.S. intelligence assessment released by FBI, NSA, and CIA) (discussing Russian cyber operations that gained access to the DNC networks and compromised the email accounts of other Democratic Party officials and political figures, leading to the exfiltration of data subsequently provided to Wikileaks for public dissemination).

known to use similar spear phishing methods in the past to infiltrate other networks, including those of U.S. government agencies.[5]

In June 2016, the DNC hired CrowdStrike, a cyber security firm, to respond to a suspected breach. Bolger Decl. Ex. 5 ("CrowdStrike Report") at 3. CrowdStrike took a forensic snapshot of all data on the DNC network, including e-mail information and data on individual computers. *See* Chris Stokel-Walker, *Hunting the DNC hackers: how Crowdstrike found proof Russia hacked the Democrats*, Wired, Mar. 5, 2017. Their investigation confirmed that two "sophisticated" known hacking organizations, colloquially referred to as "Fancy Bear" and "Cozy Bear," had infiltrated the DNC's network. CrowdStrike Report at 3. According to CrowdStrike's public report on its work, these hacking organizations are known to "engage in extensive political and economic espionage for the benefit of the government of the Russian Federation and are believed to be closely linked to the Russian government's powerful and highly capable intelligence services." *Id.* at 3.

CrowdStrike determined that Cozy Bear first infiltrated the DNC network in the summer of 2015 and installed a malicious software package that allowed them to steal information on the DNC network, including email and documents. CrowdStrike Report at 5. Fancy Bear independently breached the DNC's network in April 2016 and deployed another malware package that was also designed to steal data from the network, including the transmission of proprietary files. *Id.* On June 16, 2016, CrowdStrike published a report titled "Bears in the Midst: Intrusion into the Democratic National Committee," which explained, in broad strokes, their analysis and the basis for their conclusion that the DNC had been hacked by Fancy Bear and Cozy Bear. *See* CrowdStrike Report.

While CrowdStrike explained its process and identified certain "Indicators of Compromise," a term used to describe cyber artifacts such as IP addresses or virus remnants —

[5] *See, e.g.*, Danielle Walker, *APT28 orchestrated attacks against global banking sector, firm finds*, SC Magazine, May 13, 2015; Barbara Starr, *Official: Russia Suspected in Joint Chiefs email server intrusion*, CNN, Aug. 7, 2015; Cooper Quintin, *New Spear Phishing Campaign Pretends to be EFF*, Electronic Frontier Foundation, Aug. 27, 2015; Ellen Nakashima, *Russian hackers harassed journalists who were investigating Malaysia Airlines plane crash*," Wash. Post, Sept. 28, 2016.

the equivalent of safe cracker tools left in a safe — that it had located and linked to the two hacking collectives, *id.* at 8-9, it did not reveal the full universe of detailed technical artifacts that it collected and analyzed to come to that conclusion.

II. THE GRIZZLY STEPPE REPORT

On October 7, 2016, the Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (DNI) issued a Joint Analysis Report on election security compromises, designated as GRIZZLY STEPPE. *See* Bolger Decl., Ex. 6. The GRIZZLY STEPPE report "provided technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities," and it included information about both the Russian hack of the DNC and other Russian cyberattacks. *Id.* at 1.

Files accompanying the report contained several hundred Indicators of Compromise, which the Report said were "associated with RIS [Russian Intelligence Services] cyber actors." *Id.* at 5. Among those indicators were at least 13 IP addresses that are affiliated with Root S.A., a wholly owned subsidiary of Plaintiff XBT. Bolger Decl. ¶ 7.

III. THE DOSSIER AND THE FLORIDA LITIGATION

A. The Article and the Dossier

On January 10, 2017, BuzzFeed published an article in entitled "These Reports Allege Trump Has Deep Ties to Russia" (the "Article"). Bolger Decl., Ex. 1 ("Compl.") at Ex. 2. The Article includes an embedded document file containing a 35-page collection of memoranda that primarily discuss Russian efforts to influence the 2016 U.S. Presidential election, including alleged ties between Russia and the campaign of President Trump. Compl. Ex. 3 (the "Dossier"). The collection of reports has since been popularly dubbed "the Trump Dossier" or "the Steele Dossier".

The Article explained what the Dossier was and summarized (both directly, and by linking to other news reports) what had been reported about official use of the Dossier up to that point, including the Dossier's use in briefing the President and President-elect, actions by Senators Reid and McCain with the Dossier, and an FBI investigation into its content. The Article made clear that the allegations in the Dossier were, at that point in time, "unverified."

B. The Florida Litigation

Plaintiffs in the Florida Litigation are Aleksej Gubarev, an alleged "venture capitalist and tech expert" as well as XBT Holdings, S.A. and Webzilla, Inc., companies founded by Mr. Gubarev that "specialize in internet hosting, data and web-development" (collectively, "Plaintiffs"). *See* Compl. ¶ 16. Plaintiffs assert one claim for defamation, specifically alleging that the following allegations in the Dossier are false:

> [O]ver the period March-September 2016 a company called XBT/Webzilla and its affiliates had been using botnets and porn traffic to transmit viruses, plant bugs, steal data and conduct "altering operations" against the Democratic Party leadership. Entities linked to one Aleksei GUBAROV were involved and he and another hacking expert, both recruited under duress by the FSB, Seva KAPSUGOVICH, were significant players in this operation. . . . It was important in this event that all cash payments owed were made quickly and discreetly and that cyber and other operators were stood down/able to go effectively to ground to cover their traces.

See id. ¶¶ 26-27; Dossier at 35.

IV. THE SUBPOENA TO THE DNC

A. The Subpoena

On November 2, 2017, as part of the process of seeking information through discovery that could tend to establish the truth of the allegedly defamatory statement, BuzzFeed issued a subpoena to the DNC seeking production of technical information related to the hack on the DNC (the "Subpoena"). Bolger Decl., Ex. 3. The Subpoena sought only the technical

information/evidence used to show that the hack occurred, and clues left behind that identify the hackers.

Immediately after the Subpoena was served on the DNC, Defendants and the DNC engaged in negotiations regarding the scope of the Subpoena. In particular, Defendants represented to the lawyers from the DNC that Defendants *did not* seek any personal identifying information, including donor rolls or names of individuals to whom the DNC send or receives emails, information about the DNC's computer systems or any confidential information about the DNC's internal systems. Bolger Decl. ¶ 4. The only things that Defendants seek are the technical remnants of the hack, which Defendants hope to use to trace the identity of the hacker.

The data requested includes, but is not limited to:

- Request No. 1 –Information and technical indicators that show how the hacking organizations breached the DNC network in 2015 and 2016. This would include copies of the spear phishing emails and any attachments. Defendants do not seek the names, emails addresses, or other personal information of the individuals who received the phishing emails. Defendants seek merely the details of the sender and the malicious code embedded in the emails or downloaded via link contained within the email; and

- Requests Nos. 2 and 5: The full, unpublished report created by CrowdStrike for the DNC about the hack, and any other reports containing similar analysis conducted or commissioned by the DNC.

- Requests No. 3-4: Copies of unauthorized or foreign code/malware/software used by the hacking organizations that was identified on the network or an individual workstation. Defendants requested *only* the malware sample itself – no part of the DNC's systems are requested.

B. The DNC Response

Despite Defendants' efforts to make clear to the DNC that it sought only a very limited set of information – akin to looking at the tools a burglar leaves in the home, rather than the blueprint of the home itself – the DNC served objections to the subpoena on January 5, 2018. Bolger Decl. Ex. 4.

The DNC made several objections to the Subpoena, including that each request:

> infringes DNC's associational privilege rights guaranteed by the First Amendment to the United States Constitution, because it requests documents detailing the DNC's information technology and cyber security systems, which reveal the DNC's information technology and cyber security systems, which reveal the DNC's methods, strategies, and tactics for protecting sensitive political information. If these documents were disclosed, the DNC's internal operations, as well as its ability to effectively achieve its political goals, would be harmed. Moreover, in the event of the DNC were subjected to yet another hack, the illegal exhilaration and subsequent release of such documents would reveal the DNC's political activates, strategies, and tactics to opponents. Sensitive documents, such as membership and donor lists and reports, could also be disclosed pursuant to a hack, which would have the effect of chilling future political activity. In addition, the DNC objects [to each request] because it seeks documents which may contain DNC computer code, which is also protected by the First Amendment. The DNC further objects to any request for DNC computer code to the extent it constitutes confidential or proprietary business information or commercially sensitive information.

Id. at 6-11.

This motion followed.

ARGUMENT

It is beyond dispute that, pursuant to Fed. R. Civ. P. 45, this Court "has the power to compel documents from a nonparty witness." *In re Denture Cream Prods. Liability Litig.*, 292 F.R.D. 120, 123 (D.D.C. 2013). After the party seeking discovery has made a threshold showing of relevance, the party resisting discovery bears the burden "to show that the documents requested are either unduly burdensome or privileged." *Id*; *see also Cartagena v. Centerpoint Nine, Inc.*, 303 F.R.D. 109, 112 (D.D.C. 2014). In deciding a motion to compel, "a court must consider first whether the discovery sought is relevant." *In re Denture Cream Litig.*, 292 F.R.D. at 123. Relevance is construed as liberally as it is under Fed. R. Civ. P. 26(b), which allows parties to "obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense." *Id.* Accordingly, on a motion to compel production pursuant to Rule 45, discovery requests are "considered relevant if there is any possibility that the information sought may be relevant to the claim or defense of any party." *Id.* (citation omitted). Next, a court must

consider whether compliance would present undue burden or require the disclosure of privileged documents. *Id.* at 126-27. Where "there is no indication that the discovery is 'unreasonably cumulative or duplicative,'" and "the discovery appears generally to be unavailable from other sources," the burden does not outweigh the likely benefit. *Id.* at 127.

As discussed in greater detail below, the DNC should be compelled to produce the documents requested.

A. The Subpoena Seeks Information Highly Relevant to BuzzFeed's Ability To Establish The Substantial Truth Of The Dossier

The limited information sought in the Subpoena — the technical remnants of the hack on the DNC — is clearly relevant within the meaning of the Federal Rules. "For purposes of discovery, relevance is liberally construed[,]" and "with respect to a Rule 45 subpoena, a request for discovery should be considered relevant if there is any possibility that the information sought may be relevant to the claim or defense of any party." *In re Denture Cream Litig.*, 292 F.R.D. at 123 (citations omitted).

In fact, the requested information here is highly relevant to BuzzFeed's ability to establish that the alleged defamatory statement is substantially true. It is axiomatic that "'[t]ruth may not be the subject of either civil or criminal sanctions where discussion of public affairs is concerned.'" *Phila. Newspapers, Inc. v. Hepps*, 475 U.S. 767, 777 (1986) (quoting *Garrison v. Louisiana*, 379 U.S. 64, 74 (1964)). It is somewhat of a misnomer to describe truth as an "absolute defense" to a libel claim, however, because the United States Supreme Court has held that the First Amendment requires that, in any libel action involving issues of public concern, the burden of proving falsity must be borne entirely by the *plaintiff*. *Hepps*, 475 U.S. at 775, 777; *Masson v. New Yorker Magazine, Inc.*, 501 U.S. 496, 510-11 (1991). Although the parties in the Florida Litigation disagree over whether the case is governed by the law of Florida or New York, courts in both of those jurisdictions recognize that substantial truth requires only that "the overall 'gist or substance of the challenged statement is true.'" *Chau v. Lewis*, 771 F.3d 118, 129 (2d Cir. 2014) (citation omitted); *see also Smith v. Cuban Am. Nat'l Found.*, 731 So. 2d 702, 708

(Fla. 3d DCA 1999) ("Under the substantial truth doctrine, a statement does not have to be perfectly accurate if the 'gist' or the 'sting' of the statement is true.").

Here, the relevance of the discovery requested by the DNC is so clear as to be self-evident. Indeed, it goes directly to the substantial truth of the allegedly defamatory statement – *i.e.*, whether networks owned by Plaintiffs and/or its affiliates were involved in hacking the DNC. To give a specific example, the malware samples extracted from the DNC servers by CrowdStrike and requested in the Subpoena may bear traces that link them to their creator(s). Defendants seek the samples to determine if they can link them to known information about Plaintiffs. Without the samples, Defendants cannot make that determination conclusively. In short, there is no question that the information requested is highly relevant – even crucial – to establishing the truth of the alleged defamatory statement at issue.

B. The Information Sought By The Subpoena Is Not Privileged.

Moreover, the information sought from the DNC is not privileged. In their Objections, the DNC suggests that the information requested is protected by the associational privilege secured by the First Amendment to the United States Constitution. Bolger Decl. Ex. 4 at 2, 6-8, 10-11. The associational privilege protects against "compelled disclosure of political affiliations and activities," *AFL-CIO v. FEC*, 333 F.3d 168, 175 (D.C. Cir. 2003), because such disclosure "can impose just as substantial a burden on First Amendment rights as can direct regulation." *Id.* In particular, the associational privilege protects the disclosure of this information to avoid the risk of retaliation or harassment. *Id.* As Defendants have represented repeatedly to the DNC and do so again here, Defendants seek no information that could be protected by the associational privilege, because they are not seeking information about DNC donors, e-mail recipients, or any of the other parade of horribles that the DNC's objections assert, without any foundation. Bolger Decl. ¶ 4.

Indeed, the DNC seems tacitly to acknowledge that it is not really asserting an actual, bona fide privilege objection at all. Rather, the DNC expresses the concern that disclosure of the

information sought by Defendants will make it more likely that the DNC is hacked again in the future. And if it were hacked again in the future, then information subject to the associational privilege could be released to the public.

Thus, the DNC is raising a concern about *security* – not privilege. The DNC is concerned that the non-privileged information Movants seek through the Subpoena might somehow cause them to be hacked again. And if it were hacked again, then presumably the information stolen might implicate any number of privileges and other privacy interests –not just the associational privilege. That concern certainly should and can be addressed, but it has nothing to do with whether the information sought by the Subpoena is protected by any privilege. It clearly is not.

The DNC's argument is even farther removed from a genuine privilege objection than was the argument this Court recently rejected in another dispute related to the Dossier, *Bean LLC v. John Doe Bank*, --- F. Supp. 3d ---, 2018 WL 297125 (D.D.C. Jan. 4, 2018). In *Bean LLC*, Fusion GPS – the firm that commissioned the Dossier – argued that the associational privilege protected it from disclosing financial transactions that identified its clients to the House Intelligence Committee, in part because it feared the Committee would leak that information to the media. *Id.* at *8. Notably, unlike the Subpoena at issue here, that subpoena actually did seek documents that would identify Fusion's clients. Nonetheless, in addition to concluding that Fusion lacks associational rights in its commercial information, the court also explained that "it is worth noting that the likelihood of Fusion's financial transactions – let alone the nature of the work being performed for Fusion's client – being made public is quite low" because the records themselves did not disclose the nature of the work and there was no reason to accept the speculative concern that the committee would leak them in violation of the confidentiality it had promised. *Id.* at *9; *see also In re Crawford*, 194 F.3d 954, 959-60 (9th Cir. 1999) (where bankruptcy preparer claimed that he was entitled to omit social security number from filings because it could lead to identity theft, privacy interest was attenuated because, "[t]o weigh properly the privacy interest involved, the dire consequences of identity theft must be discounted by the probability of its occurrence . . . The realization of the injury requires two additional,

nongovernmental elements: (1) an identity thief and (2) a vulnerable account . . . Disclosure [of an SSN therefore] does not lead directly to injury, embarrassment or stigma."). In fact, "remote and speculative" concerns cannot trigger the associational privilege, even where the non-privileged information that is sought might actually incidentally identify some members. *Anderson v. Hale*, 2001 WL 503045, at *6 (N.D. Ill. May 10, 2001) (even if disclosure of email address books could lead to identification of church members, privilege did not apply because "indirect and incidental disclosure of this type is a far cry from … mandating the revelation of membership lists or associations.").

As a result, the DNC's objections do not provide a basis to withhold the requested information. As an initial matter, it is highly doubtful that anything requested in the Subpoena is relevant to a future hack; Defendants do not seek information about the DNC infrastructure or computer systems. They merely seeks the electronic remnants of the first hack. And the DNC has already released some of those indicators of compromise through the CrowdStrike report.

In any event, the DNC's concerns about security can easily be addressed by providing the information pursuant to the Protective Order that is already in place in the Florida litigation, which would limit the use of the requested information to the parties and to this litigation. In fact, "courts 'commonly require parties to produce confidential documents; the confidentiality of those documents is protected not by denying access to them, but by entering a protective order to cover them.'" *Shvartser v. Lekser*, 270 F. Supp. 3d 96, 98 (D.D.C. 2017) (quoting *Promotional Marketing Insights, Inc. v. Affiliated Computer Servs., Inc.*, 2012 WL 3292888, at *1 (D. Minn. Aug. 13, 2012)). *See also English v. Washington Metro. Area Transit Auth.*, --- F.R.D. ---, 2017 WL 4620976, at *17 (D.D.C. Oct. 13, 2017) ("Confidential materials are routinely produced in discovery, and a protective order can be used to safeguard sensitive personal information."); *Covad Commc'ns Co. v. Revonet, Inc.*, 258 F.R.D. 5, 11 (D.D.C. 2009) ("Confidentiality is not a basis for withholding information in the ordinary course if it can be protected by a protective order …."); *Hillerich & Bradsby Co. v. MacKay*, 26 F. Supp. 2d 124, 127-28 (D.D.C.1998) (denying motion to quash subpoena duces tecum where protective order would safeguard the

confidentiality of the information at issue). Indeed, the Protective Order in this case permits third parties to designate information produced in response to a subpoena "Attorneys' Eyes Only," which would shield it even from the parties themselves. Movants would have no objection to the DNC placing that designation on any information produced.

Finally, as to the DNC's claim that it cannot be required to produce computer code because it is "protected by the First Amendment" or constitutes "proprietary business information," Bolger Decl. Ex. 4 at 6, 7, 9-11, these arguments are specious at best. The information sought in the Subpoena is information left behind by the third party hackers, so the DNC has no proprietary or commercially interest in that information – the hackers do. Nor would technical markers left by hackers be the DNC's speech.

In short, none of the requested information is privileged. For this reason, the court should compel the DNC to produce documents responsive to the Subpoena.

C. There Is No Burden On The DNC To Produce This Information

Nor does the Subpoena subject the DNC to undue burden such that it can be excused from responding to the Subpoena. Specifically, the information is not unreasonably cumulative or duplicative and is unavailable from other sources. *In re Denture Cream Litig.*, 292 F.R.D. at 127 (requested discovery not unduly burdensome where "there is no indication that the discovery is 'unreasonably cumulative or duplicative'" and it "appears to generally be unavailable from other sources") (citation omitted).

As an initial matter, it is worth noting that all of the work required to gather these technical artifacts has already been done. DNC hired Crowdstrike to investigate the hack and together the DNC and CrowdStrike collected these indicators of compromise and other requested materials. Bolger Decl. Ex. 5. All the DNC need do is hand over the same materials to Defendants that Crowdstrike evaluated in reaching its conclusions. There is no burden in doing so.

In addition, the information sought can only be obtained from DNC or, potentially, from CrowdStrike. Defendants subpoenaed both entities, but was informed by CrowdStrike that it

would produce no documents without consent from the DNC. Bolger Decl. ¶ 6. Accordingly, there is no other source for this crucial evidence. In sum, the Subpoena is not unduly burdensome.

CONCLUSION

The material requested from the DNC – which amounts only to the digital remnants left by the Russian state operatives who hacked their systems – is highly relevant to Defendants' ability to establish the truth of the allegedly defamatory claims about them in the Dossier. And the DNC has identified neither privilege nor burden that would prevent them from complying with the Subpoena. For all of the foregoing reasons, Movants respectfully request that this Court compel the DNC to comply with the Subpoena. Pursuant to Local Rule 7(f), Movants respectfully request an oral hearing in this matter.

Dated: February 13, 2018

Respectfully submitted,

By: _____
Nathan Siegel
Katherine M. Bolger
Adam Lazier
Alison Schary
DAVIS WRIGHT TREMAINE LLP
1919 Pennsylvania Avenue NW, Suite 800
Washington, DC 20006
(T): (202) 973-4200
(F): (202) 973-4499
nathansiegel@dwt.com
katebolger@dwt.com
adamlazier@dwt.com
alisonschary@dwt.com

OF COUNSEL:
Allison Lucas
Nabiha Syed
BuzzFeed, Inc.
11 E. 18th Street, 13th Floor
New York, NY 10003

Attorneys for Movants BuzzFeed, Inc. and Ben Smith