UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	**CRIMINAL NO. 21-cr-28 (APM)**
v.	:	
	:	
THOMAS CALDWELL,	:	
DONOVAN CROWL,	:	
JESSICA WATKINS,	:	
SANDRA PARKER,	:	
BENNIE PARKER,	:	
LAURA STEELE,	:	
KELLY MEGGS,	:	
CONNIE MEGGS,	:	
KENNETH HARRELSON,	:	
ROBERTO MINUTA,	:	
JOSHUA JAMES,	:	
JONATHAN WALDEN,	:	
JOSEPH HACKETT,	:	
JASON DOLAN,	:	
WILLIAM ISAACS,	:	
DAVID MOERSCHEL, and	:	
BRIAN ULRICH,	:	
	:	
Defendants.	:	

UNITED STATES' NOTICE REGARDING THE STATUS OF DISCOVERY
IN ADVANCE OF SEPTEMBER 16, 2021 HEARING

The United States files this notice in advance of the hearing scheduled for September 16, 2021, to supplement representations made at the status hearing on August 10, 2021, and in the notice filed by the government on August 18, 2021, as to the status of discovery in both the instant case ("case-specific discovery") and across its investigation of all Capitol Breach cases ("office-wide discovery"). The United States has already provided the majority of discovery relevant to the individual defendants charged in this case, and the government continues to anticipate that defense versions of two evidence review platforms—the Relativity database for documentary

material and the cloud-based digital management system for digital material—will be available by early October and will be populated with discovery productions on a rolling basis.

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. Accordingly, a Capitol Breach Discovery Coordinator was appointed on or about January 27, 2021, to manage and organize this project. The coordinator began to quickly assemble a core Discovery Team to create and implement a process for the production of discovery in January 6 cases. The Discovery Team is staffed by federal prosecutors who have experience in managing complex investigations involving voluminous materials, Department of Justice experts in project management and electronic discovery management, and a lead discovery agent from the Federal Bureau of Investigation. Members of the Discovery Team consult regularly with Department of Justice subject matter experts, including Associate Deputy Attorney General and National Criminal Discovery Coordinator Andrew Goldsmith. As discussed further below, members of the Discovery Team also meet and confer on a regular basis with Federal Public Defender ("FPD") leadership and electronic discovery experts.

The Discovery Team recognized that due to the nature and volume of materials being collected, the government would require the use of an outside contractor who could provide litigation technology support services to include highly technical and specialized data and document processing and review capabilities. The government drafted a statement of work, solicited bids, evaluated them, and selected a vendor. The initial draft of a Statement of Work was completed no later than February 1, 2021. This investigation is unprecedented in size and

scope, and as more information was been learned about the scope of the evidence, the Statement of Work necessarily was revised; it was also reviewed multiple times at various levels of the Department of Justice before it was approved for publication on April 19, 2021. Final bids were received on or about May 10, 2021.

On or about May 28, 2021, the government contracted Deloitte Financial Advisory Services, LLP ("Deloitte"), a litigation support vendor with extensive experience providing complex litigation technology services, to assist in document processing, review and production of materials related to the attack on the Capitol. As is required here, Deloitte furnishes secure, complex, and highly technical expertise in scanning, coding, digitizing, and performing optical character recognition – as well as processing, organizing, and ingesting a large volume of Electronically Stored Information ("ESI") and associated metadata in document review platforms – which is vital to the United States' ability to review large data/document productions and is essential to our ability to prosecute these cases effectively. The government began transferring data to Deloitte the week of June 8, 2021.

The voluminous office-wide materials, from across the roughly 600 Capitol Breach cases, that are being prepared for discovery include:

- Thousands of hours of closed circuit video ("CCV") from sources including the U.S. Capitol Police ("USCP"), D.C. Metropolitan Police Department ("MPD"), and United States Secret Service, and several hundred MPD Automated Traffic Enforcement camera videos;

- Footage from Cable-Satellite Public Affairs Network (C-SPAN) and other members of the press;

- Thousands of hours of body worn camera ("BWC") footage from MPD, Arlington County Police Department, Montgomery County Police Department, Fairfax County Police Department, and Virginia State Police;

- Radio transmissions, event chronologies, and, to a limited extent, Global Positioning Satellite ("GPS") records for MPD radios;

- Hundreds of thousands of tips, including at least 237,000 digital media tips;
- Location history data for thousands of devices present inside the Capitol (obtained from a variety of sources);
- Subscriber and toll records for hundreds of phone numbers;
- Cell tower data for thousands of devices that connected to the Capitol's interior Distributed Antenna System (DAS) during the attack on the Capitol (obtained from the three major telephone companies);
- A collection of over one million Parler posts, replies, and related data;
- A collection over one million Parler videos and images (approximately 20 terabytes of data);
- Damage estimates from multiple offices of the U.S. Capitol;
- Data from a multitude of digital devices and Stored Communication Act ("SCA") accounts (e.g., email and social media accounts) that have been seized and searched pursuant to warrants and/or consent; and
- Responses to grand jury subpoenas, of which over 6,000 have been issued, seeking documents such as financial records, telephone records, electronic communications service provider records, and travel records.

In addition to the materials collected, tens of thousands of documents have been generated in furtherance of the investigation, to include reports documenting interviews of subjects, witnesses, tipsters and officers; investigations into allegations concerning officer conduct on January 6; source reports; evidence collection reports; evidence analysis reports; chain-of-custody documents; legal documents including preservation letters, subpoenas, 2703(d) orders, consent forms, and search warrants; and memoranda of investigative steps taken to evaluate leads or further investigations.

The government has 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.

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

[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.")

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 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 FPD 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.

As discussed in prior pleadings and hearings before this Court, 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. Deloitte has also now established a Capitol Breach defense Relativity workspace. We continue to work toward a modification of our contract to fund the additional hosting and support of that database. Modifying the Deloitte contract presents multiple contractual, technical, and legal challenges that are not posed by the Axon (Evidence.com) contract discussed in Section II.B below, but we are moving with as much haste as possible given the various complexities.

We believe that by October, the contract modifications will be completed, thus allowing

for defense access to the Relativity database.[2] To give the Court a sense of just some of the challenges that we are addressing, they include formulating concrete plans describing the staffing and technological safeguards that will be put into place to eliminate the possibility of work product being shared from one workspace to another. We must also ensure the modification, which must be fairly detailed under applicable government contracting rules and regulations, will be sufficient to support hundreds of defense cases, and are working closely with FPD in support of that effort. As this undertaking by FPD is also unprecedented, handling the contract modification correctly takes time. FPD will work with Defender Service's National Litigation Support Team to create a structure for distributing and tracking Relativity licenses and anticipates updating defense counsel with the status of their work approximately one week after the contract is modified to provide access to FPD. Finally, we must ensure that in making available hundreds of thousands of documents to hundreds of legal defense teams, we are careful to ensure that materials are properly scoped pursuant to the terms of any applicable warrants, and that access to the database is restricted in a manner that will ensure our compliance with applicable privacy laws. We are currently consulting with Department of Justice experts in privacy and discovery to ensure that these issues are properly handled.

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

[2] To be clear, while we expect the defense Relativity database will be partially populated in October, we do not expect it to be complete at that time. We will continue to populate the database with data on a rolling basis.

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 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]

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. 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

---

[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.

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.[4]

Importantly, the government is not waiting for the defense Relativity workspace to be up and running to make productions of office-wide discovery. We have already begun making documentary productions from Relativity, and until the defense Relativity workspace is accessible, we will continue to provide voluminous documents from our Relativity database through individualized productions methods – most frequently cloud-based file sharing through USAfx. (Any productions we make will also be added to the defense Relativity workspace.) On Friday, September 10, 2021, the Discovery Team made available for production in all Capitol Breach cases approximately 850 pages consisting of redacted reports from USCP investigations of alleged wrongdoing by USCP officers on January 6, 2021. The undersigned counsel made these records available to defense counsel in the instant case on Saturday, September 11, 2021. We anticipate providing Metropolitan Police Department internal investigation reports (approximately 600

[4] Under our plan, document productions from Relativity will be made on a rolling basis, and we are prioritizing the processing and production of documents that have been requested by Capitol Breach defendants. Ultimately, we will also make any documents we produce available to a defense Relativity workspace. This will allow Capitol Breach defense teams to leverage Relativity's search and analytics capabilities to search the voluminous documents for information they believe may be material to their individual cases.

pages) by next week. We are still reviewing the approximately 30,000 files in Relativity that were provided to us by USCP.

As the Discovery Team continues to receive additional documents, they will cull them of any materials potentially protected by Federal Rule of Criminal Procedure 6(e) and provide the remainder (a majority) to Deloitte for ingestion into our Relativity database for discovery review. At this time, we have provided Deloitte the following additional documents for ingestion into our Relativity database:

- Discovery productions (approximately 11,500 records) that have been made in complex Capitol Breach cases (e.g., multi-defendant conspiracies such as this case and cases involving members and affiliates of the Proud Boys) (approximately 11,500 records);[5] and

- Approximately 24,000 Federal Bureau of Investigation records.

This week, we also expect to provide Deloitte discovery productions that have been made in 75 individual cases (approximately 32,000 documents).[6]

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

[5] Although these productions were already made in the relevant cases, they will ultimately be made accessible to all Capitol Breach defendants through the defense Relativity workspace.

[6] Again, although these productions were already made in the relevant cases, they will ultimately be made accessible to all Capitol Breach defendants through the defense Relativity workspace.

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.[7] 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 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 migrated over 2,900 body-worn-camera videos totaling over 2,300 hours (nearly 100 days) into our instance of evidence.com.[8] As a result of the September 3, 2021 contract modifications, we are now technologically able to share these body-worn-camera videos to the defense instance of evidence.com. To ensure this enormous production is organized and meaningful for the defense, we are currently categorizing and tagging the videos. Further, to ensure that the videos (which display approximately 1,000 assaults upon officers and include occasional references to personal identifying information) are adequately protected, we are also

---

[7] On Friday, September 3, 2021, the government amended its contract with Axon Enterprise, Inc. ("Axon"), to fund a defense environment or "instance" of evidence.com administered by the Federal Public Defender for the District of Columbia.

[8] As discussed in greater detail below, extensive digital evidence that will be in this platform has already been provided to the defense in this case: the government has already provided defendants over 300 gigabytes of surveillance video and BWC that we have identified as relevant to these defendants, as well as numerous public source videos.|

exploring whether it is technologically possible for downloading to be automatically suppressed when highly sensitive video is shared by defense counsel to defendants.

We are hopeful we will be able to transfer the body-worn-camera footage to the defense instance of evidence.com by the end of this week (Friday, September 17, 2021), and expect to produce it no later than the end of next week (Friday, September 24, 2021). 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 is taking 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 by the end of September. An additional 7,000 hours of footage is not relevant to this case and, therefore will not be produced.

C. Incarcerated Defendants

It has come to the undersigned's attention that the detained defendants are experiencing very long wait times to be able to review the discovery materials provided in these Capitol Breach cases. In collaboration with FPD, we are developing proposals to increase access by incarcerated defendants to voluminous materials, which we expect to share with the D.C. Department of Corrections and to discuss within the next two weeks.

III. Status of Discovery in the Instant Case

As discussed at the hearing on August 10, 2021, in this case, the government has already provided the materials that are most relevant to the pending charges. The government has continued to provide discovery since that hearing. To date, the government has produced nearly two terabytes of data of discovery materials generated in this particular case. These materials include:

- U.S. Capitol surveillance footage from nearly two dozen cameras (comprising approximately 250 gigabytes of data) that the government has identified as capturing these defendants' movements through the Capitol and its exterior grounds;
- Surveillance video from two local hotels where some of these defendants and/or related subjects of this investigation stayed during the January 5-7 time period (comprising approximately 80 gigabytes of data);
- MPD bodyworn camera footage (comprising approximately 10 gigabytes of data) that the government has identified as capturing these defendants' actions on January 6;
- Public source videos located by the government that appear to capture these defendants' actions on January 6;
- Digital data extractions from approximately 50 devices and SCA accounts associated with or seized from these defendants or their homes;[9]

[9] As the Court is aware, with the consent of the defendants, the government has provided the entire, unscoped and unfiltered versions of these digital extractions to the defense. As the government hoped, it is nearly finished with the process of "scoping" these extractions, or

- Discoverable FBI reports generated between the outset of this investigation and mid-August, which include but are not limited to reports documenting some witness interviews and information about and photographs of evidence seized during search warrants executed on these defendants' homes;

- Discoverable grand jury subpoena returns received from the outset of this investigation through mid-August;[10] and

- Disclosures about information and evidence identified during this investigation that may be material to the defense.

The government has also offered the opportunity for defense counsel and their investigators to attend tours of the crime scene; the government has provided an accounting of the physical evidence seized from the defendants and has offered to make such items available for viewing; and the government has offered to hold reverse proffers or less formal phone conversations with defense counsel to help walk them through the voluminous discovery materials.

Undersigned counsel have also taken steps to identify defendants outside the instant case, who had devices or SCA accounts seized and/or searched, and who were in a position where they may have taken photos or videos on their electronic devices that could have captured the conduct or statements of the defendants charged in the instant case. For example, in disclosures made on August 12, 2021, and August 24, 2021, the government provided counsel with videos from cell phones and social media accounts of three defendants charged in other cases that captured

---

identifying content and data that is relevant under the terms of the corresponding search warrants or the government's discovery obligations, and the government is working to get the scoped editions of all of these digital extractions provided to the defense. (Some are too large to provide through the government's cloud-based file-sharing system and will need to be downloaded on external hard drives to be provided to the defense.) The government anticipates that these scoped data sets will greatly help to narrow the defendants' focus as to the evidence that the government has identified as relevant in this matter.

[10] As this investigation is ongoing, the government is producing these FBI reports and grand jury returns on a rolling basis. The government is currently up-to-date through mid-August with respect to evidence gathered with respect to the above-captioned defendants.

defendants in the instant case saying and doing things that the government thought might arguably be material to their defenses. We will continue to make such disclosures on a rolling basis. We anticipate that these efforts will be greatly facilitated once the Relativity and Evidence.com databases discussed above are up and running and more fully populated with data.

IV. 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, and to address the ongoing nature of this investigation, we are making substantial progress in our 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. 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 update the Court through the regular filing of discovery status memoranda and oral representations at any hearings scheduled by the Court.

Respectfully submitted,

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

By: _____

Kathryn L. Rakoczy
Assistant United States Attorney
D.C. Bar No. 994559
Ahmed M. Baset
Troy A. Edwards, Jr.
Jeffrey S. Nestler
Assistant United States Attorneys

Louis Manzo
Special Assistant United States Attorney
U.S. Attorney's Office for the District of Columbia
555 4th Street, N.W.
Washington, D.C. 20530

/s/ Alexandra Hughes
Alexandra Hughes
Justin Sher
Trial Attorneys
National Security Division
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20004