UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	**CASE NO. 21-CR-537-JMC**
	:	
RYAN SAMSEL,	:	
JAMES TATE GRANT,	:	
PAUL RUSSELL JOHNSON,	:	
STEPHEN CHASE RANDOLPH, and	:	
JASON BENJAMIN BLYTHE,	:	
	:	
Defendants.	:	

UNITED STATES' MEMORANDUM
REGARDING STATUS OF DISCOVERY AS OF FEBRUARY 9, 2022

The United States files this memorandum for the purpose of describing the status of implementation of our Capitol Siege[1] global discovery plan, i.e., our plan for producing or making accessible to all defense teams voluminous data collected by the government in relation to the Capitol Siege investigation, so they may identify information they deem relevant.[2] Under

[1] The "Capitol Siege" refers to the events of January 6, 2021, when thousands of individuals entered the U.S. Capitol and U.S. Capitol grounds without authority, halting the Joint Session and the entire official proceeding of Congress for hours until the United States Capitol Police ("USCP"), the Metropolitan Police Department ("MPD"), and other law enforcement agencies from the city and surrounding region were able to clear the Capitol of rioters and to ensure the safety of elected officials.

[2] By way of illustration, the data subject to the global discovery plan includes items such as:

1. Investigations into all allegations of officer misconduct arising out of January 6, 2021 (regardless of whether sustained);
2. Thousands of hours of surveillance footage from the USCP, MPD, the United States Secret Service ("USSS"), and the Senate and House floors, and body-worn-camera ("BWC") footage from multiple law enforcement agencies that responded on January 6, 2021;
3. Radio transmissions for multiple law enforcement agencies that responded on January 6, 2021;

our global discovery plan, the data that is being made accessible to all defendants far exceeds the information to which any defendant is entitled under Federal Rule of Criminal Procedure 16, the Jencks act, or our *Brady* obligations.[3] We are making such vast quantities of data available due to the unique circumstances of this matter, i.e., literally hundreds of similar crimes being committed in the same place contemporaneously.

This memorandum addresses the status of:

1. Production of voluminous amounts of video to the Federal Public Defender ("FPD") instance of evidence.com (access available since October 18, 2021), and the multiple tools the government has provided to assist the defense in locating footage they may consider relevant;
2. The ability of inmates housed in the D.C. Department of Corrections ("DOC") to access those same materials through a separate DOC instance of evidence.com (beginning as of February 4, 2022);
3. Voluminous documents produced since our last status memorandum dated November 5, 2021;
4. The ability of legal defense teams to obtain access to FPD's Relativity workspace (beginning as of January 21, 2022), and the current contents of that database;
5. Manner of production of voluminous documents in view of defense counsel access to Relativity (beginning as of February 3, 2022);
6. Plans for an e-discovery room in the DOC;
7. Access by inmates to laptops made available through the DOC's e-discovery program;
8. Access to voluminous discovery by *pro se* defendants;
9. Challenges we are overcoming; and
10. Our plan for certain trials that may proceed before our discovery plan is substantially executed.

---

4. Location history data for thousands of devices that connected to the Capitol's cellular network infrastructure, or whose presence within the restricted perimeter was captured in records obtained from Google and multiple data aggregation companies;
5. Thousands of tips;
6. Relevant materials from other subjects' case files, including results of searches of digital devices, Stored Communications Act ("SCA") accounts, and interviews of other subjects, witnesses, tipsters and victims (redacted of identifying information as appropriate); and
7. All reports and exhibits related to allegations of officer misconduct or complicity on January 6, 2021.

[3] *Brady v. Maryland*, 373 U.S. 83 (1963)

***

1. Status of Production of Video Footage to FPD Instance of Evidence.com

Since our last status memorandum describing the status of discovery (dated November 5, 2021), the following video footage has been shared to the defense instance of evidence.com and is accessible to any Capitol Siege defense counsel who requests a license from FPD:

1. 1,063 files consisting of approximately 714 hours of BWC footage recorded by 675 MPD officers.
2. 104 files consisting of approximately 102 hours of BWC and pole camera footage recorded by approximately 54 Arlington County Police Department ("ACPD") officers

At this juncture, just over 24,000 files consisting of USCP closed circuit video ("CCV") footage, BWC from multiple law enforcement agencies, and USSS surveillance footage have been made available to the defense instance of evidence.com. For context, the files provided via evidence.com amount to over nine terabytes of information and would take 102 days to view. Accordingly, solely to assist Capitol Siege defense teams in identifying video files they may consider relevant in specific cases, we have also produced the following analytical and mapping tools, all of which comprise substantial government work product:

1. MPD Radio Global Positioning Satellite ("GPS") Spreadsheet: The Discovery Team learned that radios provided to MPD officers by the D.C. Office of Unified Communications ("OUC") provide GPS location data when four or more satellites are visible to the radio. Under these circumstances, the data is transmitted: (1) every ten minutes; (2) when there is an emergency activation on the radio; and (3) each time an officer pushes the button to talk over the radio. The Discovery Team obtained MPD radio GPS records for January 6, 2021 and created a spreadsheet of data that may be plotted on a time-scaled map using commercially available GPS mapping software. In many instances, the subscriber alias for a radio is an individual officer's Computer Aided Dispatch ("CAD") number and last name. Since MPD BWC footage in evidence.com is also frequently saved under an officer's CAD number and name, a particular officer's radio location information can be used to search for BWC footage from the same time and location in evidence.com;

2. BWC Summary Spreadsheet and related zone maps: This 752-page spreadsheet was initially created by over sixty individuals as an investigative tool to assist prosecutors in locating relevant BWC footage from responding law enforcement agencies including MPD, Montgomery County Police Department, and Fairfax County Police

Department. With respect to over 2,800 BWC video files, the spreadsheet provides: (1) the name and CAD number of the officer associated with the video, (2) the video start time, (3) a short summary of notable events observed by the reviewer including potential crimes observed and the time the camera appears to enter the Capitol, if any; and (4) the apparent location of the camera between noon and midnight, using 15-minute periods of duration. The locations identified correspond to zone maps that section the interior of the Capitol, the Lower West Terrace, and the Capitol Grounds into smaller areas;

3. USSS video spreadsheet: The Discovery Team created a spreadsheet containing the filenames/titles, starting times, video length, and date of USSS video;

4. 15 camera maps of the interior of Capitol Visitor's Center and the interior of the Capitol, and one camera map of the Capitol grounds. The maps depict the general location of the cameras that are identified by unique number in each USCP CCV video filename;

5. ACPD spreadsheet: The Discovery Team created a spreadsheet listing start times of handheld camera video from Arlington County Police Department; and

6. A timeline of events drafted by the USCP, beginning December 16, 2020, memorializing critical events occurring in advance of and during the Capitol Siege.

2. <u>Status of Access to Evidence.com by Defendants Housed in the D.C. Department of Corrections</u>

Through an unprecedented collaboration among the government, FPD, FPD's National Litigation Support Team ("NLST"), American Prison Data Systems ("APDS"), the DOC, and Axon Enterprise, Inc. ("Axon"), as of February 2, 2022, a separate, stand-alone instance of evidence.com has been made available to allow in-custody Capitol Siege defendants who are pending trial to view video footage. This DOC instance of evidence.com is a mirror image of the FPD instance of evidence.com. The government and FPD have drafted a memorandum of understanding describing the contents of the DOC instance, the applicable technical settings, and the requirements for inmates to obtain access. In brief, the government will make a request for an inmate to gain access to the DOC instance of evidence.com once the assigned prosecutor

notifies the Capitol Siege Discovery Unit Chief that one of the following three things has occurred:

1. The inmate has signed Attachment A to the protective order;
2. The inmate has stated on the record in court that s/he has read the protective order, reviewed it with his/her attorney, understands the protective order, and agrees to abide by it; or
3. (a) A defense attorney has represented to the assigned prosecutor in writing that they have reviewed the protective order with their client and have been authorized to sign Attachment A on their client's behalf; and (b) the defense attorney also agrees that at the next scheduled hearing in which the client is present, s/he will put on the record that s/he signed Attachment A on the client's behalf after reviewing the protective order with him or her.

Based upon information provided by APDS, as of February 9, 2022, twenty Capitol Siege inmates should have received access to evidence.com over their APDS educational tablets.[4] As of today, assigned prosecutors are still waiting for defense counsel who represent an additional fifteen Capitol Siege defendants to confirm their respective client's agreement to abide by the terms of the protective order.

3. Status of Production of Documents to Date

Global productions made to defense counsel since November 5, 2021 (Global Production Nos. 8 to 11) have continued to focus on materials most frequently requested by defendants and include items (in addition to some of the tools referenced above) such as:

1. Two new USCP Office of Professional Responsibility ("OPR") reports and 16 associated exhibits;
2. Forty additional exhibits to previously produced USCP OPR reports;
3. One hundred sixty-two USCP Use of Force reports and exhibits;
4. A collection of MPD Use of Force reports and exhibits;
5. Sixty-five video files of the Capitol Siege recorded by MPD's Electronic Surveillance Unit and six related reports;
6. Ten video files of footage from the Senate floor from the Senate Recording Studio;
7. Ten video files of footage from the House floor from the House Recording Studio;
8. Sixty-four audio recordings of Virginia State Police radio communications;

[4] Although APDS attempted to make the link accessible on February 4, there were technological issues. As of February 9, we understand that those issues have been resolved.

9. Eight audio files of USCP radio communications and conference bridge;
10. A redacted transcript of the USCP Dignitary Protection Detail radio channel;
11. 18,484 anonymous tips received by MPD;
12. Documents relevant the interstate commerce element of charged offenses; and
13. USSS files related to Vice President Elect Kamala Harris and Vice President Michael Pence's whereabouts on January 6, 2021.

These materials are substantial. For example, the exhibits to USCP OPR and MPD Use of Force reports described above include approximately 94 audio-recorded interviews of officers and witnesses (35 USCP OPR interviews and 59 MPD use of force interviews).

4. Access to FPD Relativity Workspace

On Friday, January 21, 2022, FPD circulated instructions to defense attorneys on how to gain access to the FPD Relativity workspace. Capitol Siege defense attorneys were advised that since the Relativity database is in a FedRAMP,[5] secure environment, completing the process for obtaining access is time-consuming for FPD and its vendor. Thus, counsel should expect the process for gaining access to the database to take *at least* four to five business days from when counsel first submits a Relativity License Request Form.

5. Manner of Production Going Forward

Approximately two weeks after Capitol Siege defense counsel were notified to apply for Relativity access, and after providing ample notice to defense counsel, the Discovery Team began making its global productions directly to the defense Relativity workspace and discontinued the practice of making voluminous productions via USAfx.[6] Using a defense

[5] The Federal Risk and Authorization Management Program (FedRAMP) was established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government. FedRAMP empowers agencies to use modern cloud technologies, with an emphasis on security and protection of federal information.

[6] We expect prosecutors will continue use USAfx to make productions in individual cases.

Relativity workspace to receive materials produced by the government in discovery will have several benefits for defense teams, including but not limited to avoiding any challenges they may have experienced in downloading large productions from USAfx.[7] They will no longer need to download productions to review them, as the materials will already be available for review in the database. Additional benefits will include the ability to perform keyword searches across the materials in the database, including searches of audio and video that has been "machine" transcribed.[8] Also, within the database, materials that are linked to each other (e.g., a report and multiple exhibits), will be easily identified as connected to each other for reviewing purposes, even if the materials were not initially provided in the same discovery production.[9] Notably, many of the materials we will be providing, such as thousands of tips or the results of searches of other defendants' devices and SCA accounts, would be of little value if produced in any other manner. In addition to the fact that they would likely exceed the capacity of our file transfer system or defense downloading capabilities – and thus require an enormous number of storage devices to be provided in every single case – there would be no way to search the contents universally.

[7] USAfx is merely a tool for file transfer using the Internet, while Relativity is an online search and review database. USAfx is not an optimal nor in many cases even a workable manner of transferring extremely large volumes of data.

[8] Machine transcription is an imperfect tool that is intended to assist defense teams in locating relevant information. On high-quality audio files (e.g., equivalent to a deposition or court hearing), machine-transcription is more accurate than on audio files that contain background noise or in which the speakers are not clearly enunciating (e.g., cell phone videos, custodial interviews, radio communications, voicemails).

[9] In e-discovery parlance, linked documents (such as a report and exhibits, or an email and attachments), are also known as a document "family."

Defendants will not be provided access to the FPD Relativity workspace, given the extensive volume of highly sensitive materials currently therein and those that we will produce in the future. Pursuant to the protective order issued in Capitol Siege cases, defense counsel may not permit defendants to view such materials unsupervised by defense counsel or an attorney, investigator, paralegal, or support staff person employed by defense counsel.[10] By way of illustration, highly sensitive materials currently in the database include allegations about officers' use of force or complicity with rioters (even if ultimately not sustained), and CCV camera maps of the Capitol and grounds containing information that, if further disclosed, could negatively impact the security of the U.S. Capitol. In the future, such materials will grow to include relevant materials derived from searches of subjects' digital devices and social media accounts; interviews with defendants, tipsters, witnesses, and victims; background information accumulated about investigation subjects; and financial, communications, and travel records pertaining to investigation subjects that may bear little or no relevance to most other defendants. Notably, such information may pertain to subjects who are not currently and who may never be charged.

Of course, we will continue to notify the defense of materials have been added to the FPD Relativity workspace so that counsel and defendants may collaborate to identify any materials a defendant should review in a particular case. Subject to the protective order, defense counsel can share such documents with their respective clients through a variety of mechanisms

[10] The protective order places the burden of demonstrating need for protection on the government, and it gives the assigned prosecutor ample flexibility to negotiate sensitivity designations and redactions with respect to individual documents in specific cases. It further permits defendants to contest any sensitivity designation when no agreement may be reached.

including Internet-based file transfer systems or traditional storage devices, such as hard drives, flash drives, and discs.[11]

At this juncture, the defense Relativity workspace contains Global Productions 8 to 11, and portions of Global Production No. 2 (all of which were already made accessible to defense teams via USAfx). We are in the process of transferring Global Production Nos. 1 through 7 to the defense Relativity workspace and anticipate that process will be completed this week.

Among the materials the government expects to provide in the near future are:

1. The remainder of discoverable documents we received from the USCP and MPD in response to requests by the Discovery Team.[12]

2. Over 900 records pertaining to Federal Bureau of Investigation ("FBI") interviews of law enforcement officers. These records are currently being redacted to remove information such as officer's personal telephone numbers;

3. Search warrant documents related to the FBI's collection of: (a) cell tower data from Verizon, AT&T, and T-Mobile/Sprint; (b) Google account subscriber information and

[11] FPD and its vendor are also attempting to determine if it will be possible for defendants to view selected materials within the Relativity workspace, utilizing permissions that would ensure the selected materials are viewable only by the relevant client.

[12] We have nearly completed our assessment and review of approximately 56,000 records provided by the USCP and MPD. Discoverable documents from both data sets continue to be turned over to the defense on a rolling basis. Those discoverable materials not yet produced will be shared to the FPD Relativity workspace as soon as the on-going review and redaction process is completed.

Of approximately 22,000 MPD records we received, we determined that approximately 19,300 were unique (not duplicates) and needed review. Of those, approximately 18,200 have been reviewed and deemed discoverable – they are now in the redaction process. There are still approximately 1,000 MPD records undergoing review. The remainder have been deemed not discoverable.

Of approximately 34,000 USCP records we received, we removed a large number of files from the review process because: (1) they consisted of unscoped digital devices or social media accounts, or (2) they were duplicative. At this juncture, of the remaining approximately 13,200 documents, approximately 3,000 documents are still undergoing review, and approximately 4,200 are in the process of being redacted.

location data from the Capitol and restricted perimeter, i.e., the Google geofence warrants; (c) anonymized location data collected by ten data aggregation companies; and (d) basic subscriber information for Facebook/Instagram accounts linked to the anonymized advertising identifiers obtained pursuant to the data aggregation warrants. These materials are currently being redacted to remove law enforcement sensitive information, for example, the precise location of cellular network infrastructure that provided cellular service to the Capitol on January 6, 2021;

4. Archived Parler[13] posts and comments from around the period of January 6, 2021, hosted by the Internet Archive Project and retrieved by the FBI; and

5. Videos scraped from Parler that were deemed potentially relevant to the Capitol Siege after the FBI's review of thousands of videos from a two-week period encompassing January 6, 2021.

Finally, we currently have a surge team reviewing for discoverability and sensitivity an additional 26,000 FBI documents that were previously loaded into our Relativity database. Relevant documents will be provided after appropriate redactions are completed.

6. Status of Access to Documents in Defense Team Relativity Workspace by Inmates Housed in the D.C. Department of Corrections

We continue to collaborate with FPD and DOC with respect to the creation of an e-discovery room in the Correctional Treatment Facility in which Capitol Siege defendants can access materials provided to them by counsel from the defense team Relativity workspace. The government and FPD's vendors have worked together to establish a plan for production options

[13] Parler is social media website that was used by some individuals to coordinate in advance of the Capitol Siege. *See, e.g.,* Timberg, Craig and Harwell, Drew, "*Pro-Trump forums erupt with violent threats ahead of Wednesday's rally against the 2020 election*, The Washington Post, (Jan. 5, 2021), https://www.washingtonpost.com/technology/2021/01/05/parler-telegram-violence-dc-protests/; Frenkel, Sheera, *The Storming of Capitol Hill was Organized on Social Media,* The N.Y. Times, (Jan. 6, 2021), https://www.nytimes.com/2021/01/06/us/politics/protesters-storm-capitol-hill-building.html. Parler went offline on January 10, 2021, when Amazon Web Services canceled its hosting services. *See* Room, Tony and Lerman, Rachel, "*Amazon suspends Parler, taking pro-Trump site offline indefinitely*, The Washington Post, (Jan. 11, 2021), https://www.washingtonpost.com/technology/2021/01/09/amazon-parler-suspension/. Concerned that Parler was going to be taken offline, the government attempted to collect and preserve publicly available Parler posts, comments, and videos through a variety of methods.

and formats for detained defendants. Broadly, the options under consideration would allow counsel to share productions to detained defendants in one of two ways:

1. An HTML production format that would provide a "CSV"[14] file with metadata fields and links to the documents for review. The CSV file would also contain a column in which inmates could make notes about individual documents and send them back to counsel for review. The CSV would be delivered to inmates on a storage device or via a file transfer program.

2. Productions could be viewed within the Relativity workspace in the manner being considered per footnote 11.

Fifteen laptop computers that FPD ordered to support the proposed program are in transit to FPD. The government, FPD and DOC have made significant progress on a memorandum of understanding that will govern each party's duties and responsibilities in relation to such a program.

The implementation of this solution has met with some delays recently, in part due to the need to identify individuals who would be willing to staff the room. Under the agreement in principle, FPD will be responsible for providing necessary staffing of an e-discovery room. At a bare minimum, staff will be responsible for assigning computers for review and ensuring defendants are able to access the relevant programs.[15] Finding staff with the requisite computer skills who are willing to work full-time in a correctional setting is challenging, and that challenge is further exacerbated by the existence of the COVID-19 pandemic. In any event, even if staff were currently available, it is questionable whether the program could have been made accessible

[14] A CSV (comma-separated values) file is a text file that has a specific format which allows data to be saved in a table structured format. It can be opened in a wide variety of programs and is commonly opened in Microsoft Excel and appears as a spreadsheet.

[15] Ideally, such staff would be able to provide additional support including troubleshooting issues with computers and assistance with accessing and reviewing productions.

to large groups of inmates in recent months. Pursuant to medical stay-in-place protocols issued December 22, 2021, the DOC has suspended all in-person small group activities and volunteer services in the effort to combat the spread of COVID-19.[16]

7. Status of Access to Laptops Through DOC's E-Discovery Program

In the interim, the DOC's e-discovery laptop program has presented inmates with a reasonable alternative for viewing voluminous documentation. As described in our prior submissions, there are over 20 computers in the DOC's e-discovery program, and inmates may keep them for up to two weeks at a time once they are eligible. Based on the most recent version of the laptop waitlist (dated February 4, 2022), it appears there are approximately 18-22 inmates on the waitlist, and 14 of them were added no earlier than January 21, 2022.

8. *Pro Se* Defendants

The government and FPD continue to collaborate about a discovery plan for *pro se* defendants. Currently, subject to the terms of the protective order, standby counsel can use their own licenses for the FPD instance of evidence.com to share videos with non-detained *pro se* defendants, and detained *pro se* defendants can view video in the DOC instance. As we have previously made defense counsel aware, we have agreed to waive the requirement that a defendant be supervised while reviewing highly sensitive video in cases where access is provided through evidence.com and:

1. A protective order has been entered in the relevant case;
2. The defendant has executed the written acknowledgement to the protective order (or been subject to an equivalent admonishment by the Court); and
3. The ability of the defendant to download or reshare is suppressed by counsel before the video is shared to the defendant.

[16] We understand that the DOC imminently intends to revert to the modified stay-in-place protocols that were in effect prior to December 22, 2021.

For the reasons elaborated in part 5 above, the government will not agree to providing *pro se* defendants unfettered access to FPD's Relativity workspace. However, prosecutors assigned to *pro se* case will share production indexes with both defendants and their standby counsel. Standby counsel should discuss the materials on the production index with the *pro se* defendant, and subject to the protective order, s/he can share any materials requested utilizing the same mechanisms available to represented defendants described above. Further, in those instances where a *pro se* defendant wishes to view highly sensitive documents, standby counsel or his/her staff must supervise the defendant unless: (1) the defendant and the assigned prosecutor are able to reach a suitable compromise or (2) the Court orders otherwise.

9. <u>Challenges We Are Overcoming</u>

In November, we projected that by the end of January 2022, we would provide the discoverable portions of several hundred thousand FBI records. We were unable to meet this goal for several reasons. Our plan was to identify all data in the FBI's case management system associated with any Capitol Siege investigation subject, and then export that data for review in Relativity (after culling it of any material arguably protected by Federal Rule of Criminal Procedure 6(e)). Our request to extract this volume of data from the FBI's case management system was unprecedented. An FBI data scientist worked closely with the developers of the FBI's case management system to create a technological solution that would identify the relevant case materials and export the data for uploading to Relativity. In November 2021, we understood that the technological solution had been successfully deployed, and we expected to receive over 400,000 documents for further discovery processing at about that time. Upon subsequent review of the export, however, our technology experts recognized that the solution developed was not as successful as originally believed. Although the materials were identified

and exported, they were no longer organized in any logical fashion, i.e., by individual investigation and in chronological order. As a result, the government was required to develop additional technological solutions to ensure that documents were associated to appropriate case files and properly sequenced before they were loaded to Relativity. This was an iterative process that took time. Efforts to move quickly were also frustrated by COVID-related quarantines and snowstorms that limited access of key personnel to the technology labs necessary to complete their work. As a result of all the above, this entire process took far longer than was originally anticipated.

Ultimately, approximately 380,000 documents from the FBI's case management system were delivered to Deloitte on February 7, 2022.[17] Given the volume of material, it may take up to ten days for it to finish being uploaded. Once these materials complete uploading, they will require in-depth analysis and customization so that they may be produced to the FPD database in a standardized format, vastly facilitating future searching and review by defense teams. This process is required prior to any human review and is expected to take an additional several weeks. During this same period, we will also leverage Relativity's analytical tools to deduplicate files, potentially eliminating thousands of documents from the need for any further review. (A highly preliminary review suggests that approximately one-third to one-half of the documents may be duplicative in nature.) During this time, we also expect to identify certain types of documents that may be "bulk-coded" as for production without the need for additional human

[17] An additional 50,000 documents that were contained in results of searches for materials potentially protected by Rule 6(e) will be separately delivered directly to the government for review. Based on recent experience, our search terms were intentionally designed to be overinclusive and we expect that a sizeable portion of these materials will be sent to our Relativity database.

review. Once the remaining materials are ready for human review, we have a surge staffing plan in place to perform review and redactions, and to quality-check proposed productions.[18]

Another challenge we continue to confront is our plan to provide defense teams the ability to view materials scoped from other subjects' devices and SCA accounts, as well as law-enforcement recorded interviews of other investigation subjects. As of today, we have provided over 900 items in these categories to Deloitte for ingestion into the government's Relativity database. Processing and loading these materials is complicated because there are no cookie-cutter solutions that may be applied to all devices and interviews. There is a wide variability in the format of results obtained from searches of digital devices and SCA accounts. Similarly, subject interviews were recorded in proprietary player formats unique to the recording devices used. All this data requires thoughtful examination and decision-making to ensure it will be accessible, organized, and searchable once it is loaded to FPD's Relativity database. In addition, we are providing assigned prosecutors a short timeframe to verify there are no security concerns with the production of such items to a global database. At this juncture, almost 300 such items have been uploaded to the government's Relativity database, and we expect to begin providing them to FPD's Relativity database shortly. We are continuing to process and upload such items on a rolling basis.

10. <u>Short-Term Discovery Plan for Certain Trials</u>

The events of January 6 were historic, not only because they represented the first time that American citizens had stormed the Capitol, but because the amount of information and

[18] The extracted FBI case files discussed above represent the FBI's Capitol Siege case files as of approximately September 2021. The lessons learned from this first extraction have led to significant improvements in the overall process. We will begin the next extraction after we complete application of the technological solution to the 50,000 documents that were contained in results of searches for materials potentially protected by Rule 6(e).

evidence involved is unprecedented. As defendants are in a better position to determine what evidence they believe is exculpatory and will help in their defense, we maintain that our plan – to provide the defense with all data that may contain such information, but in a manner that will facilitate search, retrieval, sorting, and management of that information – continues to be reasonable and appropriate.[19] Notwithstanding the challenges arising from organizing and

[19] The government's approach is also consistent with the Recommendations for Electronically Stored Information (ESI) Discovery Production developed by the Department of Justice and Administrative Office of the U.S. Courts Joint Working Group on Electronic Technology in the Criminal Justice System. *See https://www.justice.gov/archives/dag/page/file/913236/download.* It is also the generally accepted approach for ensuring that arguably exculpatory materials are provided in cases involving voluminous information.

Notably, every circuit to address the issue has concluded that, where the government has provided discovery in a useable format, and absent bad faith such as padding the file with extraneous materials or purposefully hiding exculpatory material within voluminous materials, the government has satisfied its obligations under *Brady v. Maryland*, 373 U.S. 83 (1963) and progeny. *See United States v. Yi*, 791 F. App'x 437, 438 (4th Cir. 2020) ("We reject as without merit Yi's argument that fulfillment of the Government's obligation under *Brady* requires it to identify exculpatory material."); *United States v. Tang Yuk*, 885 F.3d 57, 86 (2d Cir. 2018) (noting that the "government's duty to disclose generally does not include a duty to direct a defendant to exculpatory evidence within a larger mass of disclosed evidence") (internal citations omitted); *United States v. Stanford*, 805 F.3d 557, 572 (5th Cir. 2015) ("We have previously rejected such 'open file' *Brady* claims where the government provided the defense with an electronic and searchable database of records, absent some showing that the government acted in bad faith or used the file to obscure exculpatory material."); *United States v. Gray*, 648 F.3d 562, 567 (7th Cir. 2011) ("The government is not obliged to sift fastidiously through millions of pages (whether paper or electronic). . . [and] is under no duty to direct a defendant to exculpatory evidence [of which it is unaware] within a larger mass of disclosed evidence.") (quotation marks and citations omitted); *Rhoades v. Henry*, 638 F.3d 1027, 1039 (9th Cir. 2011) (rejecting *Brady* claim on the ground that the defendant "points to no authority requiring the prosecution to single out a particular segment of a videotape, and we decline to impose one"); *United States v. Warshak,* 631 F.3d 266, 297 (6th Cir. 2010) ("As a general rule, the government is under no duty to direct a defendant to exculpatory evidence within a larger mass of disclosed evidence"); *United States v. Skilling*, 554 F.3d 529, 576 (5th Cir. 2009)(same), aff'd in part, vacated in part, remanded, 561 U.S. 358 (2010); *United States v. Pelullo*, 399 F.3d 197, 212 (3d Cir. 2005) ("*Brady* and its progeny . . . impose no additional duty on the prosecution team members to ferret out any potentially defense-favorable information from materials that are so disclosed."); *United States v. Jordan,* 316 F.3d 1215, 1253-54 (11th Cir. 2003) (concluding that the defendant's demand that the government "identify all of the *Brady* and *Giglio* material in its possession," "went far beyond" what the law requires).

producing unprecedented amounts of data that are frequently complex in nature, our plan is being executed promptly and in good faith. We have produced terabytes of organized and searchable data in hundreds of cases and continue to do so as quickly as possible.

In addition, we have developed a short-term discovery plan that will enable certain trials to proceed before our discovery plan is substantially executed. To be clear, this is not the plan we recommend, nor one that would be workable in multiple cases or complex cases. Time spent executing this plan will reduce resources available to execute the global plan described above. Pursuant to our short-term plan, we will create lists describing substantially all our holdings. Defense teams can review the lists to request specific items they believe may be relevant. We expect these lists will identify the physical and digital evidence that has been accumulated across all Capitol Siege investigations; and categories of potentially discoverable information from materials that are in our possession but have not yet been produced in global discovery, e.g., the FBI materials recently provided to Deloitte; small amounts of material from other law enforcement agencies that played a role on the January 6, 2021; damage estimates from the Architect of the Capitol; and grand jury transcripts.[20]

In addition, pursuant to this plan, assigned prosecutors will ensure that searches based on the defendant's personal and/or device identifiers, as relevant, have been or will be conducted within of the following sets of data:

[20] If additional materials requested by defense teams are extensive, we will likely need to request a continuance and tolling of the Speedy Trial Act to allow the defense adequate time to prepare for trial. This is especially true in the case of requests for the results of multiple other subjects' digital devices and SCA accounts that have not yet been scoped for relevant information. Further, if the requested materials have not been loaded and organized within our Relativity database yet, they will be turned over in their native format and the defendant will be unable to leverage FPD's Relativity's search tools to review them.

1. Cell tower data from Verizon, AT&T, and T-Mobile/Sprint Cell for devices that connected to the Capitol's cellular network infrastructure;

2. Google account subscriber information and location data from the Capitol and restricted perimeter obtained pursuant to the Google geofence warrants;

3. Location data obtained by the FBI from multiple data aggregation companies;

4. Basic subscriber information and call records obtained pursuant to applications made to twelve cell service providers under 18 U.S.C. 2703(d) for devices that, according to location data obtained pursuant to the Google geofence warrants, were present within the U.S. Capitol on January 6, 2021;

5. A repository of Archived Parler posts and comments from around the period of January 6, 2021, hosted by the Internet Archive Project and retrieved by the FBI;[21]

6. A repository of digital media tips maintained by the FBI; and

7. The government's discovery databases.

We will also perform searches of the data described above in response to defense counsel requests for materials that we are obligated to produce under Federal Rule Criminal Procedure 16, the Jencks Act, and our *Brady* obligations.[22]

Further, prosecutors will ensure that a facial recognition search has been performed within a repository of images and video that the FBI continually populates, so that all identifiable images of the defendant within that repository at a time close to trial are produced.

[21] Items 1-4 will never be provided *en masse* in global discovery because they contain highly sensitive personal identifying information for members of Congress, their staff, and law enforcement who were all lawfully present on January 6, 2021, and the process of locating that information and eliminating it from these results continues even today.

[22] We will not perform searches for materials that are not required pursuant to the above-described obligations. We advise defendants who wish to perform wider-ranging searches to wait for the substantial completion of our global discovery plan.

Finally, prosecutors will confirm that FBI case agents conduct searches of FBI databases before trial, to ensure that all relevant documents concerning a specific case or any witnesses have been identified and produced.

Conclusion

The government has taken its Capitol Siege discovery obligations seriously from the inception of this investigation and has made substantial efforts to produce vast quantities of information that is varied and frequently complex in nature in hundreds of cases. These efforts have included:

- Appointing a Capitol Siege Discovery Coordinator in January 2021;
- Assembling a Capitol Siege Discovery Team consisting of experienced attorneys, project managers, and litigation technology professionals;
- Collecting information from multiple sources involved in the response to and investigation of the Capitol Siege;
- Collaborating with FPD to develop a standard protective order for Capitol Siege cases;
- Identifying database solutions for making terabytes of video and documents accessible to hundreds of defendants;
- Funding defense databases and obtaining licenses for all Capitol Siege defense counsel, and collaborating with FPD to execute these solutions;
- Reviewing specific discovery requests by defense counsel to ensure the appropriate materials are prioritized for production;
- Creating protocols and procedures to ensure that (a) case-specific discovery is provided, (b) defendants will receive complete copies of their own unscoped devices and SCA accounts upon request; (c) devices and SCA accounts are systematically filtered for attorney-client communications; (d) relevant scoped digital data and custodial interviews will be uploaded to the government's discovery databases for production to all; and (e) increasing access to discovery by detained defendants.

We have now made substantial progress in our effort to provide the defense appropriate discovery review platforms for both documents and digital media, to populate those platforms, and to use alternative means to provide the most relevant discovery without delay. We will diligently continue to transfer data to our vendors, process it for production, and make productions as expeditiously as possible. As we continue to implement our plan, we will continue to file status memoranda with the Court on a regular basis.

Respectfully submitted,

MATTHEW M. GRAVES
United States Attorney
DC Bar No. 481052

By: /s/ *Emily A. Miller*
Chief, Capitol Siege Discovery Unit
DC Bar No. 462077
555 Fourth Street, N.W., Room 5826
Washington, DC 20530
Emily.Miller2@usdoj.gov
(202) 252-6988

By: */s/ Robert Juman*
ROBERT JUMAN
Assistant United States Attorney
Bar No. NJ 033201993
United States Attorney's Office, Detailee
555 Fourth Street, N.W.
Washington, DC 20530
Phone: (786) 514-9990
E-mail: Robert.juman@usdoj.gov