UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	**CASE NO. 21-CR-197-DLF**
v.	:	
	:	
JACKSON KOSTOLSKY,	:	
	:	
Defendant.	:	

UNITED STATES' MEMORANDUM
REGARDING STATUS OF DISCOVERY AS OF AUGUST 23, 2021

The United States files this memorandum for the purpose of describing our overall approach to discovery, and our discovery plan in relation to voluminous sets of data that the government collected in its investigation of the Capitol Breach cases, among which may be interspersed information the defense may consider material or exculpatory. The materials upon which this memorandum is focused include, for example, thousands of hours of video footage from multiple sources (e.g., Capitol surveillance footage, body-worn-camera footage, results of searches of devices and Stored Communications Act ("SCA") accounts, digital media tips, Parler video, and unpublished news footage), and hundreds of thousands of investigative documents including but not limited to interviews of tipsters, witnesses, investigation subjects, defendants, and members of law enforcement. Further, we write to provide the Court with the status of our implementation of that plan as of August 23, 2021.

I. The Government's Approach to Discovery is Intended to Ensure that All Arguably Exculpatory Materials are Produced in a Comprehensive, Accessible, and Useable Format.

The government has always understood the magnitude and complexity of the discovery project presented by the January 6 attack on the Capitol. We have taken a very expansive view of what may be material or potentially exculpatory and thus discoverable in Capitol Breach

cases. Defense counsel in Capitol Breach cases have made requests including any and all information that captures an individual defendant's conduct or statements; shows people "peacefully walking around the Capitol"; or suggests that a member (or members) of law enforcement allowed people to enter or remain in the Capitol or on restricted grounds, acted friendly or sympathetic to the rioters, or otherwise failed to do their jobs. Of course, there may be additional types of information a defendant may consider material or exculpatory, but since the government does not know the defense theory in any particular case, it is impossible to for the government to determine what other types of information a defendant may believe to be material.

To the extent the type of information described above may exist, it may be interspersed among the voluminous sets of data referenced above. Given the volume of material, and because "[d]efendants are in a better position to determine what evidence they believe is exculpatory and will help in their defense,"[1] it is our intent 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.

[1] *United States v. Meek,* No. 19-cr-00378-JMS-MJD, 2021 WL 1049773 *5 (S.D. Ind. 2021). *See also United States v. Ohle*, No. S3 08 CR 1109 (JSR), 2011 WL 651849 *4 (S.D.N.Y. 2011)(not reported in F.Supp.2d)("placing a higher burden on the Government to uncover such evidence would place prosecutors in the untenable position of having to prepare both sides of the case at once. Indeed, the adversarial system presumes that the defense will be more highly motivated to uncover exculpatory evidence, so if anything the onus is on defense counsel to conduct a more diligent search for material potentially favorable to his client. This is especially true considering that, if exculpatory evidence exists, the defense is in the best position to know what such evidence might be and where it might be located.")

II. Our General Plan for Production of Voluminous Materials Involves Two Separate Platforms.

We have developed and begun implementing a plan to use two primary platforms to process and produce discoverable voluminous materials: one for documents (e.g., items such as law enforcement investigation files and business records) and one for digital materials (e.g., video footage). (These two platforms have frequently been referred to as our "database" although, in fact, they are two separate information repositories hosted by unrelated vendors.) We are working collaboratively with Federal Public Defender ("FPD") leadership and electronic discovery experts, including Sean Broderick, the National Litigation Support Administrator for the Administrative Office of the U.S. Courts, Defender Services Office, to ensure that Federal Public Defender offices nationwide that are working on Capitol Breach cases, counsel that are appointed under the Criminal Justice Act, and retained counsel for people who are financially unable to obtain these services will have access to the same platforms, including technological functionality commensurate to that available to the government, for the purpose of receiving and reviewing discoverable materials.

A. We will Share Documents from Our Own Relativity Workspace to a Defense Relativity Workspace, and are Making Rolling Productions Via Alternative Means Until the Defense Workspace is Available.

1. Overview

Deloitte is hosting a Relativity database, or "workspace," for the government to manage and produce documents. Relativity is a cloud-based eDiscovery platform that offers functionalities including document organization, review, production, and analytics within a single environment, and is an industry leader in eDiscovery hosting. As further elaborated below, we are in the process of ingesting hundreds of thousands of documents into our Relativity

workspace, so that we may review them, process them, and produce the documents as appropriate to the defense.

Ultimately, our plan is for all discoverable documents to be shared to a wholly separate defense Relativity workspace, also hosted by Deloitte, but wholly inaccessible to the government. Deloitte is currently creating such a defense workspace within Relativity for receipt of discoverable documents, and we are working toward a modification of our contract to fund the additional hosting and support of that database.[2]

A Relativity workspace will allow Capitol Breach defense teams to leverage Relativity's search and analytics capabilities to search the voluminous documents we expect to produce for information they believe may be material to their individual cases. Defense teams will be able to perform key term searches and metadata searches across hundreds of thousands of documents in the defense workspace. Further, in conjunction with any staff they designate to support their workspace, they will be able to design coding panes that allow them to "tag" items received in discovery as they deem relevant to their cases, e.g., by location ("Lower West Terrace") or

[2] Hosting refers to storing and organizing documents in a case within a database for document review, organizing, searching, categorizing, and redacting, and providing users with accounts to access the database. Typically, providing discovery in a format that allows it to be loaded into a database satisfies the government's discovery obligations. We understand that neither the Federal Public Defender nor the Criminal Justice Act panel has a vehicle in place through which they may engage in expedited contracting for the hosting and licensing services that are necessary to meet the demands of this unprecedented volume of materials. Thus, the government has agreed to provide the necessary hosting and licensing services through Deloitte. The government has been closely coordinating with FPD to ensure that when we modify our contract with Deloitte, we obtain sufficient licenses to cover the needs of current cases as well as those of cases that may be brought in the future.

defense theories of the case ("Police Let Defendants In"); and then generate search reports based on the results associated with a particular tag or multiple tags.[3]

As elaborated below, although Relativity significantly increases the pace at which we may review and process materials to make appropriate productions, performing these tasks correctly and comprehensively takes time. Nevertheless, we expect to begin making documentary productions from Relativity within the next two weeks, as discussed in more detail below, and will do so on a rolling basis going forward. Until the defense Relativity workspace is operational and defense accounts are established documents will continue to be produced in individualized cases via other available methods – most frequently cloud-based file sharing through USAfx.

2. The Government is Steadily Populating its Own Relativity Database with Materials.

We have already populated our Relativity database with over 30,000 records from the U.S. Capitol Police ("USCP") and USCP reports related to allegations of misconduct by law enforcement in connection with the events of January 6, 2021. We are currently using our Relativity platform to process materials related to allegations of police misconduct and plan to make those reports available within approximately the next two weeks. Capitol Breach

[3] We believe that to ensure defendants have meaningful access to the defense Relativity workspace, FPD will require additional support for the workspace. As the Court is aware, "Even if the discovery is produced in an optimal way, defense counsel may still need expert assistance, such as litigation support personnel, paralegals, or database vendors, to convert e-discovery into a format they can use and to decide what processing, software, and expertise is needed to assess the [Electronically Stored Information]." *See Criminal e-Discovery: A Pocket Guide for Judges*, Chapter II (Common Issues in Criminal e-Discovery), at 12. The *Pocket Guide* serves as a supplement to the federal judiciary's bench book. We are engaging in frequent and productive discussions with FPD in the effort to resolve contractual and technical details related to the implementation of an adequate support plan.

prosecution teams will disseminate these materials once they become available. We are prioritizing these materials and Metropolitan Police Department ("MPD") use-of-force investigation files because many defendants have requested them.

We are steadily working to ingest into Relativity potentially discoverable documents that we requested and received from multiple law enforcement agencies, while ensuring that materials that are or may be protected by Federal Rule of Criminal Procedure 6(e) are adequately protected. Of course, Federal Bureau of Investigation ("FBI") files account for the majority of documentary evidence that we will need to ingest and review. The FBI estimates that there are approximately 750,000 investigative memoranda and attachments in its files associated with the Capitol Breach investigation. We intend to organize, deduplicate, and produce these materials as appropriate, using all of Relativity's tools to do so as quickly as possible. As discussed below, however, these processes are not wholly automated, and will require both technical expertise and manual assistance.

3. <u>The Workflow in Processing Materials for Discovery Takes Time.</u>

The process of populating Relativity with potentially discoverable material, all in varied formats and from different sources, is complicated. It is *not* like copying and pasting a file, or even like duplicating a hard drive. Before the hundreds of thousands of investigative files at issue here are ever loaded to Relativity, they must be meaningfully organized into folder structures that will make sense to reviewers and recipients. The materials must also be quality-checked, e.g., we must ensure that we have the password for protected documents, that the documents were provided in a format that will open, and that we remove irrelevant software and system files that would only cloud the workspace and confuse reviewers. After materials are loaded to Relativity, we must customize the manner in which they are displayed so as to be

meaningful to reviewers who will make discoverability determinations and apply appropriate redactions and sensitivity designations. Not all documents are created equal, e.g., financial records and forensic cell phone search reports cannot meaningfully be displayed in the same way.

All of these processes will be assisted by leveraging Relativity's tools as much as possible, such as by using keyword searches to identify items that must be excluded or redacted; and deduplication tools to recognize documents that have already been processed so that they are not analyzed or reproduced multiple times. Although these processes are time-consuming, they are necessary to avoid production of unorganized data dumps, unreadable files, and unusable databases; or a failure of the government to take adequate steps to prevent both victims and defendants' private information from being shared with hundreds of defendants.

B. We will Share Digital Evidence from Our Own Evidence.com Instance to a Defense Evidence.com Instance, and Make Rolling Productions as Digital Media is Processed.

Relativity was primarily designed as document review platform and not to manage terabytes of digital evidence. Although it is technologically possible to view and share video evidence within Relativity, in this case, the volume of video would significantly reduce Relativity's performance speed.

Accordingly, we will use evidence.com as a platform to manage, review, and share digital media evidence. Evidence.com is a cloud-based digital evidence management system designed by Axon Enterprise, Inc. ("Axon"), an industry leader in body-worn-camera systems. Axon refers to a singular environment of evidence.com as an "instance." The government has agreed to fund a defense instance of evidence.com and to provide the necessary licensing services through Axon. This instance will be managed and administered by FPD, and the

government will have no ability to log into or retrieve information from this instance. As recently as Saturday, August 21, 2021, we consulted with representatives from Axon about our plan and we expect our contract with Axon will be modified expeditiously. As with Relativity, the government has been closely coordinating with FPD to ensure that we cover the needs of current cases as well as those of cases that may be brought in the future. We understand that legal defense teams will likely wish to share voluminous evidence with defendants. Axon has additional infrastructure referred to as my.evidence.com that will allow defense attorneys to share voluminous evidence with individual defendants.

We have already migrated over 2,900 body-worn-camera videos totaling over 2,300 hours (nearly 100 days) into our instance of evidence.com. For the reasons relayed above, from a technological perspective, we expect to be able to share this footage with FPD's evidence.com instance within approximately the next two weeks. Before we can share voluminous video footage with FPD, we must also ensure that the footage is adequately protected. Based on a review of the body-worn-camera footage conducted by our Office, the footage displays approximately 1,000 events that may be characterized as assaults on federal officers. As these officers now, or in the future may, qualify as victims under the Crime Victims Rights Act, they have the "right to be reasonably protected from the accused" and the "right to be treated with fairness and with respect of the victim's dignity and privacy." 18 U.S.C. §§ 3771(a)(1) and (8).

When we share the footage, we also intend to share information we have developed that will help facilitate efficient defense review of body-worn-camera footage. For example:

- Individuals in our Office who reviewed all the body-worn-camera footage in our instance created a spreadsheet that identifies footage by agency, officer, video start time, a summary of events, and location of the camera in 15-minute increments. The locations are defined in zone map they created. We will share our zone map and the spreadsheet with the legal defense teams, subject to adequate protection.

- We obtained from MPD Global Positioning Satellite ("GPS") information for radios that may be of assistance in identifying the location of officers whose body-worn-camera footage is relevant to the defense. We will share this information with the legal defense teams, subject to adequate protection.

We will continue to ingest video evidence into evidence.com on a rolling basis, and to produce it regularly. As evidence.com was designed to function in coordination with body-worn-cameras designed by Axon, ingesting body-worn-camera footage into our instance was fairly simple. Other footage will need to be converted from proprietary formats before it can be ingested into evidence.com, and so processing will take longer.

At this time, the FBI is in the process of transmitting Capitol surveillance footage for ingestion into evidence.com. Because of the size of the footage, it will take several weeks to receive and ingest the footage. Based on our current understanding of the technical complexities involved, we expect to start rolling productions from 7,000 hours of footage that the USCP provided the FBI within approximately the next four weeks. An additional 7,000 hours of footage is not relevant to this case and, therefore will not be produced.

III. Conclusion.

In sum, while we have not resolved every contractual or technical detail, and while our discovery plan continually evolves to address issues as they arise, we are making substantial progress in our diligent efforts to provide the defense comparable 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 are confident that our plan will come to fruition, and although we have not reached agreement on every aspect of this plan, we continue to have good faith, productive discussions with FPD regarding production of voluminous data. In the interim, we will diligently continue to transfer data to our vendors, process it for production, and make interim productions by other means until the defense platforms are in place. As we continue to implement our plan, we will continue to file status memoranda with the Court on a regular basis.

Respectfully submitted,

CHANNING D. PHILLIPS
Acting United States Attorney
DC Bar No. 415793

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

By: */s/ Mona Lee M. Furst*
MONA LEE M. FURST
Assistant United States Attorney
Kansas Bar No. 13162
Detailee
United States Attorney's Office
District of Columbia
Mona.Furst@usdoj.gov
(316) 269-6537