AO 93 (SDNY Rev. 05/10) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Three Electronic Devices, See Attachment A

Case No. 18 MAG 2958

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Southern District of New York
(identify the person or describe the property to be searched and give its location):
Three Electronic Devices, See Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before 4-21-18
(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☑ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court.

✓ Upon its return, this warrant and inventory should be filed under seal by the Clerk of the Court. SLR
USMJ Initials

☑ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☑ for 30 days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 4-7-18 1:55 PM

Judge's signature

City and state: New York, NY

Hon. Henry B. Pitman, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 01/09) Search and Seizure Warrant (Page 2)

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the Court.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

Attachment A

I. Devices to be Searched

The devices to be searched (the "Subject Devices") are described as:

a. *Subject Device-1*: A black and red USB drive with a white label that says "Tracking #: 180208140208."

b. *Subject Device-2*: A silver DVD with a white label that reads "Cohen – 2018.03.07."

c. *Subject Device-3*: A white DVD labelled "2-28-18 Cohen SW Returns – Google and 1&1."

II. Review of ESI on the Subject Devices

Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, interpreters, and outside vendors or technical experts under government control) are authorized to review the ESI contained on the Subject Devices for evidence, fruits, and instrumentalities of one or more violations of 52 U.S.C. §§ 30116(a)(1)(A) and 30109(d)(1)(A)(1) (illegal campaign contributions) (the "Subject Offense"), as listed below:

AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of New York

18 MAG 2958

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Three Electronic Devices, See Attachment A

Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

~~A Device Containing the Results of Three Email Search Warrants, See Attachment A~~
Three Electronic Devices

located in the Southern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

PLEASE SEE ATTACHED AFFIDAVIT AND RIDER.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
52 USC 30116(a)(1)(A), 30109 (d)(1)(A)(1)	Illegal campaign contributions

The application is based on these facts:

PLEASE SEE ATTACHED AFFIDAVIT AND RIDER.

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[redacted]
Printed name and title

Sworn to before me and signed in my presence.

Date: 4-2-2018

Judge's signature

City and state: NEW YORK, NEW YORK

Hon. Henry B. Pitman, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States Of America for a Search Warrant for Three Electronic Devices, USAO Reference No 2018R00127	**TO BE FILED UNDER SEAL** **Agent Affidavit in Support of Application for a Search Warrant**

SOUTHERN DISTRICT OF NEW YORK) ss.:

Special Agent [redacted] of the United States Attorney's Office for the Southern District of New York ("USAO"), being duly sworn, deposes and says:

I. Introduction

A. Affiant

[redacted]

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic devices specified below (the "Subject Devices") for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of

electronically stored information ("ESI"). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. Prior Warrants and the Subject Devices

3. The USAO and the Federal Bureau of Investigation ("FBI") have been investigating, among other things, a scheme by Michael Cohen to defraud multiple banks. Cohen is an attorney who currently holds himself out as the personal attorney for President Donald Trump, and who previously served for over a decade as an executive in the Trump Organization, an international conglomerate with real estate and other holdings.

4. In connection with an investigation then being conducted by the Office of the Special Counsel ("SCO"), the FBI sought and obtained from the Honorable Beryl A. Howell, Chief United States District Judge for the District of Columbia, three search warrants for emails and other content information associated with two email accounts used by Cohen, and one search warrant for stored content associated with an iCloud account used by Cohen. Specifically:

a. On or about July 18, 2017, the FBI sought and obtained a search warrant for emails in the account [redacted]@gmail.com (the "Cohen Gmail Account") sent or received between January 1, 2016 and July 18, 2017. This warrant, which is numbered 17-mj-00503, is attached as Exhibit A (the "First Cohen Gmail Warrant").

b. On or about August 8, 2017, the FBI sought and obtained a search warrant for content stored in the iCloud account associated with Apple ID [redacted]@gmail.com (the "Cohen iCloud Account"). This warrant, which is numbered, 17-mj-00570, is attached as Exhibit D (the "Cohen iCloud Warrant").

c. On or about November 13, 2017, the FBI sought and obtained a search warrant for emails in the Cohen Gmail Account sent or received between June 1, 2015 and November 13, 2017. This warrant, which is numbered 17-mj-00855, is attached as Exhibit B (the "Second Cohen Gmail Warrant").

d. On or about November 13, 2017, the FBI sought and obtained a search warrant for emails in the account [redacted] the "Cohen MDCPC Account") sent or received between the opening of the Cohen MDCPC Account[1] and November 13, 2017. This warrant, which is numbered 17-mj-00854, is attached as Exhibit C (the "First Cohen MDCPC Warrant").

5. The SCO has since referred certain aspects of its investigation into Cohen to the USAO, which is working with the FBI's New York Field Office. As part of that referral, on or about February 8, 2018, the SCO provided the USAO with all non-privileged emails and other content information obtained pursuant to the First Cohen Gmail Warrant, Second Cohen Gmail Warrant, and Cohen MDCPC Warrant. On or about March 7, 2018, the SCO provided the USAO with all non-privileged content obtained pursuant to the Cohen iCloud Warrant.[2] A filter team working with the SCO had previously reviewed the content produced pursuant to these warrants for privilege.

6. On or about February 28, 2018, the USAO sought and obtained search warrants for emails in Cohen Gmail Account and Cohen MDCPC Account, among other accounts, sent or

[1] Based on my review of this warrant and the affidavit in support of it, I know that the warrant did not specify a time period, but the affidavit indicated that, pursuant to court order, the service provider had provided non-content information for the Cohen MDCPC Account that indicated that the account contained emails from the approximate period of March 2017 through the date of the warrant.

[2] The SCO had previously provided a subset of this non-privileged content on or about February 2, 2018.

received between November 14, 2017 and February 28, 2018. These warrants, which are both numbered 18 Mag. 1696, are attached as Exhibits E (the "Third Cohen Gmail Warrant") and F (the "Second Cohen MDCPC Warrant"), respectively. The content produced pursuant to these warrants is being reviewed for privilege by an SDNY filter team.

7. The search warrants described above are referred to collectively herein as the "Prior Warrants."

8. The returns of the Prior Warrants are presently contained on three electronic devices. In particular:

a. *Subject Device-1*: The non-privileged emails and content returned in response to the First Cohen Gmail Warrant, the Second Cohen Gmail Warrant, and the First Cohen MDCPC Warrant are contained on Subject Device-1, which is particularly described as a black and red USB drive with a white label that says "Tracking #: 180208140208."

b. *Subject Device-2*: The non-privileged content returned in response to the Cohen iCloud Warrant is contained on Subject Device-2, which is particularly described as one silver DVD with a white label that reads "Cohen – 2018.03.07."

c. *Subject Device-3*: The content returned in response to the Third Cohen Gmail Warrant and the Second Cohen MDCPC Warrant is contained on Subject Device-3, which is particularly described as one white DVD labelled "2-28-18 Cohen SW Returns – Google and 1&1."

9. The Subject Devices are presently located in the Southern District of New York.

C. The Subject Offenses

10. The affidavits in support of the Prior Warrants describe evidence of several different courses of conduct by Cohen, including, among other things, false statements to financial institutions relating to the purpose of an account he opened in the name of Essential Consultants

LLC and the nature of funds flowing into that account; false statements and fraudulent omissions by Cohen in connection with this attempt to refinance his debts with certain financial institutions; and activities undertaken by Cohen on behalf of certain foreign persons or foreign entities without having registered as a foreign agent. The Prior Warrants accordingly define the evidence to be seized by reference to subject offenses and specific categories of information related to these courses of conduct. The subject offenses in the Prior Warrants are summarized as follows:

Exhibit	Warrant	Subject Offenses in Prior Warrant[3]
A	First Cohen Gmail Warrant	18 U.S.C. §§ 371 (conspiracy to defraud the United States), 1005 (false bank entries), 1014 (false statement to financial institution), 1343 (wire fraud), 1344 (bank fraud), 1956 (money laundering), 951 (acting as an unregistered foreign agent), and 22 U.S.C. §§ 611 *et seq.* (Foreign Agents Registration Act ("FARA"))
B	Second Cohen Gmail Warrant	18 U.S.C. §§ 371 (conspiracy to defraud the United States), 1005 (false bank entries), 1014 (false statement to financial institution), 1343 (wire fraud), 1344 (bank fraud), 1956 (money laundering), 951 (acting as an unregistered foreign agent), and 22 U.S.C. §§ 611 *et seq.* (FARA)
C	Cohen MDCPC Warrant	18 U.S.C. §§ 371 (conspiracy to defraud the United States), 1005 (false bank entries), 1014 (false statement to financial institution), 1343 (wire fraud), 1344 (bank fraud), 1956 (money laundering), 951 (acting as an unregistered foreign agent), and 22 U.S.C. §§ 611 *et seq.* (FARA)
D	Cohen iCloud Warrant	18 U.S.C. §§ 1014 (false statement to financial institution), 1344 (bank fraud), 1956 (money laundering), 951 (acting as an unregistered foreign agent), and 22 U.S.C. §§ 611 *et seq.* (FARA)
E	Third Cohen Gmail Warrant	18 U.S.C. §§ 371 (conspiracy to commit offense or to defraud the United States), 1005 (false bank entries), 1014 (false statements to financial institution), 1343 (wire fraud), 1344 (bank fraud)
F	Second Cohen MDCPC Warrant	18 U.S.C. §§ 371 (conspiracy to commit offense or to defraud the United States), 1005 (false bank entries), 1014 (false statements to financial institution), 1343 (wire fraud), 1344 (bank fraud)

11. Based on my participation in this investigation, including my review of documents obtained pursuant to subpoena and court order, my conversations with witnesses and review of reports of conversations with witnesses, and my review of publicly available information, I have

[3] On or about February 28, 2018, the USAO sought and obtained a Rule 41 warrant, authorizing it to expand its search of the email returns for the warrants attached as Exhibits A-C (the First Cohen Gmail Warrant, Second Cohen Gmail Warrant, and First Cohen MDCPC Warrant) for additional offenses not authorized in the original warrants for those accounts. The below chart therefore lists *both* the subject offenses listed in the original warrants for these accounts and the subject offenses authorized in the February 28, 2018 warrant.

learned of evidence of an additional Subject Offense committed by Cohen, described below, which was not listed in the Prior Warrants.[4]

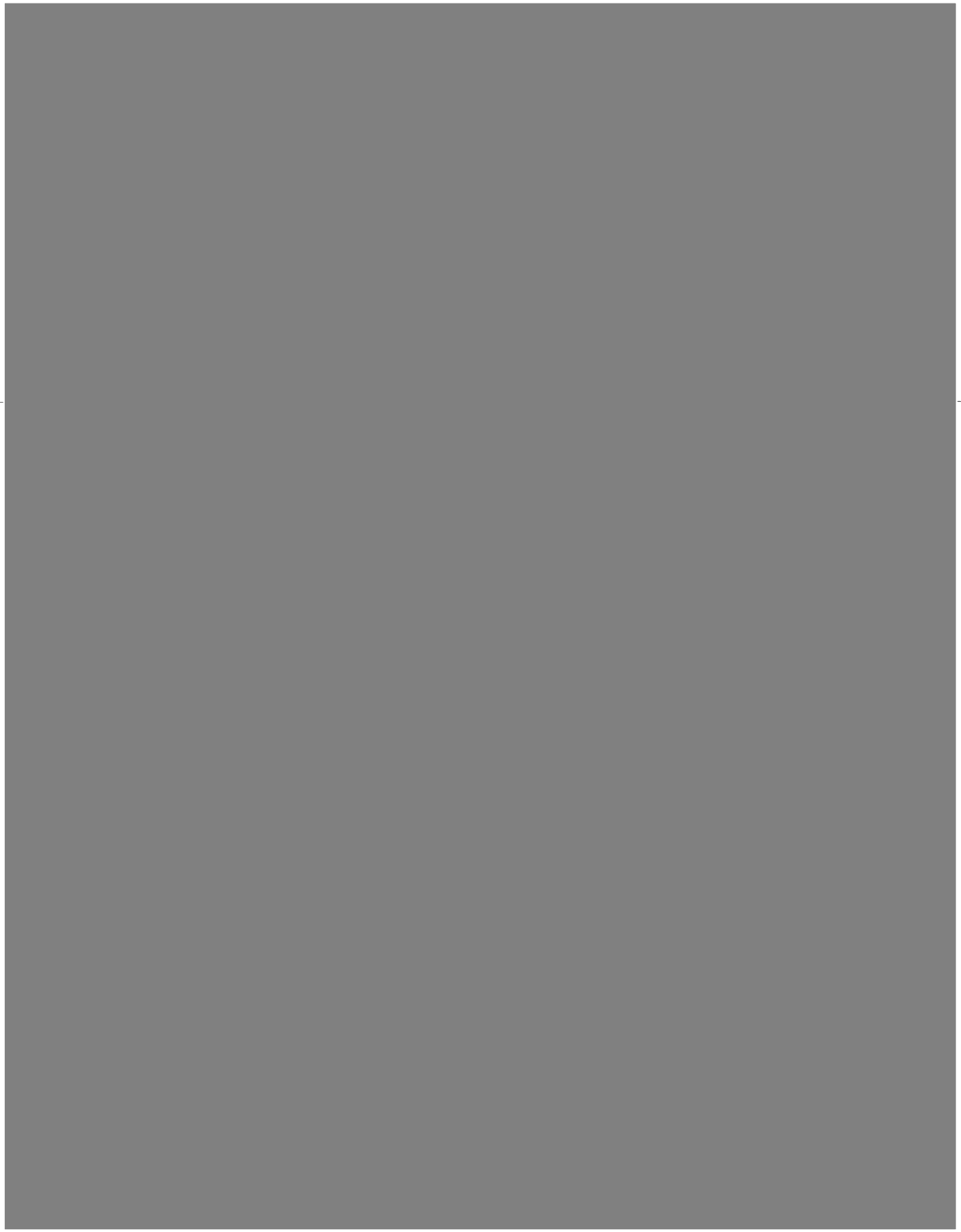
12. I am therefore requesting authority to expand the search of the returns of the Prior Warrants, as contained on the Subject Devices, for evidence related to the additional Subject Offense. As set forth below, in addition to the categories of evidence already described in the Prior Warrants, there is probable cause to believe that the Subject Devices contain evidence of violations of 52 U.S.C. §§ 30116(a)(1)(A) and 30109(d)(1)(A)(1) (illegal campaign contributions) (the "Subject Offense").[5]

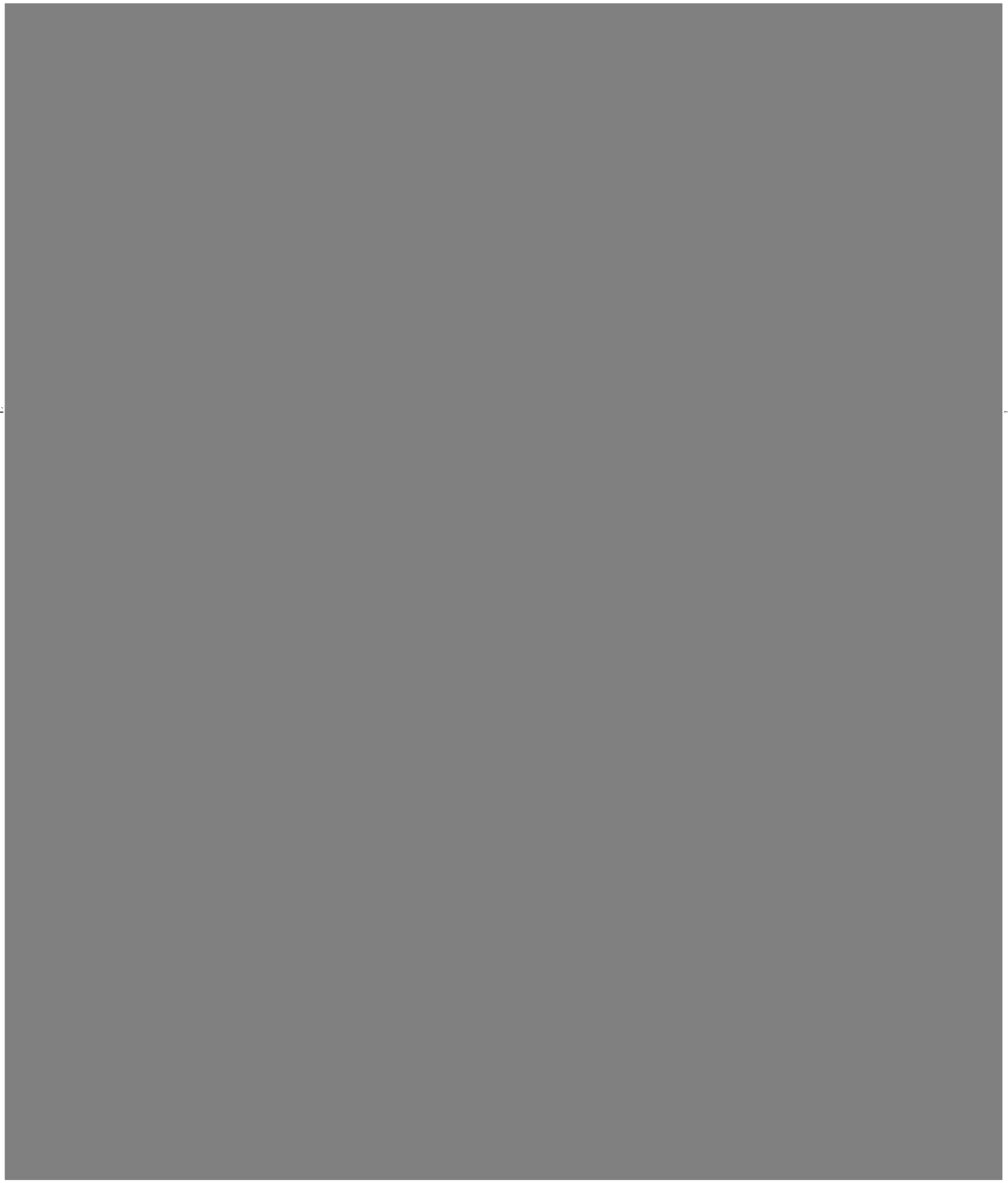
II. Probable Cause Regarding the Subject Offense

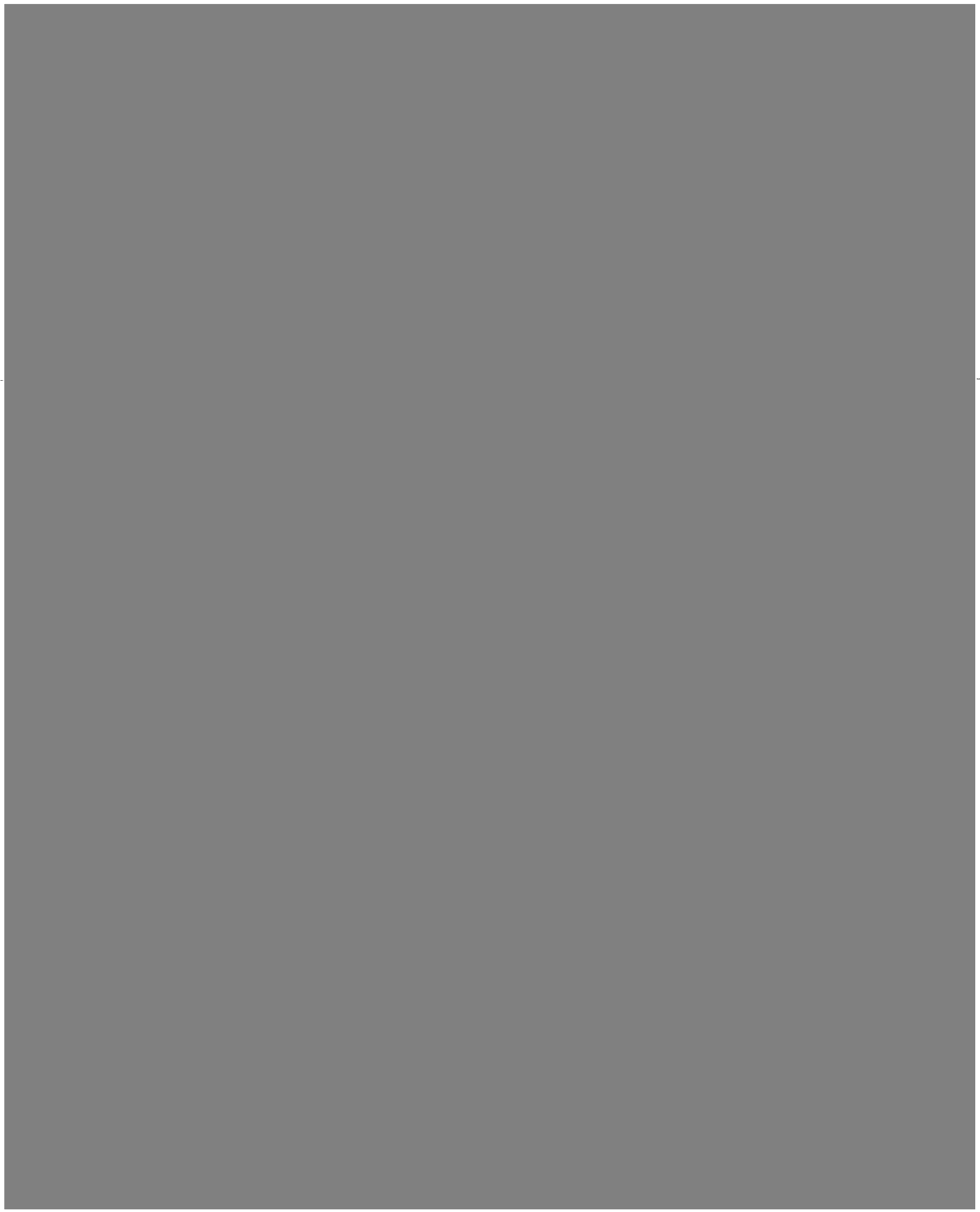
13. As set forth above, the USAO and the FBI have been investigating, among other things, a scheme by Michael Cohen to defraud multiple banks. During the course of this investigation, the USAO and FBI have obtained evidence that Cohen has also committed a criminal violation of the campaign finance laws by [redacted]

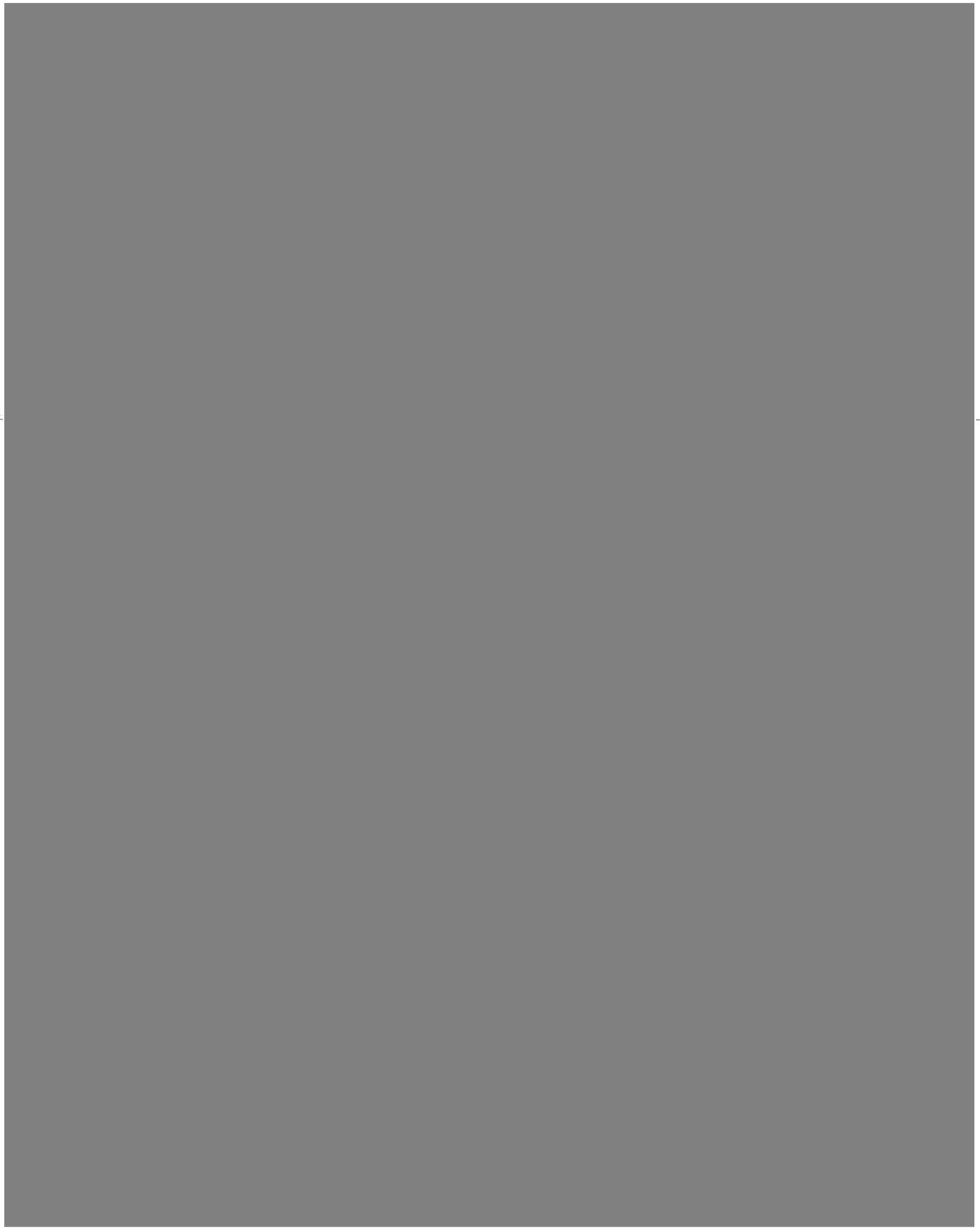
[4] As set forth below, I base this application in part on my review of emails and text messages obtained pursuant to the Prior Warrants. Each of the cited emails or texts messages is either responsive to the applicable Prior Warrant and/or was discovered in plain view during a review of the emails or texts returned pursuant to the applicable Prior Warrant.

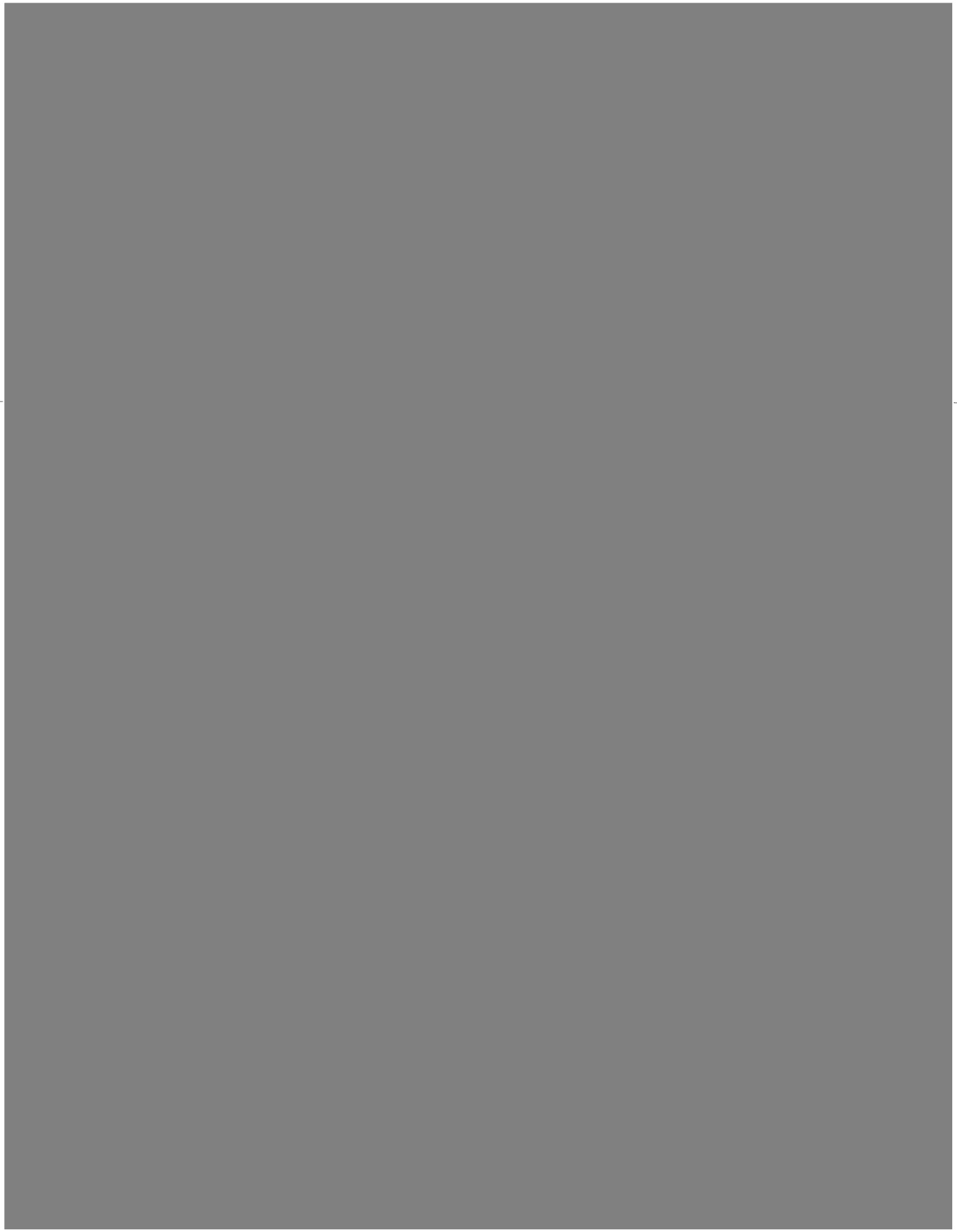
[5] The Prior Warrants describe categories of information that likely encompass evidence of the additional Subject Offense. Nevertheless, in an abundance of caution, I am seeking explicit authorization to search the Subject Devices for evidence of the Subject Offense.

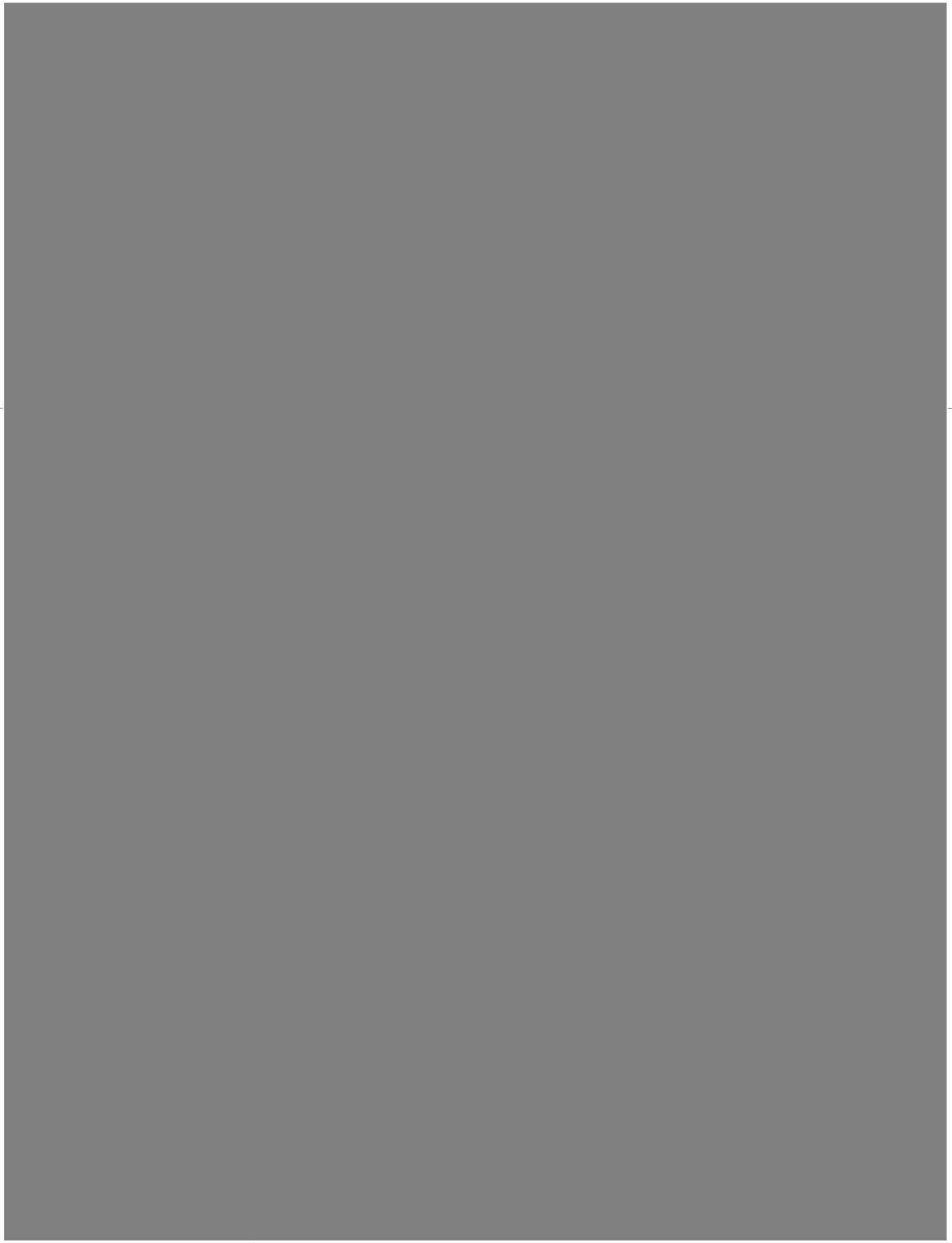


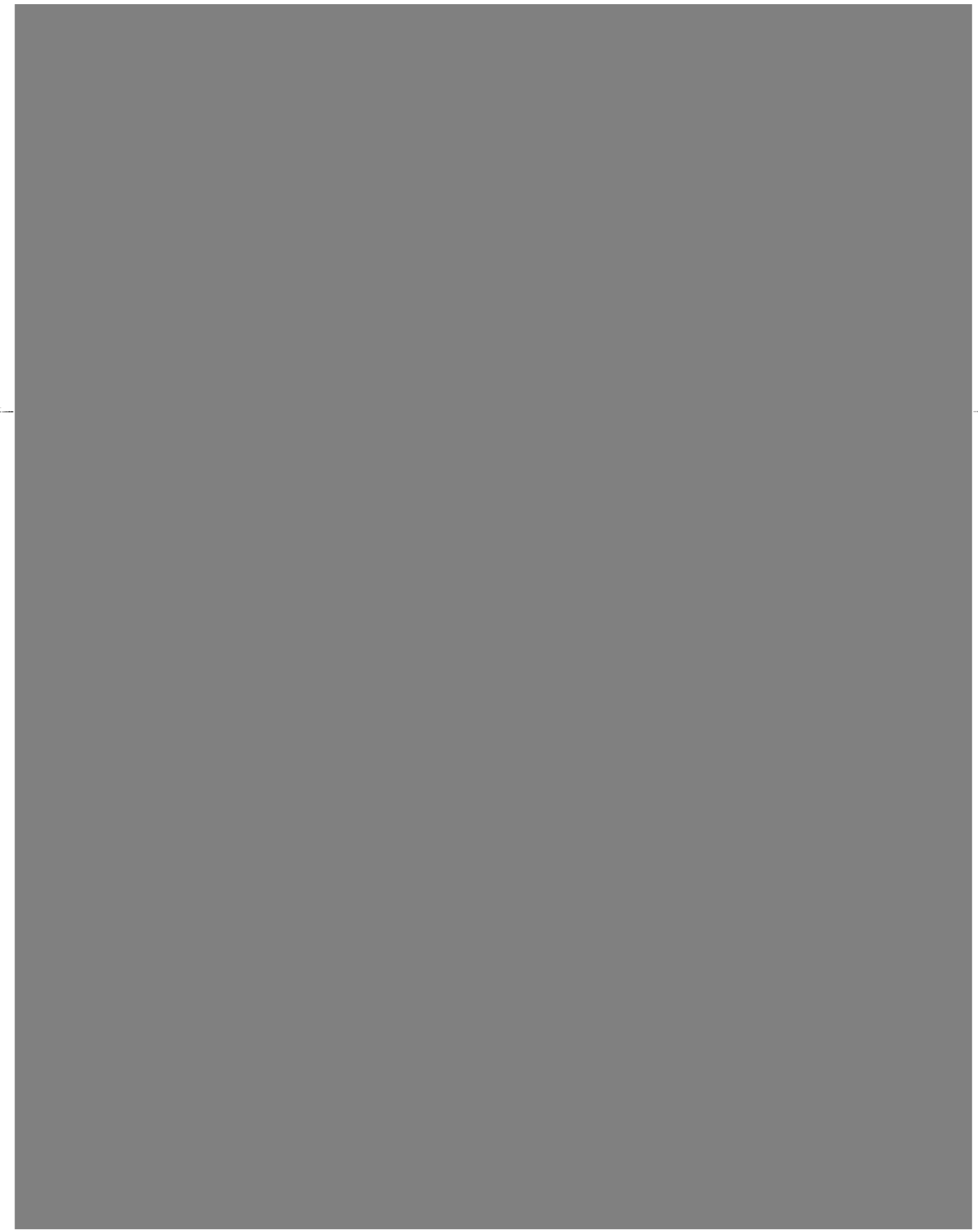


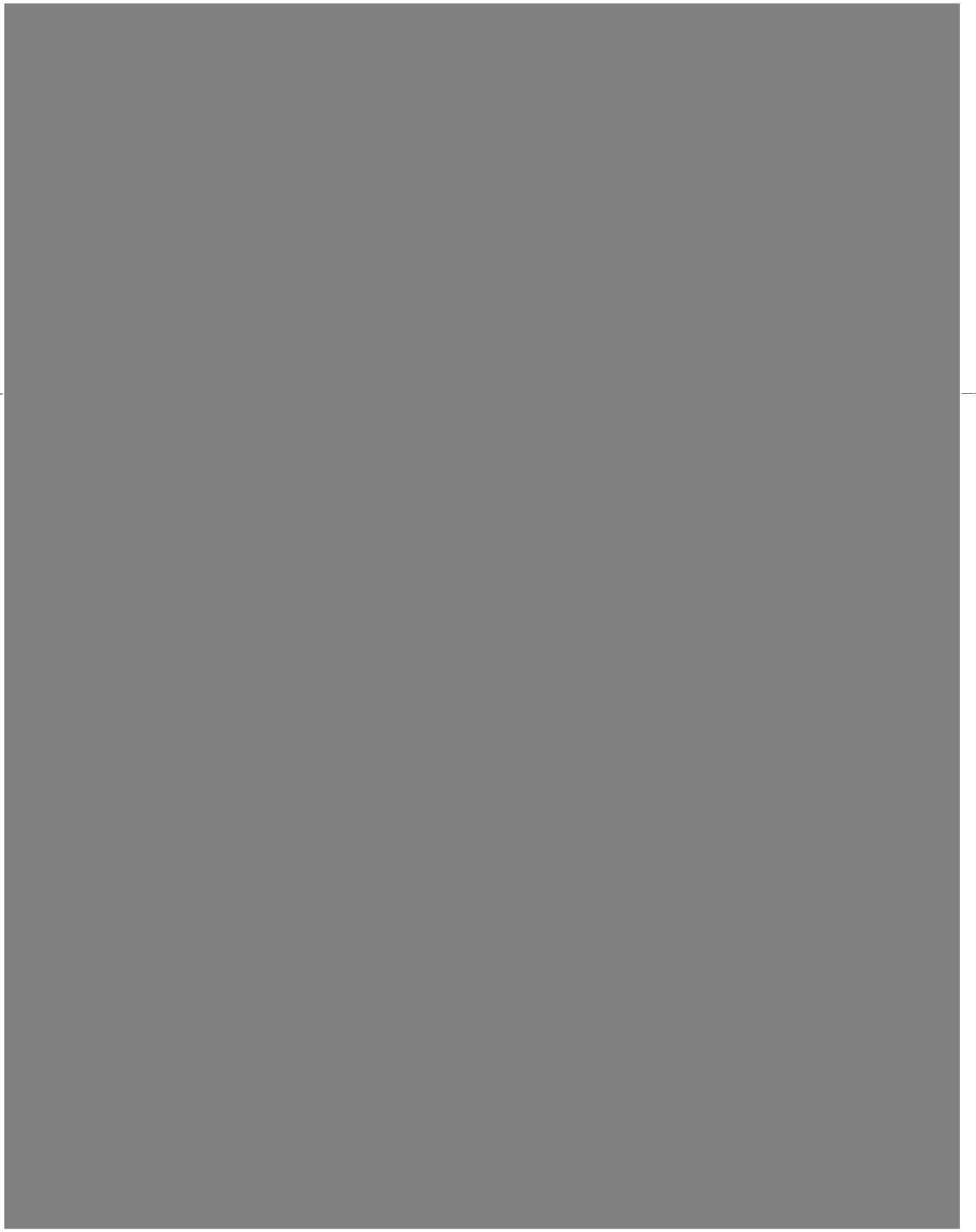


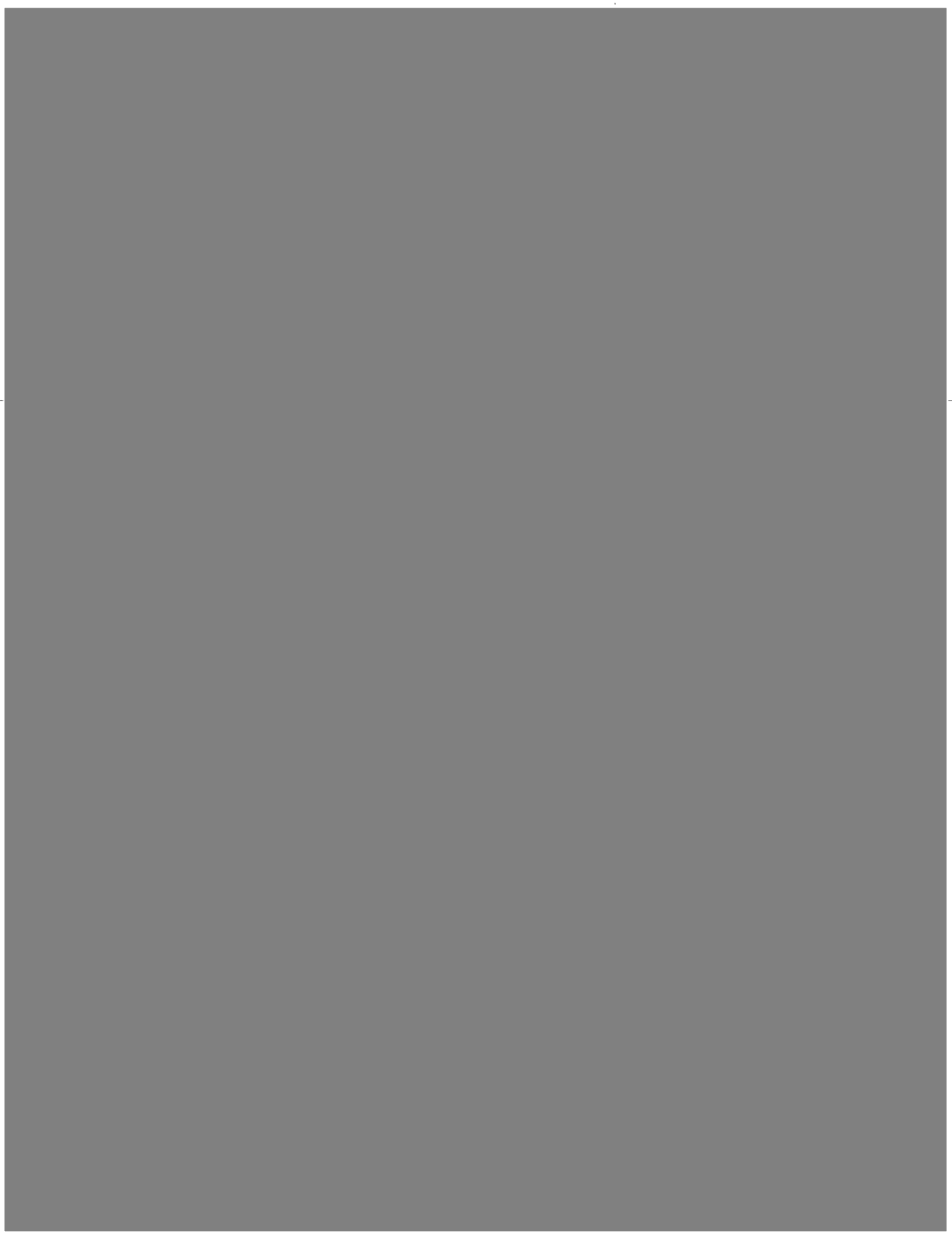


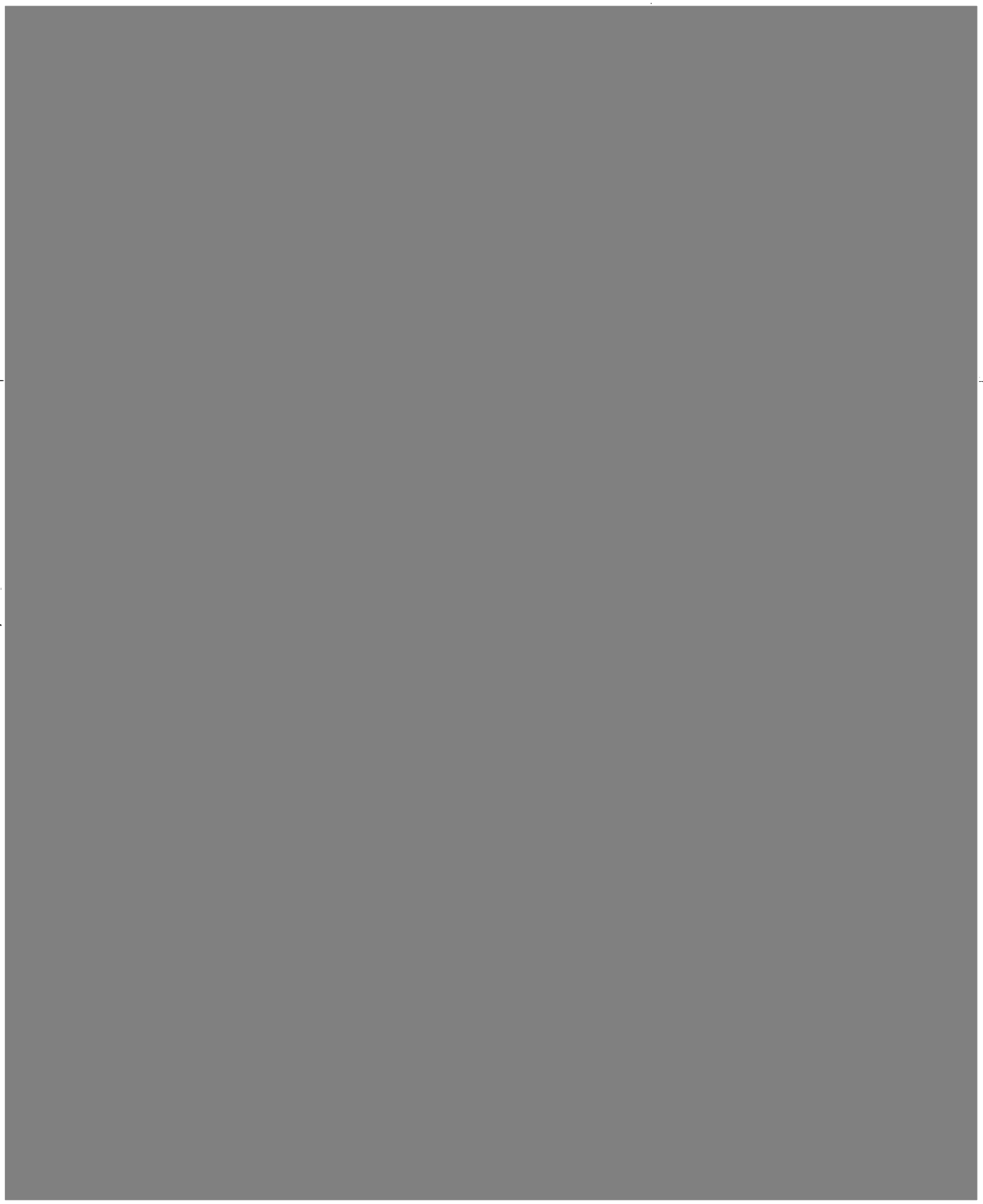


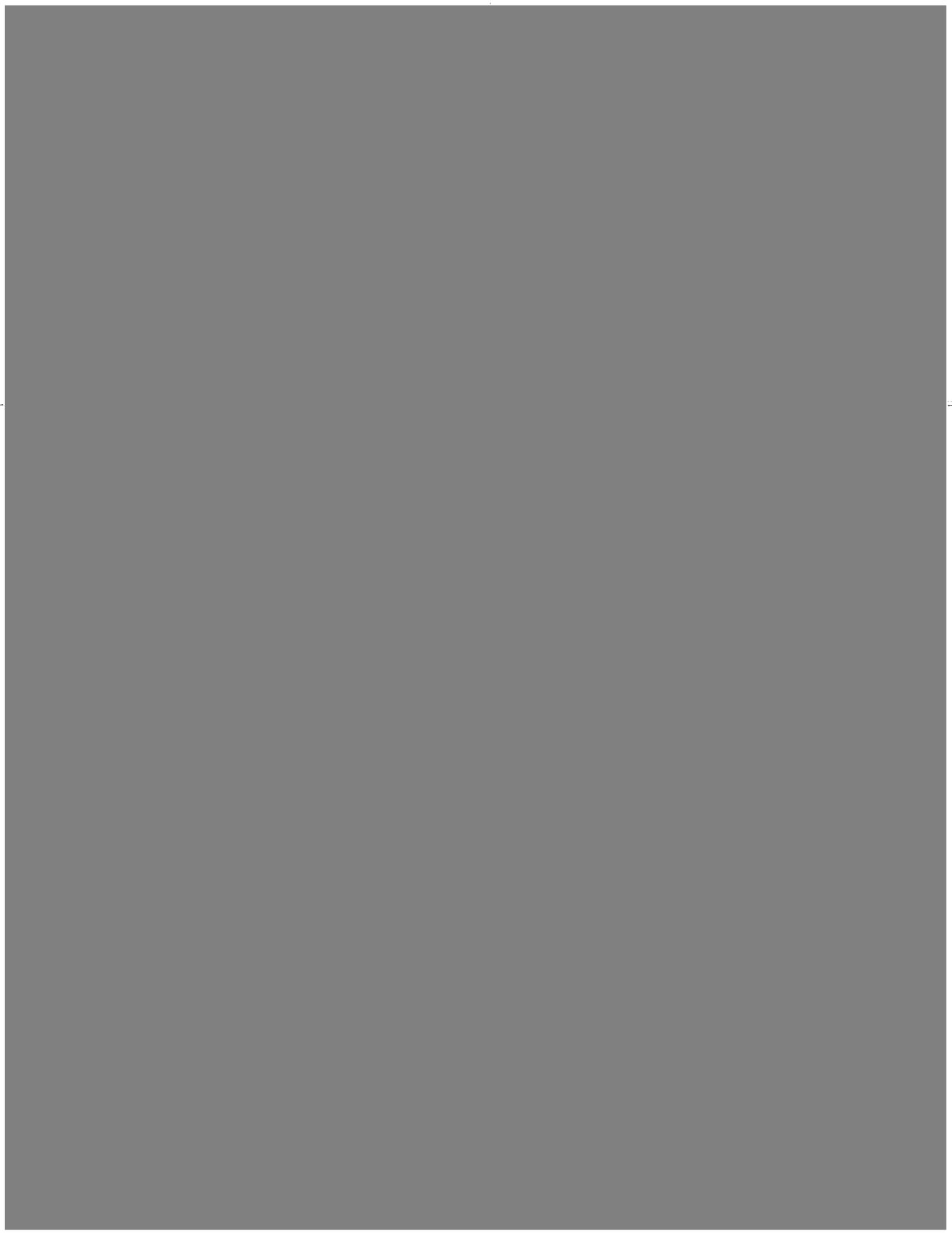


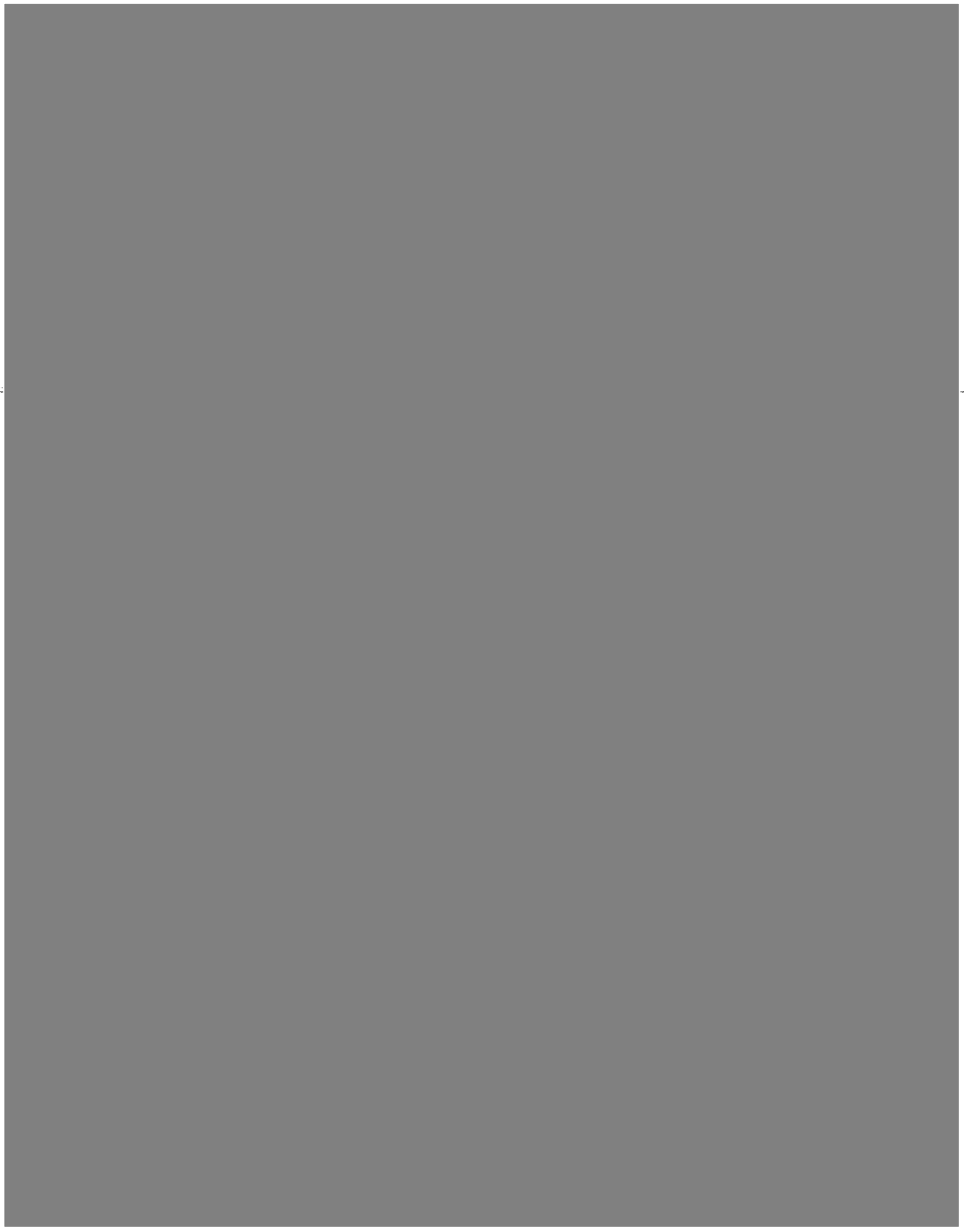


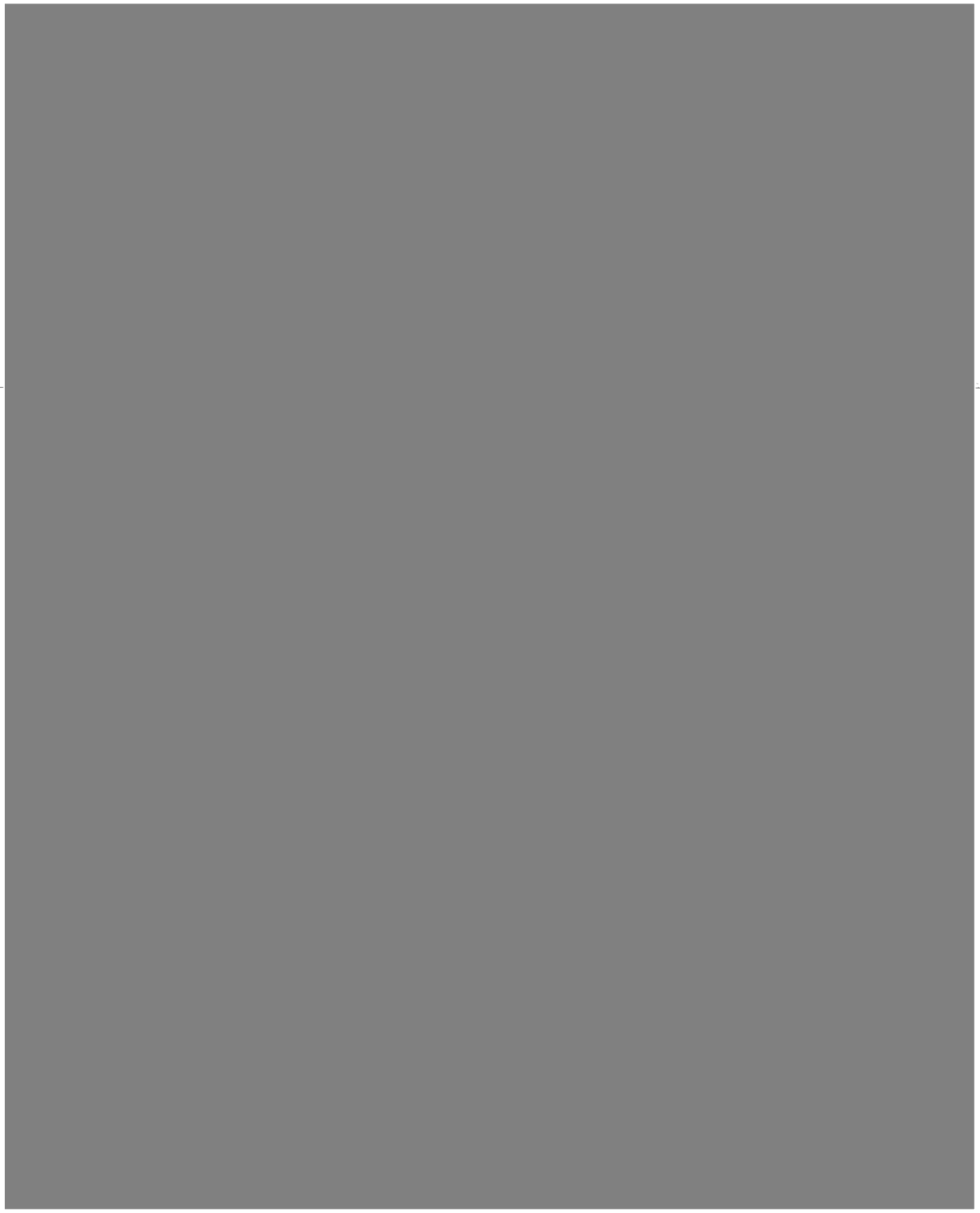


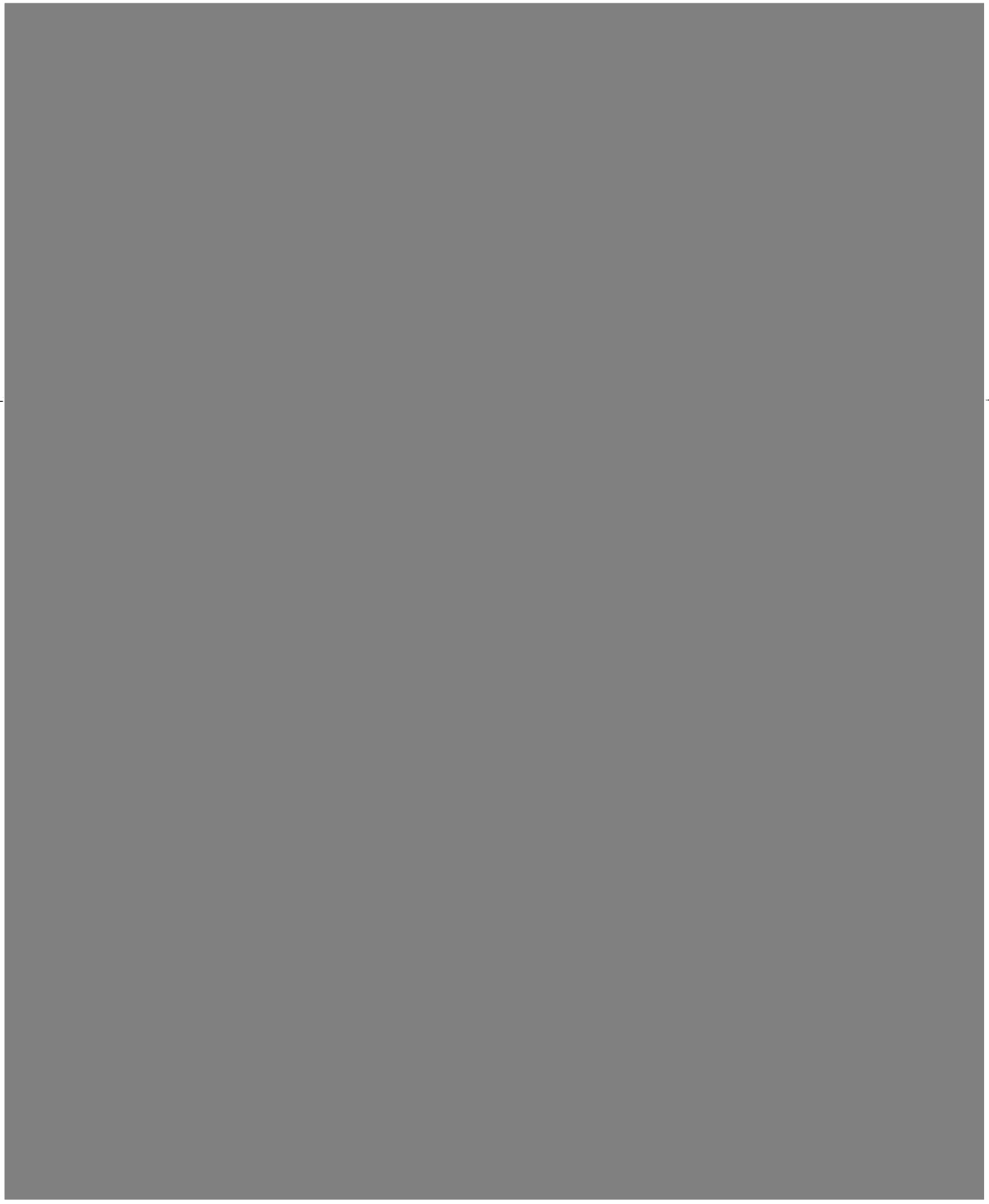


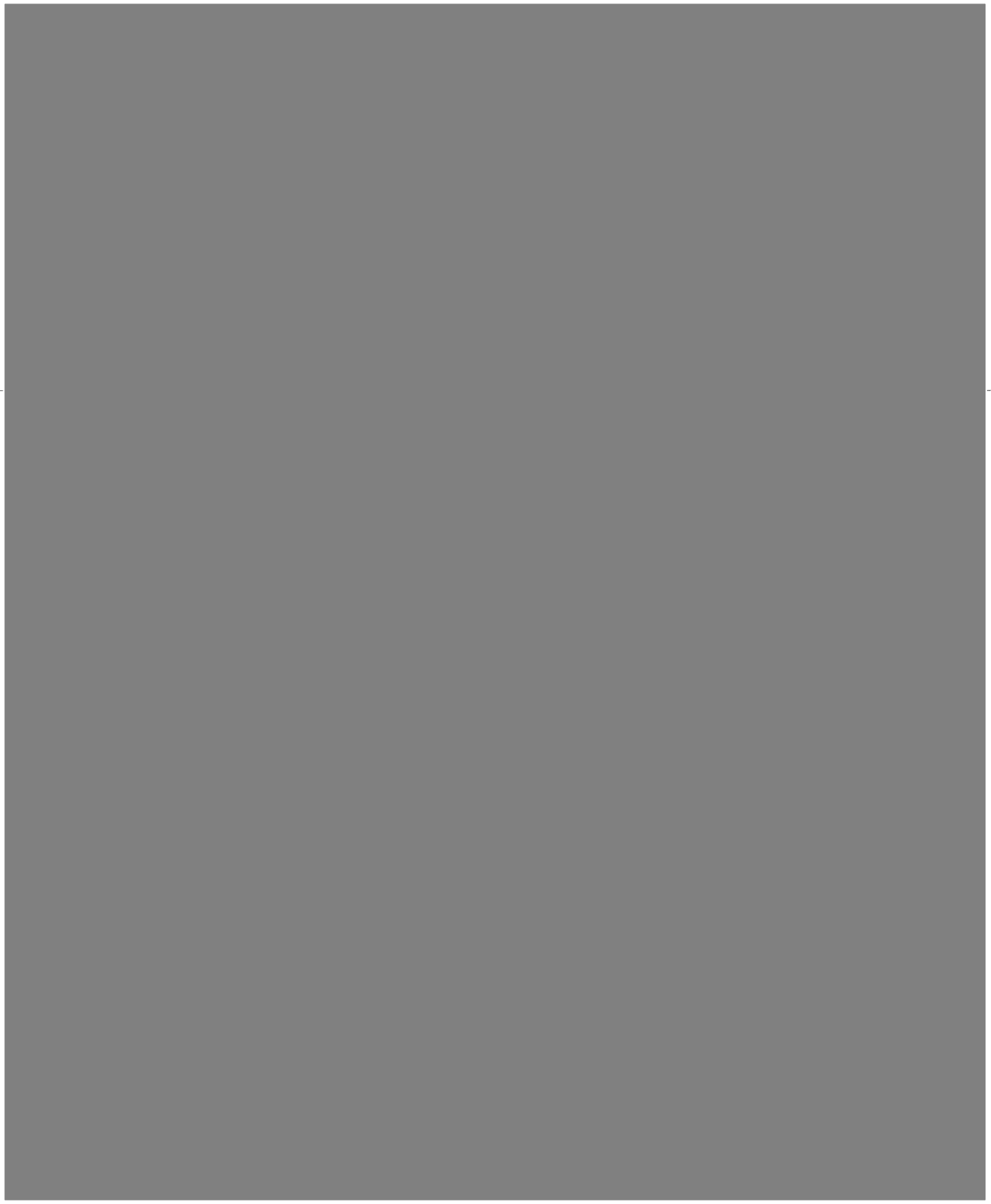


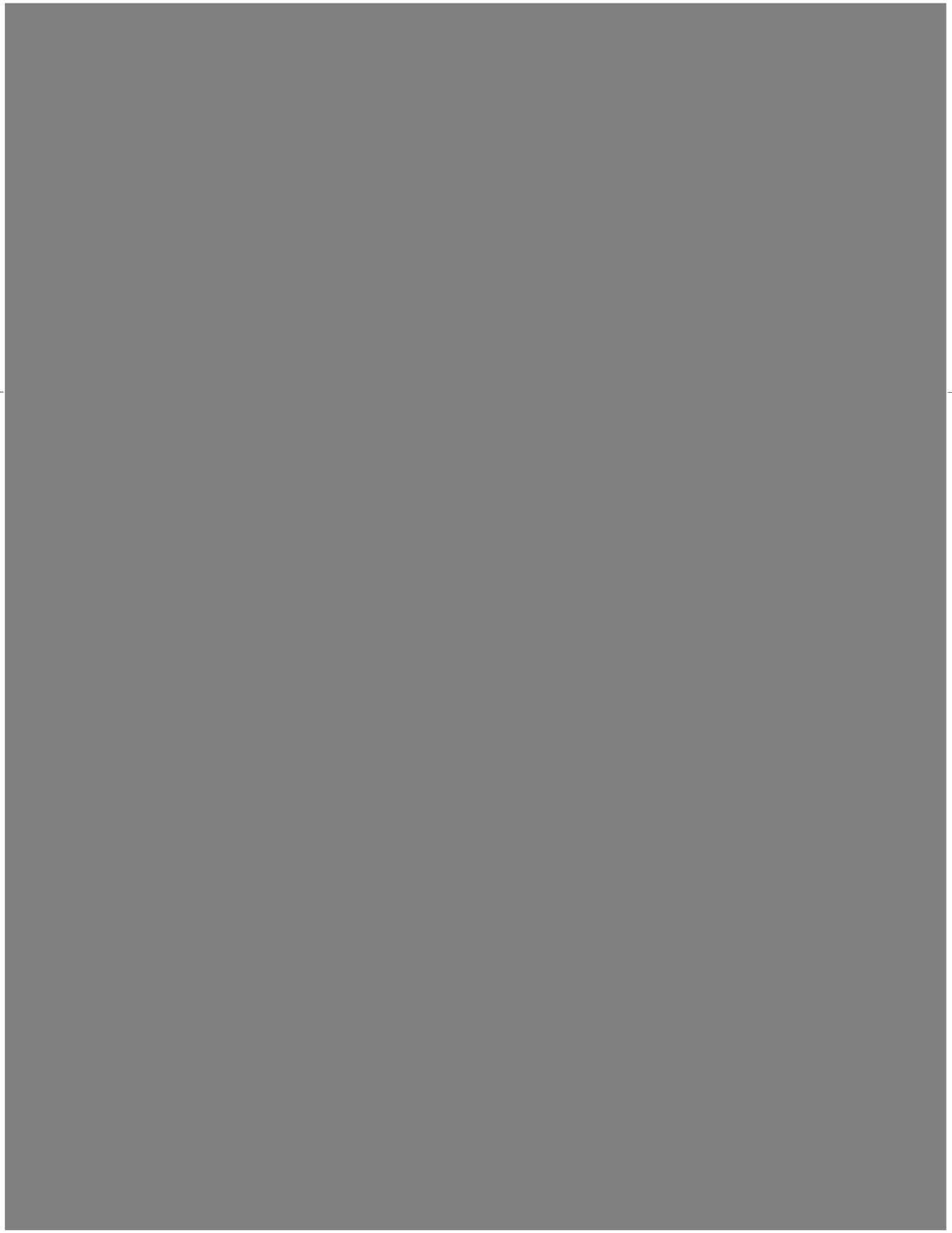


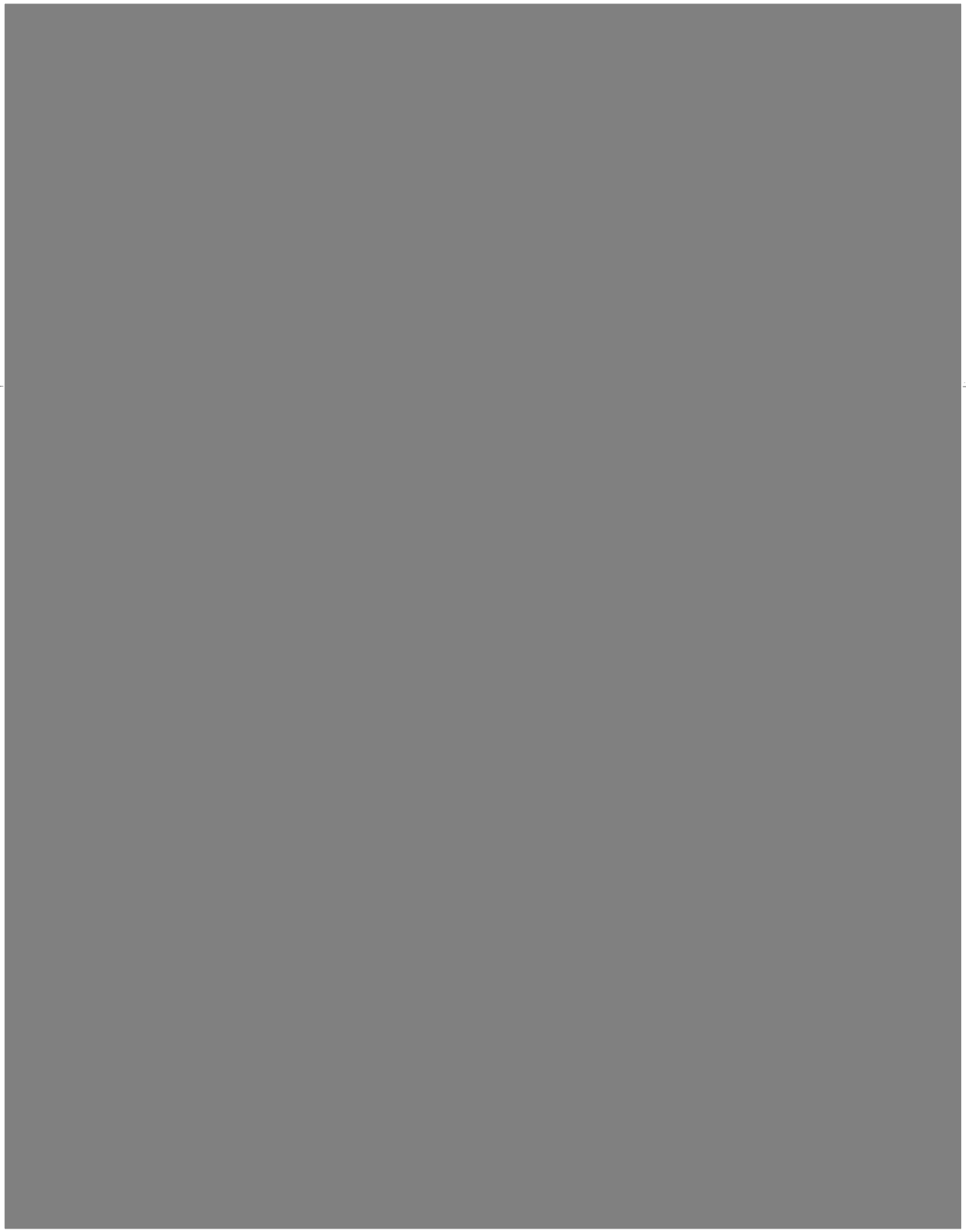












[redacted]

28. Therefore, there is probable cause to believe that a search of the Subject Devices will reveal evidence, fruit and instrumentalities of the Subject Offenses, including the following:

[redacted]

[redacted]

III. Procedures for Searching ESI

A. Review of ESI

29. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, interpreters, and outside vendors or technical experts under government control) will review the ESI contained on the Subject Devices for information responsive to the warrant.

30. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offense, including but not limited to undertaking a cursory inspection of all emails, texts or files contained on the Subject Devices. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and

consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

IV. Conclusion and Ancillary Provisions

31. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

32. In light of the confidential nature of the continuing investigation, and for the reasons more fully set forth in the Accompanying Affidavit, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.

[redacted]
Special Agent, USAO

Sworn to before me on
7th day of April, 2018

HON. HENRY B. PITMAN
UNITED STATES MAGISTRATE JUDGE

Attachment A

I. Devices to be Searched

The devices to be searched (the "Subject Devices") are described as:

a. *Subject Device-1*: A black and red USB drive with a white label that says "Tracking #: 180208140208."

b. *Subject Device-2*: A silver DVD with a white label that reads "Cohen – 2018.03.07."

c. *Subject Device-3*: A white DVD labelled "2-28-18 Cohen SW Returns – Google and 1&1."

II. Review of ESI on the Subject Devices

Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, interpreters, and outside vendors or technical experts under government control) are authorized to review the ESI contained on the Subject Devices for evidence, fruits, and instrumentalities of one or more violations of 52 U.S.C. §§ 30116(a)(1)(A) and 30109(d)(1)(A)(1) (illegal campaign contributions) (the "Subject Offense"), as listed below:

Exhibit A

AO 93 (Rev. 11/13) Search and Seizure Warrant

FILED
JUL 21 2017
Clerk, U.S. District and Bankruptcy Courts

UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH THE EMAIL ACCOUNT [redacted]@GMAIL.COM

Case: 1:17-mj-00503
Assigned To : Howell, Beryl A.
Assign. Date : 7/18/2017
Description: Search and Seizure Warrant

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before August 1, 2017 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Beryl A. Howell
(United States Magistrate Judge).

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of ____.

Date and time issued: July 18, 2017 4:30 pm

Beryl A. Howell
Judge's signature

City and state: Washington, DC

Hon. Beryl A. Howell, Chief U.S. District Judge
Printed name and title

AO 93 (Rev 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
17-MJ-00503	7/18/2017 8:18pm	Google Legal Investigations Support

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Digital Files: Letter 1150069

1150069-20170719-1

See Attachment A for list of Hash values for Production Files

FILED

JUL 21 2017

Clerk, U.S. District and Bankruptcy Courts

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 7/20/2017

[redacted]

Printed name and title

ATTACHMENT A

This warrant applies to information associated with the Google Mail Account [redacted]@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

I. Information to be disclosed by Google

To the extent that the information described in Attachment A is within the possession, custody, or control of the Google (hereinafter "the Provider"), regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that have been deleted but are still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided

during registration, all other user names associated with the account, all account names associated with the subscriber, methods of connecting;

f. All search history or web history;

g. All records indicating the services available to subscribers of the accounts;

h. All usernames associated with or sharing a login IP address or browser cookie with the accounts;

i. All cookies, including third-party cookies, associated with the user;

j. All records that are associated with the machine cookies associated with the user; and

k. All telephone or instrument numbers associated with the Account (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI").

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, contraband, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1014 (false statements to a financial institution) and 18 U.S.C. § 1956 (money laundering), as well as 18 U.S.C. § 951 (acting as an unregistered foreign agent) and the Foreign Agents Registration Act ("FARA"), 22 U.S.C. § 611 *et seq.*, involving Michael Dean Cohen and occurring on or after January 1, 2016, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Communications, records, documents, and other files involving Essential Consultants, LLC;

b. Communications, records, documents, and other files involving Bo and Abe Realty, LLC;

c. Communications, records, documents, and other files that false representations to a financial institution with relation to intended the purpose of an account or loan at that financial institution; the nature of any business or entity associated with an

account a financial institution; the source of funds flowing into an account; or the purpose or nature of any financial transactions involving that financial institution;

d. Records of any funds or benefits received by or offered to Michael Dean Cohen by, or on behalf of, any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

e. Communications, records, documents, and other files that reveal efforts by Michael Dean Cohen to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

f. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner;

g. Evidence indicating the account owner's state of mind as it relates to the crimes under investigation;

h. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s); and

i. The identity of any person(s)—including records that help reveal the whereabouts of the person(s)—who communicated with the account about any matters relating to activities conducted by Michael Dean Cohen on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals.

Exhibit B

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH THE EMAIL ACCOUNT [redacted]@GMAIL.COM

Case: 1:17-mj-00855
Assigned To : Chief Judge Howell, Beryl A.
Assign. Date : 11/13/2017
Description: Search and Seizure Warrant

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before November 20, 2017 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Beryl A. Howell.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 11/13/2017 at 4:50PM

Beryl A. Howell
Judge's signature

City and state: Washington, DC

Hon. Beryl A. Howell, Chief U.S. District Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

This warrant applies to information associated with the Google Mail Account [redacted]**@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

I. Information to be disclosed by Google

To the extent that the information described in Attachment A is within the possession, custody, or control of the Google (hereinafter "the Provider"), regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that have been deleted but are still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, all other user names associated with the account, all account names associated with the subscriber, methods of connecting;

f. All search history or web history;

g. All records indicating the services available to subscribers of the accounts;

h. All usernames associated with or sharing a login IP address or browser cookie with the accounts;

i. All cookies, including third-party cookies, associated with the user;

j. All records that are associated with the machine cookies associated with the user; and

k. All telephone or instrument numbers associated with the Account (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI").

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, contraband, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1014 (false statements to a financial institution), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1344 (bank fraud), and 18 U.S.C. § 1956 (money laundering), as well as 18 U.S.C. § 951 (acting as an unregistered foreign agent) and the Foreign Agents Registration Act ("FARA"), 22 U.S.C. § 611 *et seq.*, involving Michael Dean Cohen and occurring on or after **June 1, 2015**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Communications, records, documents, and other files involving Essential Consultants, LLC;

b. Communications, records, documents, and other files that false representations to a financial institution with relation to intended the purpose of an account or loan at that financial institution; the nature of any business or entity associated with an account a financial institution; the source of funds flowing into an account; or the purpose or nature of any financial transactions involving that financial institution;

c. Records of any funds or benefits received by or offered to Michael Dean Cohen by, or on behalf of, any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

d. Communications, records, documents, and other files that reveal efforts by Michael Dean Cohen to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

e. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner;

f. Evidence indicating the account owner's state of mind as it relates to the crimes under investigation;

g. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s); and

h. The identity of any person(s)—including records that help reveal the whereabouts of the person(s)—who communicated with the account about any matters relating to activities conducted by Michael Dean Cohen on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals.

III. Review Protocols

Review of the items described in Attachment A and Attachment B shall be conducted pursuant to established procedures designed to collect evidence in a manner consistent with professional responsibility requirements concerning the maintenance of attorney-client and other operative privileges. When appropriate, the procedures shall include use of a designated "filter team," separate and apart from the investigative team, in order to address potential privileges.

Exhibit C

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED WITH THE ACCOUNT [redacted] WHICH IS STORED AT THE PREMISES OF 1&1 INTERNET, INC.	Case: 1:17-mj-00854 Assigned To : Chief Judge Howell, Beryl A. Assign. Date : 11/13/2017 Description: Search and Seizure Warrant

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before November 20, 2017 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Beryl A. Howell
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 11/13/2017 at 4:45 pm

Judge's signature

City and state: Washington, DC

Hon. Beryl A. Howell, Chief U.S. District Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

This warrant applies to information associated with the email [redacted] that is stored at premises owned, maintained, controlled, or operated by 1&1 Internet, Inc. ("1&1"), an electronic communication and/or remote computing service provider headquartered in Sunnyvale, California.

ATTACHMENT B

I. Information to be disclosed by 1&1

To the extent that the information described in Attachment A is within the possession, custody, or control of the 1&1 (hereinafter "the Provider"), regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that have been deleted but are still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, all other user names associated with the account, all account names associated with the subscriber, methods of connecting;

f. All search history or web history;

g. All records indicating the services available to subscribers of the accounts;

h. All usernames associated with or sharing a login IP address or browser cookie with the accounts;

i. All cookies, including third-party cookies, associated with the user;

j. All records that are associated with the machine cookies associated with the user; and

k. All telephone or instrument numbers associated with the Account (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI").

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, contraband, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1014 (false statements to a financial institution), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1344 (bank fraud), and 18 U.S.C. § 1956 (money laundering), as well as 18 U.S.C. § 951 (acting as an unregistered foreign agent) and the Foreign Agents Registration Act ("FARA"), 22 U.S.C. § 611 *et seq.*, involving Michael Dean Cohen, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Communications, records, documents, and other files involving Essential Consultants, LLC;

b. Communications, records, documents, and other files that false representations to a financial institution with relation to intended the purpose of an account or loan at that financial institution; the nature of any business or entity associated with an account a financial institution; the source of funds flowing into an account; or the purpose or nature of any financial transactions involving that financial institution;

c. Records of any funds or benefits received by or offered to Michael Dean Cohen by, or on behalf of, any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

d. Communications, records, documents, and other files that reveal efforts by Michael Dean Cohen to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

e. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner;

f. Evidence indicating the account owner's state of mind as it relates to the crimes under investigation;

g. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s); and

h. The identity of any person(s)—including records that help reveal the whereabouts of the person(s)—who communicated with the account about any matters relating to activities conducted by Michael Dean Cohen on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals.

III. Review Protocols

Review of the items described in Attachment A and Attachment B shall be conducted pursuant to established procedures designed to collect evidence in a manner consistent with professional responsibility requirements concerning the maintenance of attorney-client and other operative privileges. When appropriate, the procedures shall include use of a designated "filter team," separate and apart from the investigative team, in order to address potential privileges.

Exhibit D

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED WITH THE APPLE ID [redacted]@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.	Case: 17-mj-00570 Assigned To : Howell, Beryl A. Assign. Date : 8/7/2017 Description: Search and Seizure Warrant

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before August 21, 2017 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Beryl A. Howell
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of ____

Date and time issued: August 7, 2017 2:35 PM

Beryl A. Howell
Judge's signature

City and state: Washington, DC

Hon. Beryl A. Howell, Chief U.S. District Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

This warrant applies to information associated with the Apple ID [redacted]**@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Apple, Inc. ("Apple"), a company headquartered at 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

I. Information to be disclosed by Apple, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, Inc. (hereinafter "the Provider"), regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that have been deleted but are still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided

during registration, all other user names associated with the account, all account names associated with the subscriber, methods of connecting;

f. All search history or web history;

g. All records indicating the services available to subscribers of the accounts;

h. All usernames associated with or sharing a login IP address or browser cookie with the accounts;

i. All cookies, including third-party cookies, associated with the user;

j. All records that are associated with the machine cookies associated with the user; and

k. All telephone or instrument numbers associated with the Account (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI").

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, contraband, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1014 (false statements to a financial institution), 18 U.S.C. § 1344 (bank fraud), 18 U.S.C. § 1956 (money laundering), 18 U.S.C. § 951 (acting as an unregistered foreign agent), and 22 U.S.C. § 611 *et seq.* (Foreign Agents Registration Act), involving Michael Dean Cohen and occurring on or after January 1, 2016, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Communications, records, documents, and other files involving Essential Consultants, LLC;

b. Communications, records, documents, and other files involving Bo and Abe Realty, LLC;

c. Communications, records, documents, and other files that false representations to a financial institution with relation to intended the purpose of an account or loan at that financial institution; the nature of any business or entity associated with an

account a financial institution; the source of funds flowing into an account; or the purpose or nature of any financial transactions involving that financial institution;

d. Records of any funds or benefits received by or offered to Michael Dean Cohen by, or on behalf of, any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

e. Communications, records, documents, and other files that reveal efforts by Michael Dean Cohen to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

f. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner;

g. Evidence indicating the account owner's state of mind as it relates to the crimes under investigation;

h. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s); and

i. The identity of any person(s)—including records that help reveal the whereabouts of the person(s)—who communicated with the account about any matters relating to activities conducted by Michael Dean Cohen on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals.

Exhibit E

18 MAG 1696

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All Content and Other Information Associated with the Email Accounts [redacted]@gmail.com, [redacted]@gmail.com, and [redacted] Maintained at Premises Controlled by Google, Inc., USAO Reference No. 2018R00127

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Google, Inc. ("Provider")

United States Attorney's Office for the Southern District of New York and the Federal Bureau of Investigation (collectively, the "Investigative Agencies")

1. Warrant. Upon an affidavit of Special Agent [redacted] of the United States Attorney's Office for the Southern District of New York, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email accounts [redacted]@gmail.com, [redacted]@gmail.com, and [redacted], maintained at premises controlled by Google, Inc., contain evidence, fruits, and instrumentalities of crime, all as specified in Attachments A and B hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agencies, within 7 days of the date of service of this Warrant and Order, the records specified in Section II of Attachments A and B hereto, for subsequent review by law enforcement personnel as authorized in Sections III and IV of Attachments A and B. The Government is required to serve a copy of this Warrant and Order on the Provider within 7 days of the date of issuance. The Warrant and Order may be served via

electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence or flight from prosecution, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 180 days from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

Feb 28, 2018
Date Issued

10:44 am
Time Issued

HONORABLE GABRIEL W. GORENSTEIN
Chief United States Magistrate Judge
Southern District of New York

Email Search Attachment A

I. Subject Account and Execution of Warrant

This warrant is directed to Google, Inc. (the "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043, and applies to all content and other information within the Provider's possession, custody, or control associated with the email account [redacted]@gmail.com (the "Subject Account") for the time period referenced below.

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Account:

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email) limited to items sent, received, or created between November 14, 2017 and the date of this warrant, inclusive.

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Account.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone

number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations, limited to items sent, received, or created between December 1, 2014 and the date of this warrant, inclusive.

e. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken, limited to items sent, received, or created between December 1, 2014 and the date of this warrant, inclusive.

f. *Search History.* All search history and/or web history associated with the Subject Account, limited to items sent, received, or created between December 1, 2014 and the date of this warrant, inclusive.

g. *Associated content.* All Google Docs, files maintained on Google Drive, and instant messages or Gchats associated with the Subject Account, limited to items sent, received, or created between December 1, 2014 and the date of this warrant, inclusive.

h. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise.

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (conspiracy to commit offense or to defraud

the United States), 1005 (false bank entries); 1014 (false statements to a financial institution), 1343 (wire fraud), and 1344 (bank fraud), including the following:

a. Communications, records, documents, and other files necessary to establish the identity of the person(s) who created or used the Subject Account;

b. Communications, records, documents, and other files involving Sterling National Bank, Melrose Credit Union, and/or taxi medallions;

c. Communications, records, documents, and other files involving a plan, proposal, or agreement for Michael D. Cohen and/or entities associated with him to transfer any interest in taxi medallions, and any associated debts or liabilities, to others, including to [redacted] and/or entities associated with him;

d. Communications, records, documents, and other files involving Essential Consultants, LLC or Michael D. Cohen & Associates, including those which indicate the nature and purpose of payments made to or from Essential Consultants or Michael D. Cohen & Associates;

e. Communications, records, documents, and other files necessary to establish the identity of any person(s) – including records that reveal the whereabouts of the person(s) – who communicated with the Subject Account about any matters relating to Essential Consultants, LLC, or about any plan or proposal or agreement for Michael D. Cohen and/or entities associated with him to transfer any interest in taxi medallions, and any associated debts or liabilities, to others, including to [redacted] and/or entities associated with him;

f. Communications between the Subject Account and [redacted] relating to Michael D. Cohen's bank accounts, taxes, debts, and/or finances;

g. Communications, records, documents, and other files reflecting false representations to a financial institution with relation to the intended purpose of an account or loan at that financial

institution; the nature of any business or entity associated with an account at a financial institution; the source of funds flowing into an account; or the purpose or nature of any financial transactions involving that financial institution;

h. Evidence indicating how and when the Subject Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner; and

i. Evidence indicating the Subject Account owner's intent as it relates to the Subject Offenses under investigation.

IV. Review Protocols

Review of the items described in this Attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege. When appropriate, the procedures shall include use of a designated "filter team," separate and apart from the investigative team, in order to address potential privileges.

Email Search Attachment B

I. Subject Account and Execution of Warrant

This warrant is directed to Google, Inc. (the "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043, and applies to all content and other information within the Provider's possession, custody, or control associated with the email accounts [redacted]gmail.com and [redacted] (the "Subject Accounts") for the time period between October 1, 2016 and the date of this warrant, inclusive.

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts:

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Accounts, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Accounts.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Accounts, including but not limited to name, username, address, telephone

number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Accounts, including any IP logs or other records of session times and durations.

e. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Accounts, including complaints, inquiries, or other contacts with support services and records of actions taken.

f. *Search History.* All search history and/or web history associated with the Subject Accounts.

g. *Associated content.* All Google Docs, files maintained on Google Drive, and instant messages or Gchats associated with the Subject Accounts.

h. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise.

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (conspiracy to commit offense or to defraud the United States), 1005 (false bank entries); 1014 (false statements to a financial institution), 1343 (wire fraud), and 1344 (bank fraud), including the following:

a. Communications, records, documents, and other files necessary to establish the identity of the person(s) who created or used the Subject Accounts;

b. Communications, records, documents, and other files involving a plan or proposal or agreement for Michael D. Cohen and/or entities associated with him to transfer any interest in taxi medallions, and any associated debts or liabilities, to [redacted] and/or entities associated with him;

c. Communications, records, documents, and other files necessary to establish the identity of any person(s) – including records that reveal the whereabouts of the person(s) – who communicated with the Subject Accounts about any matters relating to any plan or proposal or agreement for Michael D. Cohen and/or entities associated with him to transfer any interest in taxi medallions, and any associated debts or liabilities, to [redacted] and/or entities associated with him;

d. Communications between the Subject Accounts and others, including employees or representatives of Sterling National Bank, Melrose Credit Union, or other financial institution(s), regarding Michael D. Cohen's finances;

e. Communications, records, documents, and other files reflecting false representations to a financial institution with relation to the intended purpose of an account or loan at that financial institution; the nature of any business or entity associated with an account at a financial institution; the source of funds flowing into an account; or the purpose or nature of any financial transactions involving that financial institution;

f. Evidence indicating how and when the Subject Accounts was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner;

g. Evidence indicating the Subject Accounts owners' intent as it relates to the Subject Offenses under investigation.

IV. Review Protocols

Review of the items described in this Attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege. When appropriate, the procedures shall include use of a designated "filter team," separate and apart from the investigative team, in order to address potential privileges.

Exhibit F

18 MAG 1696

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All Content and Other Information Associated with the Email Account [redacted] maintained at Premises Controlled by 1 & 1 Internet, Inc., USAO Reference No. 2018R00127

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: 1 & 1 Internet, Inc. ("Provider")

United States Attorney's Office for the Southern District of New York and the Federal Bureau of Investigation (collectively, the "Investigative Agencies")

1. Warrant. Upon an affidavit of Special Agent [redacted] of the United States Attorney's Office for the Southern District of New York, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email account [redacted] maintained at premises controlled by 1 & 1 Internet, Inc., contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment D hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agencies, within 7 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment D hereto, for subsequent review by law enforcement personnel as authorized in Sections III and IV of Attachment D. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence or flight from prosecution, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 180 days from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

Feb 28, 2018
Date Issued

10:45 a.m.
Time Issued

HONORABLE GABRIEL W. GORENSTEIN
Chief United States Magistrate Judge
Southern District of New York

Email Search Attachment D

I. Subject Account and Execution of Warrant

This warrant is directed to 1 & 1 Internet, Inc. (the "Provider"), headquartered at 701 Lee Road, Suite 300, Chesterbrook, Pennsylvania 19087, and applies to all content and other information within the Provider's possession, custody, or control associated with the email account [redacted] (the "Subject Account") for the time period between November 14, 2017 and the date of this warrant, inclusive.

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Account:

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Account.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone

number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.

e. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

f. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise.

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (conspiracy to commit offense or to defraud the United States), 1005 (false bank entries); 1014 (false statements to a financial institution), 1343 (wire fraud), and 1344 (bank fraud), including the following:

a. Communications, records, documents, and other files necessary to establish the identity of the person(s) who created or used the Subject Account;

b. Communications, records, documents, and other files involving Sterling National Bank, Melrose Credit Union, and/or taxi medallions;

c. Communications, records, documents, and other files involving a plan, proposal, or agreement for Michael D. Cohen and/or entities associated with him to transfer any interest in taxi

medallions, and any associated debts or liabilities, to others, including to [redacted] and/or entities associated with him;

d. Communications, records, documents, and other files involving Essential Consultants, LLC or Michael D. Cohen & Associates, including those which indicate the nature and purpose of payments made to or from Essential Consultants or Michael D. Cohen & Associates;

e. The identity of any person(s) – including records that reveal the whereabouts of the person(s) – who communicated with the Subject Account about any matters relating to Essential Consultants, LLC, or about any plan or proposal or agreement for Michael D. Cohen and/or entities associated with him to transfer any interest in taxi medallions, and any associated debts or liabilities, to others, including to [redacted] and/or entities associated with him;

f. Communications between the Subject Account and [redacted] relating to Michael D. Cohen's bank accounts, taxes, debts, and/or finances;

g. Communications, records, documents, and other files reflecting false representations to a financial institution with relation to the intended purpose of an account or loan at that financial institution; the nature of any business or entity associated with an account at a financial institution; the source of funds flowing into an account; or the purpose or nature of any financial transactions involving that financial institution;

h. Evidence indicating how and when the Subject Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner; and

i. Evidence indicating the Subject Account owner's intent as it relates to the Subject Offenses under investigation.

IV. Review Protocols

Review of the items described in this Attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege. When appropriate, the procedures shall include use of a designated "filter team," separate and apart from the investigative team, in order to address potential privileges.