

# TUNNEL VISION: DURHAM TREATS CITIZENS' RESEARCH INTO REAL PAUL MANAFORT CRIMES LIKE A CRIMINAL CONSPIRACY

*On Monday, both John Durham and Michael Sussmann submitted their motions in limine, which are filings to argue about what can be admitted at trial. They address a range of issues that I'll cover in several posts:*

*Sussmann:*

- *Asks Judge Cooper to immunize Rodney Joffe or dismiss the case (addressed in this post)*
- *Asks to prohibit introduction of privilege logs (addressed in an update to this post predicting something similar would happen)*
- *Argues that Bill Priestap and Trisha Anderson's notes are inadmissible hearsay and unreliable (this post demonstrates similarities between these notes and those altered in the Mike Flynn docket)*
- *Asks to exclude allegations about the reliability of the*

*DNS data or claims about Christopher Steele (see this post)*

*Durham wants to:*

- *Admit witnesses' contemporaneous notes of conversations with the FBI General Counsel*
- *Admit emails referenced in the Indictment and other, similar emails (see this post)*
- *Admit certain acts and statements (including the defendant's February 2017 meeting with a government agency, his December 2017 Congressional testimony, and his former employer's October 2018 statements to the media) as direct evidence or, alternatively, pursuant to Federal Rule of Evidence 404(b)*
- *Exclude evidence and preclude argument concerning allegations of political bias on the part of the Special Counsel (addressed in this post)*
- *Admit an October 31, 2016 tweet by the Clinton Campaign*

*I will link my discussions in serial fashion.*

---

It's a testament to how deep John Durham is in his conspiracy-driven rabbit hole that he assumes a 24-minute meeting between Marc Elias and Michael Sussmann on July 31, 2016 to discuss the "server issue" pertained to the Alfa Bank allegations. Just days earlier, after all, Donald Trump had asked Russia to hack Hillary Clinton, and within hours, Russian hackers obliged by targeting, for the first time, Hillary's home office. Someone who worked in security for Hillary's campaign told me that from his perspective, the Russian attacks on Hillary seemed like a series of increasing waves of attacks, and the response to Trump's comments was one of those waves (this former staffer documented such waves of attack in real time). The Hillary campaign didn't need Robert Mueller to tell them that Russia seemed to respond to Trump's request by ratcheting up their attacks, and Russia's response to Trump would have been an urgent issue for the lawyer in charge of their cybersecurity response.

It's certainly possible this reference to the "server" issue pertained to the Alfa Bank allegations. But Durham probably doesn't know; nor do I. None of the other billing references Durham suggests pertain to the Alfa Bank issue reference a server.

The possibility that Durham is seeing a conspiracy to attack Donald Trump in evidence that could, instead, be evidence of Hillary's campaign response to an unprecedented nation-state attack, is a worthwhile demonstration of the way the two sides in this case have two entirely different theories of the conspiracy that occurred during that election. That's particularly apparent given the competing motions *in limine* seeking both to prohibit and to include a bunch of communications from that period. These motions are not symmetrical. Sussmann moved to,

preclude three categories of evidence  
and/or arguments that the Special

Counsel has suggested it might offer, namely, evidence and arguments concerning: (1) the gathering of DNS data by Mr. Sussmann's former client Rodney Joffe, and/or other data scientists, and fellow business personnel of Mr. Joffe (collectively "Mr. Joffe and Others"); (2) the accuracy of this data and the accuracy of the conclusions and analysis based on this data; and (3) Christopher Steele and information he separately provided to the Federal Bureau of Investigation ("FBI") (including the so-called "Steele Dossier") (all three, collectively, the "Joffe and Steele Conduct").

Sussmann is *not* moving to exclude mention his contact with Fusion GPS or reporters (though he is fighting to keep Christopher Steele out of his trial).

Whereas Durham is seeking to,

(ii) admit emails referenced in the Indictment and other, similar emails, (iii) admit certain acts and statements (including the defendant's February 2017 meeting with a government agency, his December 2017 Congressional testimony, and his former employer's October 2018 statements to the media) as direct evidence or, alternatively, pursuant to Federal Rule of Evidence 404(b),

[snip]

(v) admit an October 31, 2016 tweet by the Clinton Campaign.

Ultimately this is a fight about whether Sussmann's alleged lie amounted to reporting a tip about a real cybersecurity anomaly, as Sussmann maintains, or, as Durham argues, seeding dirt as part of a dirty tricks campaign against Trump.

Predictably, in addition to emails involving Fusion GPS, Durham wants to introduce the emails between Rodney Joffe and researchers – emails to which Sussmann was not privy – as statements of co-conspirators.

In addition, Rule 801(d)(2)(E) authorizes the admission of an out-of-court statement “by a co-conspirator of a party during the course and in furtherance of the conspiracy.” Where a defendant objects to such an admission, however, the district court must find by a preponderance of the evidence that a conspiracy existed and that the defendant and declarant were members of that conspiracy. *Bourjaily v. United States*, 483 U.S. 171, 175-76 (1987). A court can preliminarily admit hearsay statements of co-conspirators, subject to connection through proof of conspiracy. See *United States v. Jackson*, 627 F. 2d 1198, 1218 (D.C. Cir. 1980) (approving procedure). To admit a statement under Rule 801(d)(2)(E), the court must find (i) that there was a conspiracy; (ii) that its members included the declarant and the party against whom the statement is offered; and (iii) that the statement was made during the course of and in furtherance of the conspiracy. *Bourjaily* 483 U.S. at 175.

Importantly, although Rule 801(d)(2)(E) refers to “conspiracy” and “co-conspirators,” the D.C. Circuit has expressly held that “the doctrine is not limited to unlawful combinations.” *United States v. Weisz*, 718 F. 2d 413, 433 (D.C. Cir. 1983). “Rather, the rule, based on concepts of agency and partnership law and applicable in both civil and criminal trials, ‘embodies the long-standing doctrine that when two or more individuals are acting in concert toward a common goal, the out-of-court

statements of one are . . . admissible against the others, if made in furtherance of the common goal.'" United States v. Gewin, 471 F. 3d 197, 201-02 (D.C. Cir. 2006) (citing Weisz, 718 F. 2d at 433)). In quoting and citing the 1974 Senate Advisory Committee note to Rule 801(d)(2)(E), the D.C. Circuit has also explained that "[Rule 801(d)(2)(E)] was meant to carry forward the universally accepted doctrine that a joint venturer is considered as a coconspirator for the purpose of this [R]ule even though no conspiracy has been charged." Weisz, 718 F. 2d at 433 (citations and quotation marks omitted); United States v. Owens, 484 U.S. 554, 562 (1988) (invoking Advisory Committee note in interpreting Federal Rules of Evidence).

Durham describes that the object of that conspiracy was to deal dirt on Donald Trump to the US government and the media.

As an initial matter, the Government expects that the evidence at trial will show that beginning in late July/early August 2016, the defendant, Tech Executive-1, and agents of the Clinton Campaign were "acting in concert toward a common goal," Gewin, 471 F. 3d at 201-02, namely, the goal of assembling and disseminating the Russian Bank-1 allegations and other derogatory information about Trump and his associates to the media and the U.S. government.

[snip]

More specifically, these emails show that the researchers and Tech Executive-1 were acting in concert with the defendant and others to gather and spread damaging information about a Presidential candidate shortly before

the scheduled election.

And that, Durham claims, makes an attempt to understand a cybersecurity anomaly a political act.

In addition, the aforementioned communications demonstrate the materiality of the defendant's lie insofar as they reveal the political origins and purposes for this work. And those political origins are especially probative here because they provided a motive for the defendant to conceal his clients' involvement in these matters.

There is a *great deal* that is alarming and problematic with this schema. For starters, it suggests Sussmann's response to Eric Lichtblau's question asking, "I see Russians are hacking away. any big news?" (in what is clearly a follow-up of earlier conversations about the very real attack on Hillary by Russia) was part of a conspiracy and not a legitimate response to an obvious good faith and important question from a journalist.

Emails, billing records, and testimonial evidence to be offered at trial reflect that during approximately the same time period – and before approaching the FBI about these matters – the defendant provided the Russian Bank-1 allegations to a reporter from a major U.S. newspaper.

Many of the problems in Durham's argument pertain to April Lorenzen, who started looking into this anomaly in June. But Durham – who also wants to make the source of these anomalies an issue at trial – seems to suggest this conspiracy started on some calls and one meeting between Marc Elias, Joffe, and Sussmann that started on August 12.

Testimony at trial will establish that

among the individuals whom Tech Executive-1 and Originator-1 enlisted in this project were researchers at University-1 who were assigned to a then-pending federal cybersecurity contract with a U.S. government agency ("Agency-1"). At the time, Tech Executive-1 was negotiating an agreement between his then-employer ("Internet Company-1") and University-1 to sell large amounts of internet data to the university for use under the Agency-1 contract. The intended purpose of this agreement and University-1's sensitive work with Agency-1 was to gather and analyze internet metadata in order to detect malicious cyberattacks. As set forth in the Indictment, however, Tech Executive-1 and Originator-1 worked with two of these University-1 researchers ("Researcher-1" and "Researcher-2") to mine internet data for the purpose of assisting the aforementioned opposition research.

That is, Durham both includes Lorenzen's earlier actions in his scope, but imagines that the conspiracy in question didn't form until long after she identified the anomaly.

Similarly, Durham holds Sussmann accountable for the eventual articles written by Lichtblau and Franklin Foer, even though Lorenzen was far more involved in that process (and random people like "Phil" who were signing comments Guccifer 2.0 were also pushing the NYT to write a story). After the FBI killed the initial story, Durham has not shown any evidence that Sussmann was pushing the actual Alfa Bank story until after the Lichtblau and Foer stories were published.

Meanwhile, Durham's interpretation of this Lorenzen email – written in the wake of Paul Manafort's firing because his secret influence-peddling for Russian backed Ukrainian Oligarchs had become a campaign liability – is fairly shocking.



NOTE: The Russian money launderers, sometimes assisted by Americans **like those you see listed in the PDF [Tech Executive-1] just shared [the Trump Associates List]**, and *others you'll see in [name redacted]'s next document ...* Cyprus is one of the places they like. That's where [Russian Bank-1]-Forex is organized. Choose .com or .ru when studying their domains ... and remember we don't need a russian IP, domain or company for money to flow from Russians to Trump.

**[Russian Bank-1]-\* has massive tentacles in so many countries including the USA. Regarding this whole project, my opinion is that from DNS all we could gain even in the best case is an \*inference\*.**

*I have not the slightest doubt that illegal money and relationships exist between pro-Russian and pro-Trump, meaning actual people very close to Trump if not himself. And by Putin's traditional style, people Putin controls, but not himself. He controls the oligarchs and they control massive fortunes and cross nearly all major industries in a vast number of countries.*

But even if we found what [Tech Executive-1] asks us to find in DNS we don't see the money flow, and we don't see the content of some message saying "send me the money here" etc.

I could fill out a sales form on two websites, faking the other company's email address in each form, and cause them to appear to communicate with each other in DNS. (And other ways I can think of and I feel sure [Researcher-2] can think of.)

IF [Tech Executive-1] can take the *\*inference\** we gain through this team

exercise ... and cause someone to apply more useful tools of more useful observation or study or questioning ... then work to develop even an inference may be worthwhile.

That is how I understood the task. Because [Tech Executive-1] didn't tell me more context or specific things. What [name redacted] has been digging up is going to wind up being significant. It's just not the case that you can rest assured that Hil[l]ary's opposition research and whatever professional govts and investigative journalists are also digging ... they just don't all come up with the same things or interpret them the same way. But if you find any benefit in what she has done or is doing, you need to say so, to encourage her. Because we are both killing ourselves here, every day for weeks.

I'm on the verge of something interesting with hosts that talk to the list of Trump dirty advisor domain resources, and hosts that talk to [Russian Bank1]-\* domains. Take even my start on this and you have Tehran and a set of Russian banks they talk to. I absolutely do not assume that money is passing thru Tehran to Trump. It's just one of many \*inferences\* I'm looking at.

SAME IRANIAN IP THAT TALKS TO SOME TRUMP ADVISORS, also talks to:

[list of domains redacted]

(Capitals don't mean SUPER SIGNIFICANT it was just a heading.)

Many of the IPs we have to work with are quite MIXED in purpose, meaning that a lot of work is needed to WINNOW down and then you will still only be left in most cases with an \*inference\* not a certainty. Trump/ advisor domains I've been using. **These include ALL from [Tech**

**Executive-1's]** PDF [the Trump Associate's List] *plus more from [name redacted]'s work:*

[list of domains redacted]

[RUSSIAN BANK-1] DOMAINS

[list of domains redacted]

More needs to be added to both lists.

[Durham's bold, my italics]

That's true in part, because Durham suggests the entirety of this email is part of the conspiracy, but it's clear that Lorenzen was working with another person, whose name Durham redacts, who seems arbitrarily excluded from it.

But it's also true because Lorenzen sent it in the wake of Trump's false claim – made in the same appearance where he asked Russia to hack Hillary some more – that he had no business ties to Russia, when in fact he continued to pursue a Trump Tower deal that would have relied on funding from one of two sanctioned banks. She sent it in the wake of Manafort's false claims (and Rick Gates' lies to the press) that served to hide his real ties to Russian-backed oligarchs, including one centrally involved in the Russian effort to tamper in the election, Oleg Deripaska, and his money laundering through Cyprus of payments from those Oligarchs.

Manafort was helped in those lies – in the same weeks as Sussmann met with James Baker!!!! – by the son-in-law of Alfa Bank's co-founder German Khan, Alex Van der Zwaan, who went on to lie about his actions to Mueller. In the same month Sussmann met with Baker, Mueller found probable cause to investigate, Trump got a \$10 million infusion from an Egyptian state-owned bank. Lorenzen's suspicions were not only realistic, but some turned out to be absolutely true.

Similarly, Durham makes much of this email from Lorenzen:

**[Tech Executive-1's]** carefully designed actions provide the possibility of: 1.

causing the adversaries to react. Stop using? Explain? 2. Getting more people with more resources to find out the things that are unknown, whether those be NON-internet channels of connection between Trump, [Healthcare Company1][owners of Healthcare Company-1], [Russian Bank-1] ... money flows, deals, God knows *it could be [owners of Healthcare Company-1's] children married to Russians who run [Russian Bank1]*. Or like Researcher-2 shared, someone's wife vacationing with someone else's wife.

**I have no clue. These are things other people may look into, if they know a direction of interest to look. 3. Legal action to protect our country from people who act against our national interests. I don't care in the least whether I'm right or wrong about VPN from [Russian Bank-1], [TOR] from Russian Bank-1, or just SMTP artifact pointing to a 3-way connection. [Tech Executive1] has carefully crafted a message that could work to accomplish the goals. Weakening that message in any way would in my opinion be a mistake.**  
[Durham's bold, my italics]

Here, again, Lorenzen wonders about suspect ties of those married to the children of Alfa Bank's founders within days of Van der Zwaan taking actions to hide Manafort's ties to Russian-backed oligarchs.

In other words, Durham treats Lorenzen's inferences, some of which turned out not just to be right, but to be *centrally important* to the ongoing Russian attack on the US, as improper dirt on a presidential candidate and not stuff that every citizen of the United States would want to know. Durham is criminalizing a private citizen's effort (one for which he shows no direct tie to the Clinton campaign) to understand real corruption of Trump and his

campaign manager. Durham literally calls this effort to research a political candidate – a core responsibility in a democracy – a “venture to gather and disseminate purportedly derogatory internet data regarding a Presidential candidate.”

This is not the only email that pointed to real criminal evidence pertaining to Russia’s attack in 2016. He cites David Dagon justifying using this data by pointing to the FBI’s investigation into Fancy Bear – the hackers who were *in that same month* still hacking Hillary and trying to hack election infrastructure.

I believe this is at a threshold of probable cause for violation of Commerce Dept sanctions, FEC elections rules, and has releva[n]cy for the Bureau’s Fancy Bear inquiry, etc.\_ I also have some graphs/animations of the Trump [] router, which I can clean up and contribute. (They merely give a glimpse of aggregate volume, since we lack actual flows.) I’d need until the weekend.”

Again, Paul Manafort did turn out to have real ties to the APT 28 operation, Roger Stone appears to have been in direct contact with the GRU-backed persona since before it went public, and Mueller did charge an Oligarch with close ties to Putin, Yevgeniy Prigozhin, with violating FEC election rules. To suggest that it was improper to try to investigate these ongoing crimes in real time – to suggest the investigation is itself a conspiracy – undermines any possibility for a vibrant democracy.

And Durham decided belatedly (Sussmann’s filing makes it clear Durham laid all this out in a March 23 404(b) notice, 5 days past his due date) to argue that all these emails are admissible so he can argue that Joffe asked Sussmann to hide his role in all this so he could hide the emails that show real

investigation into real, ongoing crimes.

Indeed, many of the emails' contents are relevant and not hearsay for the additional reason that they shed important light on the defendant's and Tech Executive-1's "intent, motive, or state of mind," and "help to explain their future conduct." Safavian, 435 F. Supp. at 45–46. In particular, the mere fact that these emails (i) existed in written form prior to the defendant's September 19, 2016 meeting with the FBI and (ii) reflected instances of serious doubts about whether the Russian Bank-1 data might have been "spoofed," a "red herring," "wrong," or a product of "tunnel vision" or bias against Trump, provided Tech Executive-1 and the defendant with motive to conceal the origins and provenance of the Russian Bank-1 allegations from the FBI. In particular, a reasonable jury could infer from these and other facts that Tech Executive-1 made the defendant aware of these prior doubts and therefore supplied the defendant – as Tech Executive-1's representative – with a motive to conceal their client relationship from the FBI General Counsel. A jury could similarly infer that even if Tech Executive-1 did not make the defendant aware of these communications, he nevertheless instructed the defendant to deny the existence of such a client relationship for the same reason (i.e., to avoid the FBI's potential discovery of the doubts reflected in these prior discussions).

Durham's conspiracy theorizing is not just a dangerous attack on citizenship. It is also cherry picking. He has left out a number of the people who were pursuing the DNS question, including those – Matt Blaze and others – whom Sussmann said he had consulted with in his

meeting with Baker, but put in people that Sussmann did not even know.

Sussmann notes he wasn't involved in any of this data-gathering, nor was the Clinton campaign.

There cannot be any credible argument that the data-gathering sheds light on Mr. Sussmann's representation of Mr. Joffe, because there is no evidence that Mr. Sussmann was involved in the data-gathering or that it was being done to give to Mr. Sussmann, as Mr. Joffe's counsel. It is just as specious to suggest that the data-gathering bears on Mr. Sussmann's attorney-client relationship with the Clinton Campaign. There is no evidence that the Clinton Campaign directed or was involved in the gathering of data, via Mr. Sussmann or otherwise. Nor is there any evidence of communications on issues pertinent to the Indictment between Mr. Joffe and the Clinton Campaign. As such, the manner in which data was gathered has no bearing on Mr. Sussmann's attorney-client relationship with the Clinton Campaign.

In what is likely to be a persuasive argument to Judge Cooper, Sussmann argued that the only thing that can be relevant to the charge against him – a false statements charge, not conspiracy to defraud the US – is his state of mind.

Evidence that lacks a connection to the charge or the defendant's scope of knowledge, including as to the defendant's state of mind, is decidedly not relevant. See, e.g., *United States v. Wade*, 512 F. App'x 11, 14 (2d Cir. 2013) (excluding testimony about another act because it "was not temporally or physically linked" to the crime at issue and the "testimony presented a risk of juror confusion and extended litigation of a collateral matter"); *United States v. Libby*, 467 F. Supp. 2d 1, 15-16

(D.D.C. 2006) (rejecting attempts to “elicit . . . what others were told” as “simply irrelevant to the defendant’s state of mind” in a false statements and perjury case); *United States v. George*, 786 F. Supp. 56, 64 (D.D.C. 1992) (without the “crucial link” that “defendant knew what information others had,” that information is not material to the defendant’s state of mind in an obstruction and false statements case); *United States v. Second*, 726 F. Supp. 845, 848-49 (D.D.C. 1989) (information of which the defendant had no knowledge is necessarily immaterial to the defendant’s state of mind, intent, or motive in a false statements case).

[snip]

First, evidence regarding the accuracy of the data or the conclusions drawn from that data is simply irrelevant to the false statement charge against Mr. Sussmann. Mr. Sussmann is not charged with defrauding the government or with a conspiracy to do that or anything else. There is no allegation or evidence that Mr. Sussmann was privy to any of the communications between Mr. Joffe and Others about the data or its analyses that the Special Counsel misleadingly cites in the Indictment.

I think Durham’s bid to include communications with those (Lorenzen and Manos Antonakakis) Sussmann did not have direct contact with is likely to fail. So most of Durham’s conspiracy theorizing will likely remain on the pages of these filings.

But along the way, Durham’s tunnel vision about 2016 led him to forget to exclude the things that *do* go to Sussmann’s state of mind, such as the very real Russian attack on Hillary Clinton and Donald Trump’s public call for more such attacks.



So while Durham may be excluded from claiming that a private citizen's attempt to learn about real crimes by a Presidential candidate before he is elected amounts to a criminal conspiracy, it is too late for Durham now to try to exclude evidence about Sussmann's understanding of Donald Trump's very real role in a hack of his client.