UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE FACEBOOK ACCOUNT IDENTIFIED BY THE USERNAME AARON.ALEXIS THAT IS STORED AT PREMISES CONTROLLED BY FACEBOOK, INC.	**Case 13-MJ-742 (JMF)**

MEMORANDUM OPINION

On September 27, 2013, this Court was presented with an application for a search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure and 18 U.S.C. § 2703(a), (b) and (c), to compel Facebook, Inc. to disclose certain records and contents of electronic communications relating to the Facebook account identified by the user name "Aaron.Alexis." See generally Affidavit in Support of an Application for a Search Warrant [#1-1].[1] This Court did issue a Search and Seizure Warrant Order [#2], but in light of the Court's determination that the government's request was "overbroad under the Fourth Amendment because of the unwarranted invasion into the privacy of third parties," the Court's Order significantly narrowed the scope of what information Facebook could give the government. Id. at 1. That Order also promised that a memorandum opinion would explain the Court's reasons for issuing the modified search and seizure warrant.

I. BACKGROUND

As part of its investigation into the September 16, 2013, shooting at the Washington Navy Yard, perpetrated by Aaron Alexis, the government learned that Alexis had a Facebook account where he posted "long statements about his perspectives on life and would write about

[1] The docket in this matter is public, as the government did not request that it be sealed.

those things or people who bothered him . . . most postings were depressing and negative in nature and could be described as mini-rants." [#1-1] at 6.

The government subsequently filed with the Court its application for a search warrant, which was intended to operate in a bifurcated manner. First, the government outlined the information that it wanted Facebook to "disclose" to the government:

a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have been tagged in them;
d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and other information about the user's access and use of Facebook applications;
e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;
f) All "check ins" and other location information;
g) All IP logs, including all records of the IP addresses that logged into the account;
h) All records of the account's usage of the "Like" feature, including all Facebook posts and non-Facebook webpages and content that the user has "liked";
i) All information about the Facebook pages that the account is or was a "fan" of;
j) All past and present lists of friends created by the account;
k) All records of Facebook searches performed by the account;
l) All information about the user's access and use of Facebook Marketplace;
m) The types of service utilized by the user;
n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

p) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

[#1-1] Attachment B at 1-2.[2] Second, the government specified the information that it would "seize":

a. Records and information, and items related to violations of [18 U.S.C. §§ 1111, 1113, and 1114];
b. Records, information, and items related to the identity of Aaron Alexis;
c. Records, information, and items related to the Washington Navy Yard or individuals working or present there;
d. Records, information, and items related to any targeting of, or planning to attack, the Washington Navy Yard or individuals working or present there, or any records or information related to any past attacks;
e. Records, information, and items related to the state of mind of Alexis, or any other individuals seeking to undertake any such attack and/or the motivations for the attack;
f. Records, information, and items related to any organization, entity, or individual in any way affiliated with Alexis;
g. Records, information, and items related to any associates of Alexis or other individuals he communicated with about his planned violent attacks, including the one perpetrated at the Washington Navy Yard on September 16, 2013;
h. Records, information, and items related to Alexis or his associates' schedule of travel or travel documents;
i. Records, information, and items related to any firearms or ammunition;
j. Records, information, and items related to any bank records, checks, credit card bills, account information, and other financial records; and
k. Records relating to who created, used, or communicated with the user ID, including records about their identities and whereabouts.

Id. at 3-4.[3] The government did not specify what it would do with the information that was disclosed to it by Facebook but that it would not seek to "seize."

The Court was concerned that the government's requested warrant was overbroad, evaded the fundamental requirement that a search warrant particularly describe what items are to

[2] Attachment B, which lists the information that is to be disclosed and seized, is an attachment to the government's application. However, because the Court declined to allow the government access to all of the material in the attachment, the Clerk's office did not scan it and did not place it on ECF. Regardless, the relevant portions are quoted in this Memorandum Opinion, and the Court will request that the Clerk's office place these pages on ECF contemporaneously with this Memorandum Opinion.

[3] The style of the sequential lettering in the two lists differs in the original and is accurately reproduced here.

be seized, and failed the necessity of showing that the items seized were contraband, instruments of committing a crime, or evidence of a crime's commission. See Fed. R. Crim. P. 41(c). Thus, the search requested by the government was the very "general" search that precipitated the enactment of the Fourth Amendment.

In response, this Court crafted an Order that limited Facebook's disclosure to information about Alexis's account and the content of messages that he sent. [#2] at 1-2. Facebook was also ordered to disclose records of communications—but not the content of communications—between third parties and Alexis's account. Id. at 2. The government was permitted to "seize" only information directly related to its investigation, and the Order specified that "[a]ll records and content that the government determines [were] NOT within the scope of the investigation, as described above, must either be returned to Facebook, Inc., or, if copies (physical or electronic), destroyed." Id. at 3.

For the sake of completeness, the relevant portions of the Court's Order are reproduced below:

1. Facebook, Inc. is instructed to comply strictly with the terms of this Order and to provide only the following materials to the government:
    a. All contact and personal identifying information related to the Account, including the Account holder's full name, user identification number, birth date, gender, contact e-mail addresses, Facebook login details, physical addresses (including city, state, and zip code), telephone numbers, screen names, websites, billing information, and other personal identifiers associated with the Account;
    b. All records relating to use of the Account, including session times, login/logout times, IP addresses from which it was accessed, and the types of services used;
    c. All records related to the Account's privacy settings;
    d. All activity logs for the Account and all other records showing the Account's posts, messages, and other activities on Facebook;
    e. All photos and videos uploaded by the Account;
    f. All records—but not content—relating to the Account's list of friends, including any friend requests that were pending or rejected;

g. All records of communications—but not content—sent to the Account from another account or group, including the user ID of that account or group and the user name of the account or group, the date and time of the communication, whether attachments existed (subject to the limitations expressed *infra*); and
h. All records—including content—of communications generated by or sent from the Account to any other user or group (including postings).

2. Facebook, Inc. is instructed to comply strictly with the terms of this Order and is **PROHIBITED** from providing the following materials to the government without an additional Order from this Court:
   a. The contents of any communications sent to the Account;
   b. Photos and videos uploaded by other users, even if Aaron Alexis is "tagged" or otherwise mentioned or identified in the photos or videos; and
   c. Any records or details about any groups of which the Account was a member, including those that were "liked" or of which the Account was a "fan" (or other similar term) other than the user ID and name of the user or group.
3. Upon receipt of the above-described records and content, the government will then conduct a search to determine which relate to the following areas of investigation, as identified in the government's application. These areas are:
   a. Allegations that Aaron Alexis violated:
      i. 18 U.S.C. § 1111;
      ii. 18 U.S.C. § 1113;
      iii. 18 U.S.C. § 1114;
   b. Records and content related to the identity of Alexis;
   c. Records and content related to any targeting of, or plans to attack, the Washington Navy Yard or individuals working or present there;
   d. Records and content related to any other attacks planned or carried out by Alexis;
   e. Records and content related to the motive of Alexis for the attack, including evidence of mental illness;
   f. Records and content related to whether Alexis had any accomplices in planning or carrying out the attack on the Washington Navy Yard or individuals working or present there;
4. All records and content that the government determines are **NOT** within the scope of the investigation, as described above, must either be returned to Facebook, Inc., or, if copies (physical or electronic), destroyed.

Id. at 1-3.

II. LEGAL ANALYSIS

The Court has two primary concerns about the government's application: 1) no probable cause existed for the search and seizure of information related to third parties; and 2) the

government did not provide any explanation for what it would do with information disclosed by Facebook but deemed irrelevant to this investigation and not "seized."

A. The Government Lacked Probable Cause for Information Relating to Third Parties

The Supreme Court has recognized two constitutional protections served by the warrant requirement of the Fourth Amendment. "First, the magistrate's scrutiny is intended to eliminate altogether searches not based on probable cause. The premise here is that any intrusion in the way of search or seizure is an evil, so that no intrusion at all is justified without a careful prior determination of necessity." Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971). Thus, it is this Court's duty to reject any applications for search warrants where the strict standard of probable cause has not been met. Second, "those searches deemed necessary should be as limited as possible. Here, the specific evil is the 'general warrant' abhorred by the colonists, and the problem is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings." Id. These twin inquiries are inseparably intertwined by the text of the Fourth Amendment: "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. To follow the dictates of the Fourth Amendment and avoid issuing a general warrant, a court must be careful to ensure that probable cause exists to seize each item specified in the warrant.

Here, there was certainly probable cause to search and seize items in Alexis's Facebook account because there was probable cause to believe that it contained evidence indicating his motive in perpetrating the shooting and whether he conspired with anyone.

The government's application, however, wholly failed to provide any explanation whatsoever for why there was probable cause to search and seize information about third parties.

Instead, there were only bare requests, such as for "[r]ecords relating to who created, used, or *communicated with* the user ID, including records about their identities and whereabouts." [#1-1] Attachment B at 4 (emphasis added). Without probable cause to seize this material, this Court cannot issue a warrant authorizing its seizure.

In addition to the lack of probable cause, a separate constitutional concern arises from the government's apparent attempt to obtain information about any Facebook groups that Alexis may have joined. The application requests "[a]ll information about the Facebook pages that the account is or was a 'fan' of," as well as "[r]ecords, information, and items related to any organization, entity, or individual in any way affiliated with Alexis." Id. at 2-3. The plain language of this request would require Facebook to turn over membership lists, which implicates the right to free association found in the First Amendment. See NAACP v. Alabama, 357 U.S. 449, 462 (1958) ("This Court has recognized the vital relationship between freedom to associate and privacy in one's associations."). Whether these groups were potentially political advocacy groups is immaterial, as this constitutional protection "pertain[s] to political, economic, religious or cultural matters, and state action which may have the effect of curtailing the freedom to associate is subject to the closest scrutiny." Id. at 460-61.

Depending on what the government found after a search of Alexis's account, probable cause could exist to learn more information about another individual or a group. But no such probable cause existed for the initial foray into Alexis's Facebook profile, and it was therefore premature for the government to seek so much information about third parties.

The Court is particularly concerned because this is the second time this year that it has rejected an overly broad search and seizure warrant application directed to Facebook, at least in part because it unduly invaded the privacy of third parties. In a previous opinion, which remains

sealed, the Court noted that the government's application "casts a remarkable dragnet over communications that surely have nothing to do with this case, including those to and from third parties, who will never know of the government's seeing their communications with John Doe about unrelated matters." In the Matter of the Search of Information associated with Facebook Account: http://facebook.com/[John.Doe] that is stored at premises controlled by Facebook, Inc., 13-MJ-485, slip op. at 2 (D.D.C. June 14, 2013) (Facciola, M.J.) (sealed). The government should exercise caution and more narrowly tailor future warrant applications directed at Facebook; individuals may voluntarily share their information with Facebook, but the government, by seeking a search warrant, justly reasons that probable cause for searching within a Facebook account is still a constitutional necessity, particularly when it will have to see third party communications that are innocuous and irrelevant and sent by persons who could not possibly have anticipated that the government would see what they have posted.

B. The Government Failed to Explain What It Would Do with Material Produced by Facebook That Is Irrelevant to Its Investigation and Thus Outside the Scope of the Search and Seizure Warrant

1. The Two-Step Process of Rule 41 Necessarily Results in the Government Seizing Information Outside the Scope of the Search Warrant

As an initial matter, it may be strange that a court would even need to raise concerns about what the government might do with information that it collects that falls outside the scope of a search and seizure warrant. After all, such collection would appear to be a *per se* violation of the Fourth Amendment. But due to the current "reality that over-seizing is an inherent part of the electronic search process" that gives the government "access to a larger pool of data that it has no probable cause to collect," this Court is obliged to create minimization procedures to limit the possibility of abuse by the government. United States v. Schesso, 730 F.3d 1040, 1042 (9th Cir. 2013) (citing United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir.

2010) (en banc) (per curiam)). See also Comprehensive Drug Testing, 621 F.3d at 1178 (Kozinksi, J. concurring) (suggesting procedures magistrate judges should follow to prevent "turning all warrants for digital data into general warrants").

Part of the problem comes from Rule 41, which creates a two-step procedure for the search and seizure of electronic information that necessarily allows seizing far more information than a warrant specifies. See Fed. R. Crim. P. 41(e)(2)(B). Under that Rule, a warrant "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or other information consistent with the warrant." Id. According to the 2009 notes from the Advisory Committee, this procedure was codified because "it is often impractical for law enforcement to review all of the [electronic] information during execution of the warrant at the search location. . . . officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant." Fed. R. Crim. P. 41 advisory committee's notes.

It is with the two-step procedure in Rule 41 in mind that the government has created the fiction that, although a great deal of information will be disclosed to it by Facebook, it will only "seize" that which is specified in the warrant. Compare [#1-1] Attachment B at 1 with [#1-1] Attachment B at 3; See generally In re Applications for Search Warrants for Information Associated with Target Email Accounts/Skype Accounts, Nos. 13–MJ–8163, 13–MJ–8164, 13–MJ–8165, 13–MJ–8166, 13–MJ–8167, 2013 WL 4647554, at *1 (D.Kan. Aug. 27, 2013) ("In re App.") (the government's search warrant applications used the same bifurcated distinction between information disclosed and information "seized"). By distinguishing between the two categories, the government is admitting that it does not have probable cause for all of the data

that Facebook would disclose; otherwise, it would be able to "seize" everything that is given to it. Yet despite this attempted distinction—which has no apparent basis in the Fourth Amendment—even the material that is not within this second "seizure" category will still be turned over to the government, and it will quite clearly be "seized" within the meaning of that term under the Fourth Amendment. See Brower v. County of Inyo, 489 U.S. 593, 596 (1989) (noting that a "seizure" occurs when an object is detained or taken).

However, other courts to consider this issue have determined that copying electronic data or taking the original hard drives offsite—even if the government knows that the information contained within is beyond the scope of the warrant—does not violate the Fourth Amendment. See, e.g., Guest v. Leis, 255 F.3d 325, 334-35 (6th Cir. 2001) (citing cases from the First, Ninth, and Tenth Circuits) ("In the instant cases, when the seizures occurred, defendants were unable to separate relevant files from unrelated files, so they took the computers to be able to sort out the documents off-site. Because of the technical difficulties of conducting a computer search in a suspect's home, the seizure of the computers, including their content, was reasonable in these cases to allow police to locate the offending files."). These cases, which all predate the 2009 Amendments to Rule 41, remain persuasive until the Supreme Court or the D.C. Circuit rule otherwise. See United States v. Evers, 669 F.3d 645, 652 (6th Cir. 2012); see also United States v. Winther, 2011 WL 5837083, at *11-12 (E.D.Pa. November 18, 2011) (citing cases that have upheld the constitutionality of a two-step procedure even when that procedure takes longer than the time allocated in the warrant for execution).

In light of the substantial authority upholding the process authorized by Rule 41, this Court will continue to issue warrants employing the two-step procedure. However, the Court

does think it appropriate to incorporate appropriate minimization procedures into the warrants to comply with the Fourth Amendment.

2. In This Case, Minimization Procedures Can Satisfy the Fourth Amendment

The Court is aware of the concerns raised by Magistrate Judge David Waxse and others that "the initial section of the warrants authorizing the electronic communications service provider to disclose all email communications (including all content of the communications), and all records and other information regarding the account is too broad and too general." In re App., 2013 WL 4647554 at *8. The current two-step procedure that has been codified in Rule 41 is born from an attempt to balance the practical needs of the government with the requirements of the Fourth Amendment. Without question, the requirements of the Fourth Amendment are paramount; if the government cannot create a practical way to perform electronic searches and seizures that does not violate the Fourth Amendment, then it is simply not entitled to that information. This is clearly an evolving area of the law, but the Court is not yet prepared to go as far as Magistrate Judge Waxse and conclude that that the two step procedure authorized by Rule 41—seize all data and segregate what the warrant permits to be seized from what it does not at a later time—is now to be condemned as a violation of the Fourth Amendment.

This Court will insist, however, that some safeguards must be put in place to prevent the government from collecting and keeping indefinitely information to which it has no right. As with the decision by Magistrate Judge Rian Owsley in In the Matters of the Search of Cellular Telephone Towers, this Court is satisfied—for the time being—that it can lessen any potential Fourth Amendment violation by enforcing minimization procedures on the government. See Nos. C–13–523M, C–13–525M, C–13–526M, C–13–527M, C–13–528M, 2013 WL 1932881, at *2 (S.D.Tex. May 8, 2013) (requiring the government, which obtained a warrant to "dump" all

phone numbers from cell towers, to "return any and all original records and copies, whether hardcopy or in electronic format or storage, to the Provider, which are determined to be not relevant to the Investigative Agency's investigation").

With this issue in mind, this Court began issuing, in September 2013, "Secondary Orders" to search and seizure warrants for electronic records. These "Secondary Orders" explicitly require that contents and records of electronic communications that are not relevant to an investigation must be returned or destroyed and cannot be kept by the government. See, e.g., In the Matter of the Search of Information Associated with [Redacted] That is Stored at Premises Controlled by Yahoo! Inc., 13-MJ-728 (D.D.C. September 25, 2013) (sealed) (Facciola, M.J.) ("All contents and records that the United States government determines are not within the scope of Attachment B (II)(A), (B), and (C) shall be either returned to Yahoo!, Inc., or, if copies, destroyed."). Without such an order, this Court is concerned that the government will see no obstacle to simply keeping all of the data that it collects, regardless of its relevance to the specific investigation for which it is sought and whether the warrant authorized its seizure.

The basis in the Fourth Amendment for those orders, and the minimization order here, is that the government had not established probable cause for the entirety of Alexis's Facebook account—which its more narrow "seizure" section of the application tacitly admitted. Thus, it would violate the Fourth Amendment for the government to permanently seize all contents, records, and other data related to the account. The Court's Order required that "[a]ll records and content that the government determines are NOT within the scope of the investigation, as described above, must either be returned to Facebook, Inc., or, if copies (physical or electronic), destroyed." [#2] at 3. This minimization procedure was intended to help strike the appropriate

balance between the competing interest of the government and the requirements of the Fourth Amendment, and the Court is satisfied, for the moment, with that approach.

Minimization procedures may be an appropriate way to protect the purpose of the Fourth Amendment even when changes in technology dramatically change the way in which search and seizures actually occur in the real world. However, it is clear that they are not perfect. While there has never been anything stopping the government from exceeding the scope of an otherwise valid warrant when searching a physical place, it is clearly easier to do so when the government has an identical copy of an entire hard drive or database. Perhaps of even bigger concern is the potential applicability of the "plain view" doctrine with respect to electronic searches, which has been the subject of considerable consternation in the Ninth Circuit. See Comprehensive Drug Testing, 579 F.3d at 997-99 ("the government should, in future warrant applications, forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it has gained access only because it was required to segregate seizable from non-seizable data. If the government doesn't consent to such a waiver, the magistrate judge should order that the seizable and non-seizable data be separated by an independent third party under the supervision of the court, or deny the warrant altogether.") superseded by 621 F.3d 1162, 1178 (9th Cir. 2010) (en banc) ("The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect.").

Finally, since the 2009 amendment to Rule 41, there has been a sea change in the manner in which computers, which now contain enormous amounts of data, are searched with technology assisted review replacing other forms of searching, including the once thought gold

standard of file-by-file and document-by-document review.[4] Thus, the premise of the 2009 amendment—that law enforcement had to open every file and folder to search effectively—may simply no longer be true. Indeed, this Court finds it hard to believe that a law enforcement agency of remarkable technical ability such as the FBI is opening every file and folder when it seizes a computer that contains a terabyte of data. The Court cannot imagine that it has the time or personnel to do it, nor see any reason to do it when there are more efficient means to do what its agents have to do. Thus, the boilerplate that has appeared in every search warrant application for as long as law enforcement has been searching computers insisting that the agents must open every file and folder may simply be incorrect and therefore an illegitimate premise for the kind of searching law enforcement will actually do.

III. Conclusion

The government has once again relied on boilerplate language that is inapposite to the relevant facts. See In the Matter of the Application of the United States of America for an Order Authorizing Disclosure of Historical Cell Site Information for Telephone Number [Redacted], 1:13-MC-199, 1:13-MC-1005, 1:13-MC-1006, slip op. at 7 (D.D.C. Oct. 31, 2013) (Facciola, M.J.) ("Generic and inaccurate boilerplate language will only cause this Court to reject future § 2703(d) applications."). Counsel for the government represented to the Court that the list of requested items in the application was the standard list used by the Department of Justice for search warrants involving Facebook accounts, although the Court notes that this application requested the production of more information than the request that was previously denied in 13-MJ-485. The facts in this case clearly do not warrant such disclosure.

[4] For an explanation of the technology and a glossary of the terms used in it, see Maura R. Grossman & Gordon V. Cormack, The Grossman-Cormack Glossary of Technology-Assisted Review, with a Foreword by John M. Facciola, U.S. Magistrate Judge, 2013 Fed. Cts. L. Rev. 7 (2013).

This Court is also troubled that its minimization procedure approach—while acceptable in this case—may not be appropriate to curb excessive searches and seizures in the future. Other courts have suggested alternatives, including:

1. Asking the electronic communications service provider to provide specific limited information such as emails or faxes containing certain key words or emails sent to/from certain recipients;
2. Appointing a special master with authority to hire an independent vendor to use computerized search techniques to review the information for relevance and privilege;
3. If the segregation is to be done by government computer personnel, the government must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant;
4. Magistrate judges should insist that the government waive reliance upon the plain view doctrine in digital evidence cases; and
5. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents

See In the Matter of Applications for Search Warrants for Case Nos. 12-MJ-8119-DJW and Information Associated with 12-MJ-9191-DJW Target Email Address, Nos. 12-MJ-8119, 12-MJ-8191, 2012 WL 4383917, at *10 (items 1-2); Comprehensive Drug Testing, 521 F.3d at 1180 (Kozinski, J. concurring) (items 3-5); see also In re Search Warrant, 71 A.3d 1158, 1186 (Vt. 2012) (upholding nine *ex ante* restrictions on a search warrant for electronic data but holding that the issuing officer could not prevent the government from relying on the plain view doctrine). This list is non-exhaustive, and the government should take time to seriously consider how to minimize the amount of information that its search warrant applications seek to be disclosed. There is no doubt that the current state of affairs, as evidenced by the government's original application for Alexis's Facebook account, is untenable. If the government cannot adopt stricter search parameters in future applications, it may find this Court unwilling to issue any search and seizure warrants for electronic data that ignore the constitutional obligations to avoid "general"

electronic warrants that are as offensive to the Fourth Amendment as the searches that led to its enactment.

Digitally signed by John M. Facciola
DN: c=US, email=john_m._facciola@dcd.uscourts.gov, o=United States District Court for the District of Columbia, cn=John M. Facciola
Date: 2013.11.26 15:57:31 -05'00'

JOHN M. FACCIOLA
UNITED STATES MAGISTRATE JUDGE