

EXHIBITS TO PLAINTIFFS' OPPOSITION

## EXHIBIT 1

LAW OFFICES  
SMITHWICK & BELENDIUK, P.C.

5026 WISCONSIN AVENUE, N.W.  
SUITE 301  
WASHINGTON, D.C. 20016  
TELEPHONE (202) 363-4050

GARY S. SMITHWICK  
ARTHUR V. BELENDIUK

COUNSEL

MARK B. DENBO  
M. SCOTT JOHNSON

Direct Dial (202) 363-4559  
Email: [abelendiuk@fccworld.com](mailto:abelendiuk@fccworld.com)

June 19, 2025

**BY EMAIL**

Douglas C. Dreier  
Assistant United States Attorney  
U.S. Department of Justice  
601 D Street, NW  
Washington, D.C. 20530  
[Douglas.dreier@usdoj.gov](mailto:Douglas.dreier@usdoj.gov)

Re: Proposed Narrowing of FOIA Request  
*Burleigh v. FCC*,  
Civil Action No. 25-1268 (ABJ)

Dear Mr. Dreier:

Plaintiffs are in receipt of your letter of June 17, 2025. The Federal Communications Commission ("FCC") seeks to further narrow the scope of Plaintiffs' February 25, 2025, Freedom of Information Act ("FOIA") request. The FCC requests that Plaintiffs narrow the scope of the FOIA request to individuals with `doge.eop` email addresses and to a specific list of custodians suggested by the FCC. As discussed herein, while Plaintiffs cannot agree to everything the FCC requests, they are willing to further limit their FOIA request.

The Chairman of the FCC, Brendan Carr is closely associated with the current administration. He wrote the telecommunications chapter for Project 2025, which has been widely seen as a blueprint for the Trump administration. Further, Brendan Carr has a close relationship with Elon Musk. He has been a vocal supporter of Musk's ventures, particularly Starlink. It is reasonable to conclude that he has been actively engaged with Elon Musk and/or the Department of Government Efficiency ("DOGE"), also known as the U.S. DOGE Service ("USDS"). Based on information and belief, Elon Musk and/or DOGE/USDS representatives have been in contact with Brendan Carr and the FCC staff, at least informally, since before the 2024 presidential election. In its official capacity DOGE has been involved with the FCC since January 20, 2025. It is generally understood, but not officially disclosed, that DOGE has employees embedded at the FCC.

This cannot be confirmed because DOGE/USDS has not released much public information about its personnel.<sup>1</sup>

DOGE has operated with an unusual amount of secrecy. See, *Citizens for Resp. & Ethics in Washington v. U.S. Doge Serv.* (“CREW”), No. 25-cv-511 (CRC), 2025 WL 752367, at \*3 (D.D.C. Mar. 10, 2025). To avoid leaks, people involved with DOGE communicate through Signal. Id. That DOGE and other government officials “operate in secrecy using auto-deleting messaging apps like Signal, [] call[s] into question the Government’s integrity...” Id \*30, citing *Brennan Ctr. for Just. at N.Y.U. Sch. of L. v. Dep’t of Com.*, 498 F. Supp. 3d 87, 97 (D.D.C. 2020). It is unclear to what extent top FCC management communicate with DOGE personnel who use the doge.eop email address.

The available evidence indicates that Carr, the FCC staff and Musk, including other associates or members of DOGE, have been communicating through text messages, messaging apps and private email accounts. The D.C Circuit has made clear that “agency records”—even those stored on a personal email account—are subject to FOIA. *Competitive Enter. Inst. v. Off. of Sci. & Tech. Pol’y*, 827 F.3d 145, 149, 423 U.S. App. D.C. 503 (D.C. Cir. 2016). Thus, for example, if Brendan Carr has exchanged text messages on his mobile phone, used a text messaging app, or exchanging emails on a private email account with Elon Musk, these messages properly fall within Plaintiffs’ FOIA request.

The FCC asks that its search be limited to doge.eop email addresses. This would narrow the scope to such a degree that otherwise producible documents under FOIA would not be provided. It would exclude all emails from individuals who work or have worked for DOGE but have not been assigned or have not used their DOGE emails exclusively. It would exclude all DOGE related communications from the FOIA request start date of October 1, 2024, through at least January 20, 2025, the date DOGE “officially” came into being.

Significantly, the FCC has not represented that it and its personnel communicated with individuals associated with DOGE only through the official doge.eop email address. As we pointed out at our recent meeting with you and FCC counsel, you have given Plaintiffs no assurance that all individuals representing DOGE/USDS before or at the FCC had doge.eop email addresses or used them exclusively in their contacts with the agency. Your letter states that “The FCC would be willing to consider searching for

---

<sup>1</sup> OPM regulations require that information like name and position title of most federal employees be available to the public. 5 C.F.R. § 293.311(a).

Douglas C. Dreier

June 19, 2025

Page 3

communications from additional email domains if provided with examples identifying the additional domains to be searched and demonstrating why searching those domains may lead to responsive records." This is an unreasonable request, as Plaintiffs have no way of knowing who such individuals are or their means of communicating with the FCC. This knowledge resides with the FCC and its managers, who can easily identify the DOGE/USDS representatives and any email or text contacts with the covered senior FCC officials.

In good faith and to expedite the delivery of documents, the Plaintiffs have narrowed their request to the FCC Commissioners, including the Chairman and their staffs, Bureau Chiefs, Deputy Bureau Chiefs and Division Chiefs. This represents the top echelon of FCC managers and the persons who would best know where and when any contacts with DOGE personnel occurred and what form those communications took, i.e. official emails, personal emails, mobile phone texts or Signal messages. In the spirit of compromise and to hasten the process, Plaintiffs offer to drop their request that the FCC's search include the files of Division Chiefs and Deputy Bureau Chiefs. This further reduces the number of accounts and individuals required to search for records.

Plaintiffs do not believe that the FOIA request is overly burdensome, as the FCC claims. Plaintiffs' FOIA request is "reasonably described": it is limited to identified FCC officials, dates and to specific individuals i.e. those associated with DOGE. *See, e.g., Shapiro v. CIA*, 170 F. Supp. 3d 147, 155 (D.D.C. 2016); *Pub. Emps. for Envtl. Resp. v. EPA*, 314 F. Supp. 3d 68, 76 (D.D.C. 2018). However, FOIA does not require every request to be precisely described. After all, "FOIA requesters are frequently in no position to know how an agency classifies its documents or what terminology the agency might have used—that is often why they are making a request in the first place." *Gun Owners of Am., Inc. v. FBI*, 594 F. Supp. 3d 37, 47 (D.D.C. 2022). In this case, the Plaintiffs do not know the email addresses, cell phone numbers or other means of communications used by FCC management to communicate with DOGE volunteers, employees or other individuals associated with DOGE. This is information the FCC needs to provide. The FCC's top management knows the individuals associated with or working for DOGE with whom they have been in contact. The agency can easily determine precisely which records are being requested. Nor are the records difficult to locate. They exist in emails and text messages controlled by the management of the agency. For Plaintiffs to limit the request further, the FCC must provide more information, either as part of this negotiation or through the court's discovery process.

Douglas C. Dreier  
June 19, 2025  
Page 4

Please let us know if you wish to discuss this matter. Ken Levy and I are available most of next week to meet with you.

Sincerely,

/s/ Arthur Belendiuk

Arthur V. Belendiuk  
Counsel for Nina Burleigh and Frequency Forward

EXHIBIT 2

Mr. Adam Candeub  
General Counsel and Designated Agency Ethics Official  
Federal Communications Commission  
54 L Street, N.E.  
Washington, D.C. 20554

Dear Mr. Candeub:

I am a Software Engineer with the Office of the Administrator at the Office Personnel Management. I propose to donate my services as a gift to the Commission pursuant to section 4(g)(3) of the Communications Act, 47 U.S.C. §154(g)(3), and its implementing regulations found at 47 C.F.R., §1.3000, et seq.

Specifically, I propose to voluntarily provide services to the FCC to provide support, expertise, and guidance in facilitating FCC operations and improving information technology (IT) and other systems and improving FCC and governmental efficiency, transparency, and responsibility. I expect to provide 40 hours of my time per week for a period of 120 days, which may be extended for an additional 120 days. The estimated market value of my services for 120 days is \$59,860.

I offer this gift unconditionally, and its acceptance by the Commission is not contingent on any promise or expectation that the Commission's receipt of the gift will benefit me or any other person or entity in any regulatory matter. In addition, I offer my services without expectation of payment and fully understand and agree that I will not receive any compensation therefor from the Federal Communications Commission. Accordingly, I waive any right to seek payment from the government for these services in the future.

Sincerely,

(b) (6)

Tarak Makecha

**Kristi Thompson**

---

**From:** Makecha, Tarak (b) (6)  
**Sent:** Thursday, March 13, 2025 1:33 AM  
**To:** Adam Candeub  
**Cc:** Wick, Jordan (b) (6); EOP/DOGE; Scott Delacourt; Greg Watson  
**Subject:** Re: Process for onboarding to FCC

You don't often get email from (b) (6). [Learn why this is important](#)

Let's go with Friday or Monday when we can have a chance to meet all the key people. Just let me know what works best based on everyone's calendar.

Looking forward to it...

Get [Outlook for iOS](#)

---

**From:** Adam Candeub <Adam.Candeub@fcc.gov>  
**Sent:** Wednesday, March 12, 2025 11:10:05 PM  
**To:** Makecha, Tarak (b) (6) >  
**Cc:** Wick, Jordan (b) (6); EOP/DOGE (b) (6); Scott Delacourt <Scott.Delacourt@fcc.gov>; Greg Watson <Gregory.Watson@fcc.gov>  
**Subject:** FW: Process for onboarding to FCC

Hi Tarak,

Responding to your text, below is the email chain reflecting the last interaction we had with DOGE. Scroll to the end, and it contains instructions re: onboarding. I am cc-ing Scott Delacourt who can provide more additional info.

As I said in my text, I'd be happy to introduce you to people tomorrow. You requested to meet Scott, Greg, Ellen Standiford as well as Sunny Diemart.

My afternoon is pretty jammed, but if you could come around 10.30 I could certainly introduce you to some, if not all, of the people on your list. I just can't speak to everyone's availability at this time.

Alternatively, you could come Friday or Monday and I could arrange a schedule which would ensure that you could meet with everyone in a timely way.

Let me know how to proceed. Thanks so much and looking forward to working with you, Adam

---

**From:** Scott Delacourt <Scott.Delacourt@fcc.gov>  
**Sent:** Friday, February 28, 2025 3:28 PM  
**To:** Lindemann, Kendall (b) (6); EOP/DOGE (b) (6)  
**Cc:** Gleason, Amy (b) (6); EOP/DOGE (b) (6); Ellen Standiford <Ellen.Standiford@fcc.gov>; Greg

**Microsoft Outlook**

**Subject:** depart Spokane WA Alaska Airlines 3650 at 7:05pm arrive Seattle at 8:24pm - Confirmation (b) (6)  
**Location:** from Spokane WA

**Start:** Fri 7/2/2021 10:05 PM  
**End:** Fri 7/2/2021 11:24 PM  
**Show Time As:** Tentative

**Recurrence:** (none)

**Meeting Status:** Not yet responded

**Organizer:** Drema Johnson  
**Required Attendees:** Brendan Carr

**CWT SatoTravel | Your Itinerary**

Trip on Jun 30, 2021 Locator: (b) (6)

Date: Jun 29, 2021

Traveler **BRENDAN CARR** - (b) (6)  
 ATTN-BRENDAN CARR FCC  
 445 12TH ST SW WASHINGTON DC 20554  
 US  
 THIS IS YOUR OFFICIAL RECEIPT FOR TRAVEL PLEASE RETAIN FOR  
 VOUCHERING OR REIMBURSEMENT PURPOSES.

Customer Number (b) (6) Agent EI

**Wednesday, June 30, 2021**

Confirmation (b) (6)



**Flight ALASKA AIRLINES 199**

**DEPARTURE**  
**BALTIMORE WASHNTN, MD**  
 7:15 AM, Jun 30, 2021

**ARRIVAL**  
**SEATTLE/TACOMA, WA**  
 10:00 AM, Jun 30, 2021

Status Confirmed  
 Class Coach Class - Y  
 Duration 05:45 (Non-stop)  
 Equipment Boeing 737 800 Jet  
 Meal Service Snack  
 Reserved Seats 11C (Aisle)  
 Frequent Flyer (b) (6)  
 Notes ONEWORLD

CABIN-ECONOMY

**Wednesday, June 30, 2021**

Confirmation (b) (6)



**Hotel THE HISTORIC DAVENPORT**

**LOCATION**  
 18 SOUTH POST ST  
 SPOKANE, WA US 99201

**CONTACT**  
 Tel 1-509-4558888  
 Fax 1-509-6244455

Reserved For BRENDAN CARR  
 Status Confirmed  
 Check-In Jun 30, 2021  
 Check-Out Jul 02, 2021  
 Number of Rooms 1  
 Rate USD 125.00/night  
 Cancellation Policy Cancel 1 day prior

**Friday, July 02, 2021**

Confirmation (b) (6)



**Flight DELTA AIR LINES INC 3650**

DEPARTURE  
**SPOKANE, WA**  
**7:05 PM, Jul 02, 2021**

ARRIVAL  
**SEATTLE/TACOMA, WA**  
**8:24 PM, Jul 02, 2021**

Status Confirmed  
 Class Coach Class - L  
 Duration 01:19 (Non-stop)  
 Equipment E7W  
 Meal Service None  
 Reserved Seats 16C  
 Notes \*GEG-SEA OPERATED BY /SKYWEST DBA DELTA CONNECTION

CABIN-ECONOMY

**Friday, July 02, 2021**

Confirmation (b) (6)



**Flight UNITED AIRLINES 2497**

DEPARTURE  
**SEATTLE/TACOMA, WA**  
**11:55 PM, Jul 02, 2021**

ARRIVAL  
**CHICAGO/OHARE**  
**5:58 AM, Jul 03, 2021**

Status Confirmed  
 Class Coach Class - K  
 Duration 04:03 (Non-stop)  
 Equipment 7M9  
 Meal Service Dinner  
 Reserved Seats 39D  
 Frequent Flyer (b) (6)  
 Notes ARR-TERMINAL 1

CABIN-ECONOMY

**Saturday, July 03, 2021**

Confirmation (b) (6)



**Flight UNITED AIRLINES 3515**

DEPARTURE  
**CHICAGO/OHARE**  
**7:15 AM, Jul 03, 2021**

ARRIVAL  
**BALTIMORE WASHNTN, MD**  
**10:06 AM, Jul 03, 2021**

Status Confirmed  
 Class Coach Class - M  
 Duration 01:51 (Non-stop)  
 Equipment Embraer Jet  
 Meal Service No Meal Service  
 Reserved Seats 23B  
 Frequent Flyer UAPV550567  
 Notes DEP-TERMINAL 2

\*ORD-BWI OPERATED BY /REPUBLIC AIRWAYS DBA UNITED EXPRESS CABIN-ECONOMY.

Name Invoice / Ticket / Date Base Tax 1 Tax 2 Tax 3 Total

CARR BRENDAN (b) (6) /29JUN21 515.35 61.85 577.20

CARR BRENDAN (b) (5) 29JUN21 126.51 23.89 150.40  
CARR BRENDAN (b) (5) 22JUN21 USD 1,527.07 114.53US 17.20ZP 20.20XT 1,679.00

**Total Amount**

**2,405.60**

Form of Payment: VXXXXXXXXXXXX (b) (5)

**GENERAL INFORMATION**

THANK YOU FOR BOOKING WITH CWTSATOTRAVEL PLEASE NOTE OUR PHONE NUMBERS FOR YOUR ACCOUNT CWTSATOTRAVEL RESERVATIONS 866-809-3517

ONSITE HOURS OF OPERATION ARE MON-FRI 830AM-500PM FOR AN AFTER HOURS EMERGENCY, PLEASE CONTACT CWTSATOTRAVEL AT 866-809-3517.

**\*\*IF INTERNATIONAL 800 NUMBER DOES NOT WORK PLEASE\*\***

FOR INFORMATION ON TSA SECURE FLIGHT PROGRAM VISIT [WWW.TSA.GOV](http://WWW.TSA.GOV)  
RESERVED SEATS SUBJECT TO CANCEL 30 MIN PRIOR TO FLIGHT

FOR AIRPORT SECURITY INFORMATION SEE [WWW.TSA.GOV](http://WWW.TSA.GOV)

UNUSED PAPER TICKETS MUST BE RETURNED TO CWTSATOTRAVEL CONTACT CWTSATOTRAVEL TO REFUND ELECTRONIC TICKETS FARES ARE NOT GUARANTEED UNTIL TICKETED

**From:** [Gregory A. Watson](#)  
**To:** [Brendan Carr](#)  
**Cc:** [Benjamin Arden](#); [Danielle Thumann](#)  
**Subject:** Quick trip update  
**Date:** Friday, June 4, 2021 2:14:03 PM

---

As discussed, quick trip update. Still have a lot of other irons in the fire and running down other leads, but making good progress.

## WA

### Seattle

- TMO 12-1pm (confirmed)
- Options after
  - Boeing plane manufacturing facility
  - SpaceX/starlink manufacturing site, or
  - Fly to Spokane

### Spokane

- Precision Ag (Andrew Nelson family wheat farm visit & tech demo)  
See: <https://www.farmproven.tech>
- Telehealth (CHAS – FCC telehealth winner)
- Tower climb with Legacy Tower/TMO. Near Spokane airport. Serves local Air Force base, 110' water tower. Final antenna install, will make first LTE call using 2.5 GHz spectrum from top of tower.
- Manufacturing visit to Peak Industries in Spokane. NATE member. They make COWs and other tower infrastructure on site.
- CMR's Tech & Innovation Advisory Cmte (broad representation of district stakeholders) – there are some promising leads on the list and I'm working through contacting them.
- NTCA member who serves a dam north of Spokane that is owned by the City of Seattle. Hydropower is a big district interest for CMR.
- ISAAC Foundation (autism and special needs address flag for first responders). (b) (5)

## Idaho

- Intermax WISP. Serves a local airport and has offered to do an aerial tour to see their towers in the area. Also has contacts in the small aircraft manufacturing business. And a contact to fire stations and crews that respond to forest fires. He's offered to go fly fishing, too.

## Oregon

- So far, only one lead here with NTCA member with an active build along our main route. Still looking for more leads in this area, but there are a few irons in the fire.

CenturyLink is one of the main service providers in the region. They are getting back to me with possible options early next week.

NE Oregon and SW Washington is wine country, so I think that could be a unique precision ag type visit and am looking for a lead on that.

**Greg Watson**

Policy Advisor

FCC Commissioner Brendan Carr

EXHIBIT 3

1  
2 UNITED STATES DISTRICT COURT  
3 FOR THE SOUTHERN DISTRICT OF NEW YORK

4 THE AUTHORS GUILD, et al., )  
5 Plaintiffs, )  
6 vs. ) Civil Action No.  
7 NATIONAL ENDOWMENT FOR THE ) 25-cv-3923  
8 HUMANITIES, et al., )  
9 Defendants. )  
\_\_\_\_\_ )

10  
11  
12  
13  
14 VIDEO-RECORDED DEPOSITION OF  
15 JUSTIN FOX  
16 New York, New York  
17 Wednesday, January 28, 2026  
18  
19  
20  
21  
22

23 Reported Stenographically By:  
24 PATRICIA A. BIDONDE  
25 Registered Professional Reporter  
Realtime Certified Reporter  
JOB#: 2026-1011068

30

1 J. Fox  
2 communicating with before you were issued a  
3 government phone?  
4 A. Anthony Armstrong, Josh Gruenbaum,  
5 Nate Cavanaugh.  
6 Q. Anyone else?  
7 A. Ethan Shaotran.  
8 Q. Who were the first two people?  
9 A. Anthony Armstrong.  
10 Q. Who is that?  
11 A. One of the leadership within DOGE  
12 that I initially communicated with.  
13 Q. Okay. And who is the second name?  
14 A. Josh Gruenbaum.  
15 Q. Who is that?  
16 A. Head of federal acquisition  
17 services for GSA.  
18 Q. Okay. Thank you. And how -- you  
19 said you were communicating with them via  
20 Signal?  
21 A. Signal.  
22 Q. And nothing else besides Signal?  
23 A. No.  
24 Q. Was that group chat or were they  
25 individual communications with each one of

31

1 J. Fox  
2 them?  
3 A. Some group chat, some individual.  
4 Q. Okay. And then once you were  
5 hired by the government, did you migrate all  
6 of those communications to your government  
7 phone?  
8 MS. DOUD: Objection.  
9 A. With those individuals, no.  
10 Q. Okay. So you were still  
11 communicating with Nate Cavanaugh, Ethan  
12 Shaotran, and the other two on your personal  
13 phone after being hired. Is that right?  
14 A. Yes.  
15 Q. Okay. And did you do anything to  
16 search those communications in response to any  
17 of those requests that we've gone through from  
18 your subpoena?  
19 A. They were all deleted  
20 automatically. That's the default setting in  
21 Signal.  
22 Q. And you don't think that you ever  
23 spoke to them on any other service beyond  
24 Signal, including Nate, for instance?  
25 A. No.

32

1 J. Fox  
2 Q. The Signal platform, can you tell  
3 me a little bit about it. You mentioned auto  
4 delete, can you explain what you mean.  
5 MS. DOUD: Objection.  
6 A. It's a messaging and calling  
7 platform that everybody was using that I  
8 downloaded to communicate with Nate, Josh,  
9 Anthony.  
10 Q. Okay. Did you download it  
11 specifically to communicate with those people?  
12 How did they tell you to download Signal?  
13 A. Download Signal and call me there.  
14 Q. Okay. But did they tell you that  
15 in person?  
16 A. Anthony Armstrong, I had -- he was  
17 a mentor of mine. And he said, Download  
18 Signal, I want to talk to you about  
19 potentially joining. So all of our  
20 communications were on Signal.  
21 Q. Okay. How did Mr. Armstrong tell  
22 you that?  
23 A. In person.  
24 Q. In person. Okay. Were you  
25 sharing text messages with Mr. Armstrong

33

1 J. Fox  
2 before you downloaded Signal?  
3 A. Yes.  
4 Q. Ever about DOGE?  
5 A. No.  
6 Q. Did you search those texts to come  
7 to the understanding that you never texted him  
8 about DOGE?  
9 A. I remember him being very focused  
10 on switching to Signal to talk about anything.  
11 Q. Okay. Thank you. I appreciate  
12 that. So stepping back from all these  
13 communications.  
14 MR. ONAYEMI: And we can pull  
15 down Exhibit 1, thank you, Jacob.  
16 Q. Did you bring any documents with  
17 you today to the deposition?  
18 A. No.  
19 Q. When did you first become aware of  
20 this lawsuit?  
21 A. At some point in government. I  
22 don't remember when exactly.  
23 Q. Do you remember how you became  
24 aware of it?  
25 A. Like, a letter came addressed to

EXHIBIT 4

**From:** Cipollone, Elisa  
**To:** Prasad, Shannon; Brendan Carr; Giordano, Michael  
**Cc:** Smith, J.J.; McDonald, Michael  
**Subject:** [EXTERNAL]: RE: PRODUCER INTRO FOR TONIGHT'S INGRAHAM ANGLE - BRENDAN CARR (DC)  
**Date:** Sunday, November 3, 2024 4:44:56 PM

---

CAUTION: This email originated from outside of the Federal Communications Commission. Do not click on links or open attachments unless you recognize the sender and trust the content to be safe. If you suspect this is a phishing attempt, please use the 'Report Message' feature in Microsoft Outlook or forward the email to the NSOC.

One follow up question – Senator Tim Kaine also appeared on SNL last night, is that a problem as well?

From: Cipollone, Elisa  
Sent: Sunday, November 3, 2024 3:39 PM  
To: Prasad, Shannon <Shannon.Prasad@FOX.COM>; Brendan.Carr@fcc.gov; Giordano, Michael <Michael.Giordano@fox.com>  
Cc: Smith, J.J. <JJ.Smith@FOX.COM>; McDonald, Michael <Michael.McDonald@FOX.COM>  
Subject: RE: PRODUCER INTRO FOR TONIGHT'S INGRAHAM ANGLE - BRENDAN CARR (DC)

Hello Brendan,

The topic is on Kamala's SNL appearance last night – if you have any other talking points to add beyond your tweets, feel free to pass along.

Thank you,

Elisa

From: Prasad, Shannon <Shannon.Prasad@FOX.COM <<mailto:Shannon.Prasad@FOX.COM>>>  
Sent: Sunday, November 3, 2024 12:43 PM  
To: Brendan.Carr@fcc.gov <<mailto:Brendan.Carr@fcc.gov>>; Cipollone, Elisa <Elisa.cipollone@FOX.COM <<mailto:Elisa.cipollone@FOX.COM>>>; Giordano, Michael <Michael.Giordano@fox.com <<mailto:Michael.Giordano@fox.com>>>  
Cc: Smith, J.J. <JJ.Smith@FOX.COM <<mailto:JJ.Smith@FOX.COM>>>; McDonald, Michael <Michael.McDonald@FOX.COM <<mailto:Michael.McDonald@FOX.COM>>>  
Subject: PRODUCER INTRO FOR TONIGHT'S INGRAHAM ANGLE - BRENDAN CARR (DC)

Hi Brendan.

Connecting you with Gio and Elisa. They will be your segment producers tonight. We have you hitting around 7:08pm. Booking the DC Bureau Pod 4 for the segment. I have your cell as ~~XXXXXXXXXX~~ Gio and Elisa will provide editorial details and will need talking points.

If you need anything else, just let us know.

Thanks!

-Shannon

Shannon Prasad

Booking Producer

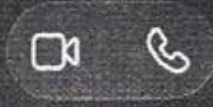
The Ingraham Angle

EXHIBIT 5

9:04



Brendan Carr



Brendan Carr

+1 [redacted]  
No groups in common

The disappearing message time will be set to 1 week when you message them.

+ Message [reply icon] [camera icon] [microphone icon]

Q W E R T Y U I O P  
A S D F G H J K L  
↑ Z X C V B N M [delete icon]  
123 [emoji icon]



EXHIBIT 6



## Federal Communications Commission

### Information Technology and Privacy Rules of Behavior (ROB)

The FCC provides access to Information Technology (IT) computing resources (hardware, software, and information) to its employees and contractor staff. These resources are provided to facilitate completion of assigned responsibilities, with prior authorization. Policies governing FCC computing resources are further detailed in the FCC Cybersecurity and Privacy Policy. The current version of the policy can be found on the FCC IT Intranet page at: <http://intranet.fcc.gov/omd/it/security.php>.

All information contained on FCC computing resources is subject to monitoring by authorized FCC personnel at any time. Individual users of the FCC information and systems should not have any expectation of privacy while accessing FCC computers, networks, or e-mail.

Individuals authorized to use FCC computing resources shall be aware that all FCC-owned computer resources assigned, controlled, accessed, and maintained by FCC employees and contractor personnel are subject to periodic test, review, and audit by the FCC.

All individuals who use FCC computing resources must comply with the FCC Cybersecurity & Privacy Policy, relevant IT policies and procedures, and the specific Rules of Behavior listed below. No bureau or office has the authority to relax or modify the requirements set forth herein. Your acknowledgement of these Rules of Behavior constitute agreement; such compliance is required and is a condition prerequisite of your authorization to use FCC computing resources. You understand that non-compliance may constitute misuse of Government property or resources in violation of Federal regulations and FCC policies and may subject you to criminal, civil, disciplinary, or adverse action.

I agree that:

- I will complete mandatory Computer Security Awareness Training before accessing any FCC system, will complete subsequent refresher training as required, and will comply with all conditions and requirements set forth in such training before and while accessing any FCC system or computer resource.
- I will always comply with all copyright and license restrictions on FCC computing resources.

I will only use FCC computing resources for official FCC business, except that limited personal use is permissible so long as it is *de minimis*, does not interfere with performance of official duties, does not impact the security of information and information systems, does not cause degradation of network services, and does not result in any additional cost to the Agency. I acknowledge that limited personal use does NOT allow for any Prohibited Use, as defined below.

- I will not use FCC computing resources to perform any illegal, unethical, or inappropriate activities. Examples of such Prohibited Uses include, but are not limited to:
  - Viewing, downloading, accessing, searching for, transferring, sharing, storing, creating, sending, or providing access to any type of restricted or inappropriate material, messages, or content
  - Gambling or gaming
  - Lobbying Congress or any other federal, state, or local government with respect to any pending or proposed legislation, resolution, appropriation, or measure
  - Engaging in political activity, including campaigning

- Using, downloading, or distributing illegal copies of copyrighted materials such as software, music, or videos
- Conducting private or personal for-profit activities
- Conducting unauthorized not-for-profit activities, such as solicitation for charities, religious, or political causes. Exceptions to this include, for example, the FCC participation in the Combined Federal Campaign
- Accessing classified information from an unclassified network without a current security clearance and a need to know, even if that information is on the Internet.
- I will abide by applicable federal laws or orders, FCC directives or policies, including, but not limited to, those governing official use of social media, cybersecurity compliance, telework, and remote access.
- I will not access FCC computing resource without utilizing one of the following authorized multi-factor authentication (MFA) methods, in addition to any password and/or PIN required by the relevant system:
  - RSA SecureID (physical or smartphone app)
  - Okta Verify (smartphone app)
  - FCC issued Personal Identity Verification (PIV) card
- I will handle FCC information according to FCC policies and procedures.
  - I request assistance from the Cybersecurity<sup>1</sup> or Privacy<sup>2</sup> team if I have questions regarding the proper handling of FCC information.
- I will log-off or lock devices when unattended as I am responsible for any activity that occurs on my assigned user account.
- I will immediately report any violations or requests by others to violate these Rules of Behavior to the Cybersecurity team.
- I understand that personal credentials (including User IDs and passwords) issued are only for my use, I will not disclose these credentials to anyone at any time for any reason, except as required by the FCC CISO and/or appropriate law enforcement authorities.
  - If I think my credentials are known by another party (someone other than myself) I will change the credentials immediately and create a ticket with the FCC Service Center.
- I understand that ANY document, message, email, or other material sent, received, created, or stored via FCC resources may become an official record, and I have no right to privacy.
- I will not send or post threatening, harassing, intimidating, abusive, or inappropriate material or messages.
- I will not conduct any FCC official business on personal email or forward any non-public data to personal accounts.
- I will not attempt to access any data, systems, or perform any action which is not required in normal execution of my job responsibilities.
  - If I discover I have more access than is required to execute my job responsibilities, then I will immediately report this to the FCC Service Center.
- I will not attempt to bypass any technical or other controls that limit access to computing resources.
  - If additional access is required, I will open a ticket with the FCC Service Center requesting access with proper business justification.
- I will not install any unapproved software on FCC controlled computing resources.
  - If I have questions about whether software is approved, I will create a ticket with the FCC Service Center.
- I will not remove any computing resources from an FCC facility except as required by official FCC business and following all defined policies and procedures.

### Virtual Private Network (VPN)

- Personal VPNs are not to be used, prior to connecting to the FCC network.

<sup>1</sup> cybersecurity@fcc.gov

<sup>2</sup> privacy@fcc.gov

## Telework

- At my alternate workplace, I will follow security practices that are the same as or equivalent to those required of me at my primary workplace.
- I will physically protect any GFE or personal device I use for teleworking when they are not in use.
- I will protect sensitive data at my alternate workplace. This includes disposing of sensitive information by shredding or other appropriate means.
- I will avoid downloading FCC information on personal devices to ensure all data is contained within the FCC network. This includes downloading FCC attachments outside of FCC OneDrive or SharePoint.
  - If I do download attachments to my personal device, I will move the information to an approved FCC storage location such as, OneDrive, SharePoint, or a shared drive. I will permanently delete the information from my personal device.

## Privileged User Access

- I am responsible for all actions taken under my privileged account. I understand that exploitation of my account(s) may have catastrophic effects on all applicable FCC IT resources.
- I will use my Privileged User account only to perform authorized privileged activities.
  - I will use my non-privileged (i.e., general) user account to perform general day-to-day desktop functions (e.g., email, word processing, Internet access, timekeeping).
- I will ensure personally identifiable information (PII) is properly secured and restricted from general access using approved data loss prevention tools and privacy controls as applicable to the environment (e.g., SharePoint, OneDrive, etc.)
- I will not use my privileged account to grant unauthorized privileges to other users to make any unauthorized modifications, access, browse, modify, copy, or delete data/information.
  - I will not access, modify, configure, or use operating systems, cloud environments, software applications or programs except as specifically authorized.
- I will use multifactor authentication (MFA) to perform privileged functions. I will protect the authentication method used from disclosure.
  - If using username/password for a privileged account, I will choose strong, complex passwords in accordance with FCC policy.
  - I will promptly change authentication information whenever compromise is known or suspected.
- I will not make unauthorized copies of security or configuration information (e.g., the etc./password file) for any IT resource.
- I will not attempt to stress, test, circumvent, perform network line monitoring, or conduct keystroke monitoring without authorization.
- I will not connect unauthorized hardware to the FCC network or information system.
- I will not install unauthorized software on FCC information systems (including but not limited to network devices, servers, workstations, appliances, laptops, mobile phones, printers, and copiers).

## Privacy Rules of Behavior

I understand that as an FCC employee or contractor it is my responsibility to comply with FCC policies and measures necessary to prevent the unauthorized access, disclosure, modification, or destruction of personally identifiable information (PII).

- I will comply with the following Rules of Behavior when working with PII:
- I will follow FCC privacy policies and procedures, including FCCINST 1113.2, Compliance with Privacy Laws and Guidance, when handling PII whether in paper or electronic form.

- I will seek guidance from the FCC OGC Privacy Team, my supervisor, or Contracting Officer Representative (COR), as appropriate, if I have any questions on how to protect PII.
- I will complete mandatory training provided by the FCC related to privacy.
- I will not exceed my authority to access PII.
- I will not use PII for a purpose other than that which it is authorized.
- I will not disclose PII to unauthorized persons or entities.

### **Security Incidents and Privacy Reporting**

In the case of a security incident or privacy breach, I will immediately report within 1 hour of discovery, any suspected security or privacy incidents, suspicious behavior, and/or unauthorized access to the Network Security Operations Center (NSOC) at [NSOC-Monitor@fcc.gov](mailto:NSOC-Monitor@fcc.gov).

### **Disciplinary Actions**

I understand that if I do not comply with the ROB, I may be subject to disciplinary or adverse actions and criminal penalties that may be imposed under federal law. I understand that the FCC may take corrective action against employees and contractors who fail to protect data including, but not limited to:

- Removal of an individual's authority to access FCC information systems or data
- Revocation of an individual's security clearance, if applicable
- Employee discipline, up to and including removal
- Contractor suspension or debarment
- Seeking damages under applicable contract law
- Reimbursement to the government for unauthorized charges
- Criminal prosecution

Moreover, legal actions that may result in civil or criminal penalties may also be initiated by third parties including, but not limited to, the Office of Inspector General, the Department of Justice, and individuals harmed by my action or inaction.

## Contact Details

---

**FCC Service Center**  
[Service-Center@fcc.gov](mailto:Service-Center@fcc.gov)  
202-418-1200

## User Certification

---

I certify that I have read the above statements, fully understand my responsibilities, and agree to comply. I recognize that any violation of the requirements indicated above may be cause for disciplinary actions, up to and including removal.

Full Name:

Bureau/Office:

Signature:

Date:

EXHIBIT 7

## Microsoft Outlook

---

**Subject:** Jordan Wick/Scott Delacourt - IT modernization  
**Location:** Microsoft Teams Meeting

**Start:** Fri 7/11/2025 4:00 PM  
**End:** Fri 7/11/2025 4:30 PM  
**Show Time As:** Tentative

**Recurrence:** (none)

**Organizer:** Scott Delacourt  
**Required Attendees:** jordan.wick@gsa.gov

---

## Microsoft Teams [Need help?](#)

### [Join the meeting now](#)

Meeting ID: (b) (6)

Passcode: (b) (6)

---

### Dial in by phone

+1 360-726-3256 (b) (6) United States, Vancouver

[Find a local number](#)

Phone conference ID: (b) (6)

For organizers: [Meeting options](#) | [Reset dial-in PIN](#)

---

### Microsoft Outlook

---

**Subject:** IT planning and oversight

**Location:** Microsoft Teams Meeting

**Start:** Mon 7/14/2025 4:00 PM

**End:** Mon 7/14/2025 4:30 PM

**Recurrence:** (none)

**Meeting Status:** Meeting organizer

**Organizer:** Scott Delacourt

**Required Attendees:** jordan.wick@gsa.gov; Anthony Patrone

**SkypeTeamsProprietary:** (b) (6)

**SkypeTeamsMeeting:** (b) (6)

**SchedulingServiceUpdateUrl:**

(b) (6)

**TeamsVtcTenantId:** (b) (6)

**MeetingTemplateId:** default

---

### Microsoft Teams [Need help?](#)

#### Join the meeting now

Meeting ID: (b) (6)

Passcode: (b) (6)

---

#### Dial in by phone

+1 360-726-3256 (b) (6) United States, Vancouver

[Find a local number](#)

Phone conference ID: (b) (6)

EXHIBIT 8

Q: So, earlier we talked about some of your communications with Mr. Davis, including the context of you emailing yourself. I think you were saying and then using that email on signal to send it to Mr. Davis. Do you ever remember talking about that with Mr. Robinson earlier?

A: I do.

Q: Okay. Walk me through that process exactly.

A: There was a weekly score card, as it was called, where we reported on savings across each agency. It was block text in an excel spreadsheet file that was downloaded. Steve preferred that it be sent over Signal. Signal is not on a government device, so we downloaded it and sent it to Steve on signal. That was the extent of it.

Q: So, Mr. Davis was not on any government device?

A: I don't know if he was on a government device or not. I know he preferred to receive the score card on Signal.

Q: Okay. Have you ever ... do you know whether Mr. Davis had a government email?

A: I believe he had an EOP email address that he did not use.

Q: Okay, and you never communicated with him on that email address?

A: I'm sure I sent him an email or two, but it was incredibly infrequent.

Q: So, I understand sending Mr. Davis something off of email based on his request, but why did you email something to yourself first before sending it to Mr. Davis?

A: There was no other way to get the score cards that we generated to Steve on Signal.

Q: You couldn't go directly from your government email signal?

A: Correct.

Q: Why not?

A: I don't think GSA allowed the downloading of Signal among many other apps.

Q: Okay, so GSA doesn't allow the downloading of Signal? Is that what you are saying?

A: I believe so. Yeah.

Q: Okay. But you then sidestep that by sending documents to your personal phone so that you can then use Signal.

A: Absolutely. For the weekly score card, that was the process, yes.

Q: And that didn't send any alarms about whether or not you should be using Signal to do government work? The fact that GSA didn't let you use signal on your phone?

A: GSA didn't let you use a myriad of software that would have been common in a standard business. And so I don't know if Signal is representative of ... I don't think Signal is a unique case frankly. There are dozens of apps that weren't on a government device.

Q: Do you think there's a reason that the Government disallowed using certain services on their devices?

Objection.

A: I'm not sure.

Q: Okay. Don't you think maybe they were concerned about data leaks or sharing information with people that shouldn't be receiving that information?

Objection

A: I really don't know.

Q: Okay you have no idea why they were not allowed Signal on government funds?

Objection

A: Yeah, I'm not sure. I know many government officials use signal, so I'm not totally sure.

Q: Do you think maybe it was for the maintenance of records that they don't allow Signal and not to delete that from government phones?

Objection

A: Yeah, again I don't know.

Q: You really don't know?

A. I really don't know.