UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information stored by Google related to investigation of violations of 18 U.S.C. § 371 and other offenses	)	Case No. MJ20-643

APPLICATION FOR A SEARCH WARRANT

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

See Attachment A, incorporated herein by reference.

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

See Attachment B, incorporated herein by reference.

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

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

The search is related to a violation of:

Code Section	*Offense Description*
26 U.S.C. § 5861(d)	Unlawful Possession of Destructive Devices
18 U.S.C. § 844(i), 371	Arson, Conspiracy

The application is based on these facts:

✓ See Affidavit of FBI Special Agent Michael Stults, continued on the attached sheet.

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

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Michael Stults, FBI Special Agent

Printed name and title

◯ The foregoing affidavit was sworn to before me and signed in my presence, or

◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 10/07/2020

Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, Chief United States Magistrate Judge

Printed name and title

ATTACHMENT A

Property To Be Searched

This warrant is directed to Google LLC and applies to:

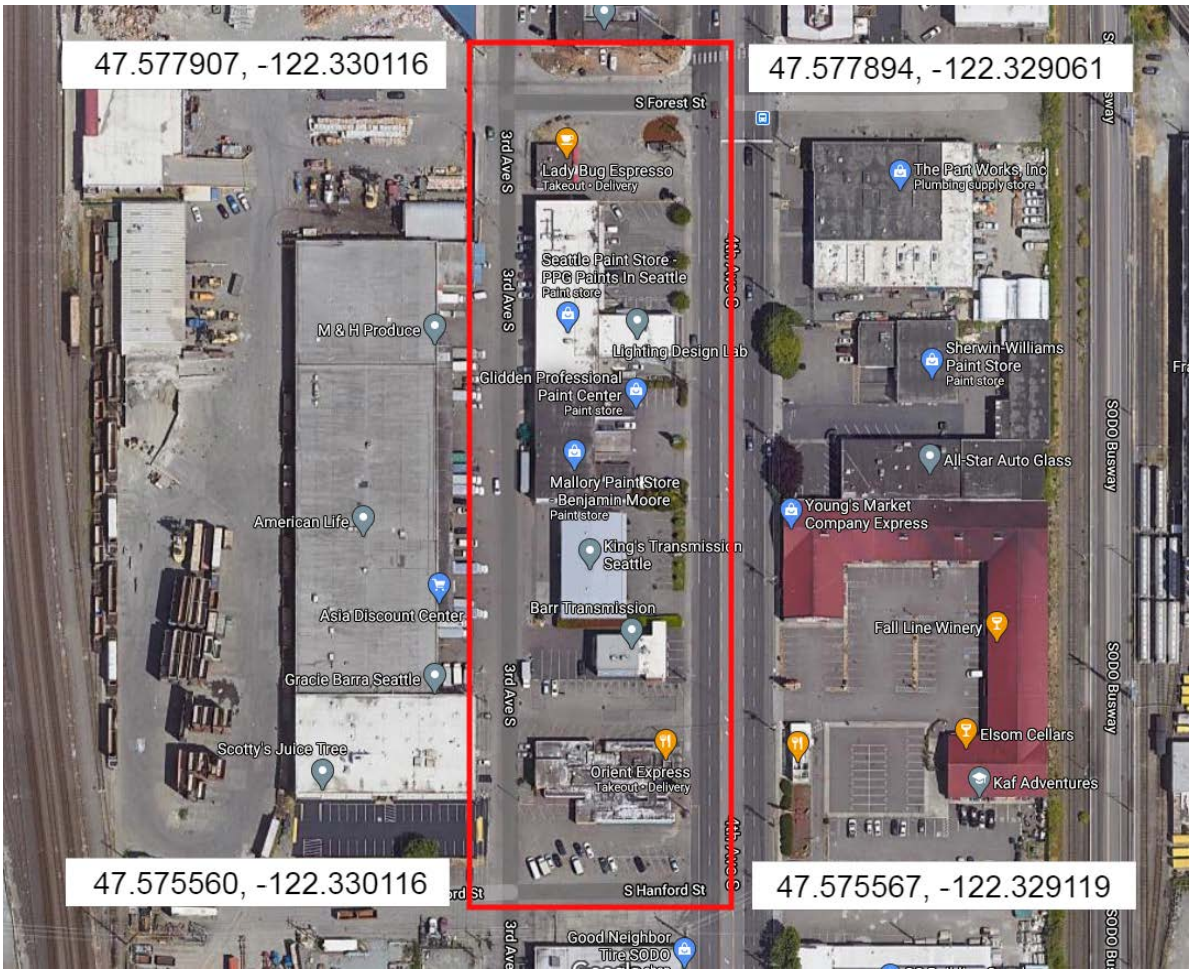
(1) Location History data, sourced from information including GPS data and information about visible wi-fi points and Bluetooth beacons transmitted from devices to Google, reflecting devices that Google calculated were or could have been (as indicated by margin of error, *i.e.*, "maps display radius") located within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below ("Initial Search Parameters"); and

(2) Identifying information for Google Accounts associated with the responsive Location History data.

Initial Search Parameters

- **Date:** August 24, 2020
- **Time period:** From 10:00 p.m. to 11:15 p.m. (PDT)
- **Target Location:** Geographical area (see map below) identified as a polygon defined by the following four latitude/longitude coordinates connected by straight lines:
  - 47.577907, -122.330116
  - 47.577894, -122.329061
  - 47.575560, -122.330116
  - 47.575567, -122.329119

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

Particular Items to Be Seized

I. Information to be disclosed by Google

The information described in Attachment A, via the following process:

1. Google shall query location history data based on the Initial Search Parameters specified in Attachment A. For each location point recorded within the Initial Search Parameters, and for each location point recorded outside the Initial Search Parameters where the margin of error (*i.e.*, "maps display radius") would permit the device to be located within the Initial Search Parameters, Google shall produce to the government information specifying the corresponding unique device ID, timestamp, location coordinates, display radius, and data source, if available (the "Device List").

2. The government shall review the Device List and identify to Google the devices about which it seeks to obtain Google account identifier and basic subscriber information. The government may, at its discretion, identify a subset of the devices.

3. Google shall disclose to the government identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Accounts associated with each device ID appearing on the Device List about which the government inquires.

This warrant does not authorize the disclosure or seizure of any tangible property or the content of any wire or electronic communication, as defined in 18 U.S.C. § 2510(8)

II. Information to Be Seized

All information described above in Section I that constitutes evidence of violations of Title 18, United States Code, Section 5861(d) (Unlawful Possession of Destructive Devices), Title 18, United States Code, Section 844(i) (Arson), and Title 18, United States Code, Section 371 (Conspiracy), committed on August 24, 2020, by unknown persons.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Michael Stults, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since 2018. During my time as a Special Agent, I have participated in investigations pertaining to arson and other federal criminal violations. I have completed the New Agents Training Course at the FBI Academy in Quantico, Virginia. In addition to conducting federal criminal investigations, I have also completed training in information security technologies and open source intelligence gathering. I have training and experience in arrest procedures, search warrant applications, the execution of searches and seizures, and various other criminal laws and procedures. I have participated in the process of search warrants involving the geolocation data and cellular technologies.

I make this affidavit in support of an application for a warrant to search information that is stored at premises controlled by Google LLC ("Google"), a provider of an electronic communications service and remote computing service headquartered in Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government the information further described in Attachment B.I. The government will then review that information and seize the information that is further described in Attachment B.II.

This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 5861(d) (Unlawful Possession of Destructive Devices); Title 18, United States Code, Section 844(i) (Arson); and Title 18, United States Code, Section 371 (Conspiracy), have been committed

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

by unknown persons. There is also probable cause to search the information described in Attachment A for evidence of these crimes as further described in Attachment B.

JURISDICTION

This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO GOOGLE'S SERVICES AND RELEVANT TECHNOLOGY

Based on my training and experience, I know that cellular devices, such as mobile telephones, are wireless devices that enable their users to send and receive wire and/or electronic communications using the networks provided by cellular service providers. In order to send or receive communications, cellular devices connect to radio antennas that are part of the cellular network called "cell sites," which can be mounted on towers, buildings, or other infrastructure. Cell sites provide service to specific geographic areas, although the service area of a given cell site will depend on factors including the distance between towers. As a result, information about what cell site a cellular device connected to at a specific time can provide the basis for an inference about the general geographic location of the device.

Based on my training and experience, I also know that many cellular devices such as mobile telephones have the capability to connect to wireless internet ("wi-fi") access points if a user enables wi-fi connectivity. Wi-fi access points, such as those created through the use of a router and offered in places such as homes, hotels, airports, and coffee shops, are identified by a service set identifier ("SSID") that functions as the name of the wi-fi network. In general, devices with wi-fi capability routinely scan their environment to determine what wi-fi access points are within range and will display the names of networks within range under the device's wi-fi settings.

Based on my training and experience, I also know that many cellular devices feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

devices, such as between a mobile device and Bluetooth-enabled headphones. Bluetooth uses radio waves to allow the devices to exchange information. When Bluetooth is enabled, a mobile device routinely scans its environment to identify Bluetooth devices, which emit beacons that can be detected by mobile devices within the Bluetooth device's transmission range, to which it might connect.

Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system ("GPS") technology. Using this technology, the phone can determine its precise geographical coordinates. If permitted by the user, this information is used by apps installed on a device as part of the app's operation.

Based on my training and experience, I know Google is a company that, among other things, offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

In addition, based on my training and experience, I know that Google offers numerous apps and online-based services, including messaging and calling (*e.g.*, Gmail, Hangouts, Duo, Voice), navigation (Maps), search engine (Google Search), and file creation, storage, and sharing (*e.g.*, Drive, Keep, Photos, and YouTube). Many of these services are accessible only to users who have signed in to their Google accounts. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address (*e.g.*, example@gmail.com). Other services, such as Maps and YouTube, can be used with limited functionality without the user being signed in to a Google account.

Based on my training and experience, I also know Google offers an Internet browser known as Chrome that can be used on both computers and mobile devices. A user has the ability to sign-in to a Google account while using Chrome, which allows the user's bookmarks, browsing history, and other settings to be uploaded to Google and then synced across the various devices on which the subscriber may use the Chrome browsing software, although Chrome can also be used without signing into a Google account. Chrome is not

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

limited to mobile devices running the Android operating system and can also be installed and used on Apple devices and Windows computers, among others.

Based on my training and experience, I know that, in the context of mobile devices, Google's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, devices that do not run the Android operating system, such as Apple devices.

According to my training and experience, as well as open-source materials published by Google, I know that Google offers accountholders a service called "Location History," which authorizes Google, when certain prerequisites are satisfied, to collect and retain a record of the locations where Google calculated a device to be based on information transmitted to Google by the device. That Location History is stored on Google servers, and it is associated with the Google account that is associated with the device. Each accountholder may view their Location History and may delete all or part of it at any time.

Based on my training and experience, I know that the location information collected by Google and stored within an account's Location History is derived from sources including GPS data and information about the wi-fi access points and Bluetooth beacons within range of the device. Google uses this information to calculate the device's estimated latitude and longitude, which varies in its accuracy depending on the source of the data. Google records the margin of error for its calculation as to the location of a device as a meter radius, referred to by Google as a "maps display radius," for each latitude and longitude point.

Based on open-source materials published by Google and my training and experience, I know that Location History is not turned on by default. A Google accountholder must opt-in to Location History and must enable location reporting with respect to each specific device and application on which they use their Google account in order for that usage to be recorded in Location History. A Google accountholder can also prevent additional Location History records from being created at any time by turning off the Location History setting for their Google account or by disabling location reporting for a particular device or Google

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

application. When Location History is enabled, however, Google collects and retains location data for each device with Location Services enabled, associates it with the relevant Google account, and then uses this information for various purposes, including to tailor search results based on the user's location, to determine the user's location when Google Maps is used, and to provide location-based advertising. As noted above, the Google accountholder also has the ability to view and, if desired, delete some or all Location History entries at any time by logging into their Google account or by enabling auto-deletion of their Location History records older than a set number of months.

Location data, such as the location data in the possession of Google in the form of its users' Location Histories, can assist in a criminal investigation in various ways. As relevant here, I know based on my training and experience that Google has the ability to determine, based on location data collected and retained via the use of Google products as described above, devices that were likely in a particular geographic area during a particular time frame and to determine which Google account(s) those devices are associated with. Among other things, this information can indicate that a Google accountholder was near a given location at a time relevant to the criminal investigation by showing that the device reported being there.

Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information often provide clues to their identity, location, or illicit activities.

Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

its system. This information can include the date on which the account was created, the length of service, records of login (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

SUMMARY OF INVESTIGATION

A. The Seattle Police Officers Guild.

The Seattle Police Officers Guild ("SPOG") is the largest police labor union in the Pacific Northwest. According to its website, the SPOG represents over 1,300 members including all of the officers and sergeants serving on the Seattle Police Department ("SPD"). The SPOG headquarters is located in the building at 2949 Fourth Avenue South, in Seattle.

The SPOG is involved in interstate and foreign commerce and in activities affecting interstate and foreign commerce. For example: (a) the SPOG is a member of the United Coalition of Public Safety ("UCOPS"), a national organization comprised of approximately 20 police unions from at least seven states across the United States representing more than 38,000 law enforcement officers, with the President of the SPOG concurrently serving as the Treasurer of UCOPS; (b) the SPOG provides space within its building to Crime Stoppers, a national organization that spans the United States to create a network of local programs that work together to prevent and solve crimes in communities and schools across the nation; (c) the SPOG also provides space within its building to Code 4 Northwest, a crisis response and referral network for Washington State active and retired first responders, EMS, corrections, civilian support personnel, and their families; (d) the SPOG accepts and processes payments and donations from individuals located outside of the State of Washington by providing a link on its website to the national www.stopdefunding.com

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

campaign; and (e) the SPOG provides benefits to its members including insurance coverage from insurance companies located in Oregon and California.[1]

Since late May 2020, the SPD and the SPOG have been focal points of regular demonstrations and, on multiple occasions, have been targeted in acts of violence and property destruction.

B. The Attack on the SPOG Building on August 24, 2020.

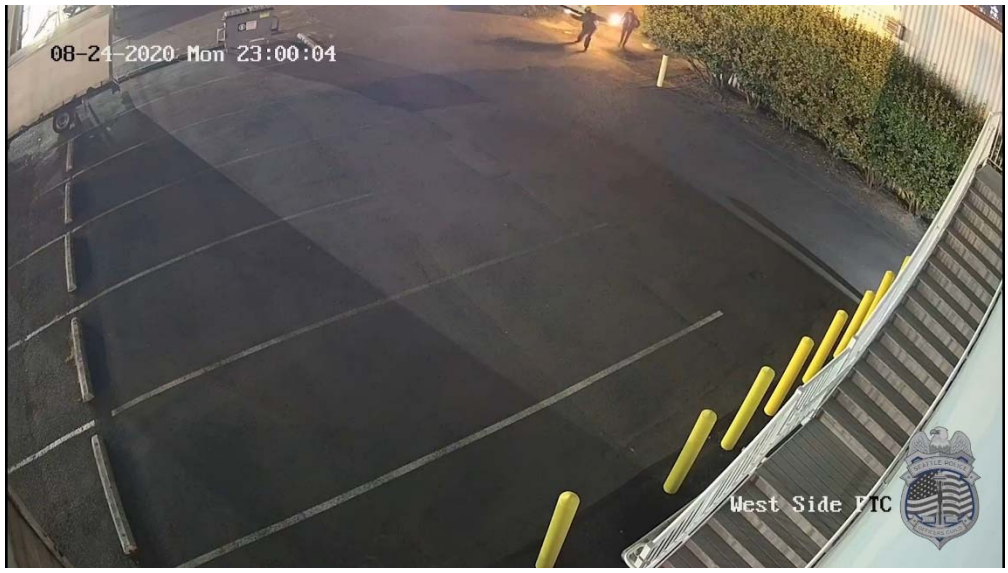
On August 24, 2020, at approximately 11:00 p.m., two unknown suspects intentionally damaged the SPOG building using what I believe to be improvised incendiary devices. This incident was captured by security cameras located on the SPOG building. The footage shows the suspects lighting and throwing what appears to be three glass bottles with ignited fabric or paper wicks (*i.e.*, Molotov cocktail devices) at the northwest side of the SPOG building, in an apparent attempt to set the structure on fire.[2]

---

[1] The Seattle Police Department itself also is involved in interstate and foreign commerce and in activities affecting interstate and foreign commerce. *See United States v. Odom*, 252 F.3d 1289, 1294 (11th Cir. 2001) ("The legislative history of § 844(i) reveals that the statute was crafted specifically to include some non-business property such as police stations and churches.") (citing *Russell v. United States*, 471 U.S. 858, 860 (1985)); *United States v. Laton*, 352 F.3d 286, 300 (6th Cir. 2003) ("When it crafted § 844(i) to encompass the arson of police stations, Congress recognized that the provision of emergency services by municipalities can affect interstate commerce in the active sense of the phrase.") (citing *Jones v. United States*, 529 U.S. 848, 853 n.5 (2000); *Russell*, 471 U.S. at 860–61); *Belflower v. United States*, 129 F.3d 1459, 1462 (11th Cir.1997) (holding that § 844(i) covered the bombing of a police vehicle which a local sheriff's deputy used in his law enforcement responsibilities and that destruction of a police car had "a significant impact on interstate commerce" because the deputy patrolled traffic and made arrests on an interstate highway, issued citations to out-of-state drivers, participated in interstate narcotic investigations, assisted out-of-state authorities in apprehending suspects, recovered stolen property from other states, and attended law enforcement training sessions in other states).

[2] The Ninth Circuit Court of Appeals recently reaffirmed the well-settled proposition that a Molotov cocktail device constitutes a "destructive device" under federal law. *United States v. Barker*, 689 Fed. Appx. 555 (9th Cir. 2017) ("We hold that a Molotov cocktail fits within the firearm category of 'a destructive device.' A Molotov cocktail is an incendiary device that is quite similar to a grenade. Therefore, possession constitutes a crime of violence."). Federal "courts have uniformly held that a fully-assembled Molotov cocktail device – defined as a device comprising a bottle, gasoline, and a rag – constitutes an 'incendiary ... bomb' or 'similar device' under section 5845(f)." *United States v. Simmons*, 83 F.3d 686, 687–88 (4th Cir. 1996) (citing *United States v. Peterson*, 475 F.2d 806, 811 (9th Cir. 1973) (device comparable to a Molotov cocktail was a "destructive device"); *United States v. Neal*, 692 F.2d 1296, 1303-04 (10th Cir.1982) (affirming conviction for possession of a destructive device made from "a one gallon plastic jug, a flammable liquid, and a rag wick"); *United States v. Campbell*, 685 F.2d 131, 132 (5th Cir.1982) (sustaining indictment for possession of a destructive device "made from cloth rags, [and] flammable liquid with a fuse made of incense sticks"); *United States v. Ross*, 458 F.2d 1144, 1144-46, 1144 n. 1 (5th Cir. 1972) (affirming conviction for possession of "crude incendiary devices" consisting of "a quart glass bottle with cloth therein and containing a flammable liquid and having a cloth wick in the mouth of said bottle); *United States v. Curtis*, 520 F.2d 1300, 1304 (1st Cir.1975) ("[W]hile gasoline, bottles and rags all may be legally possessed, their combination into the type of home-made incendiary bomb

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



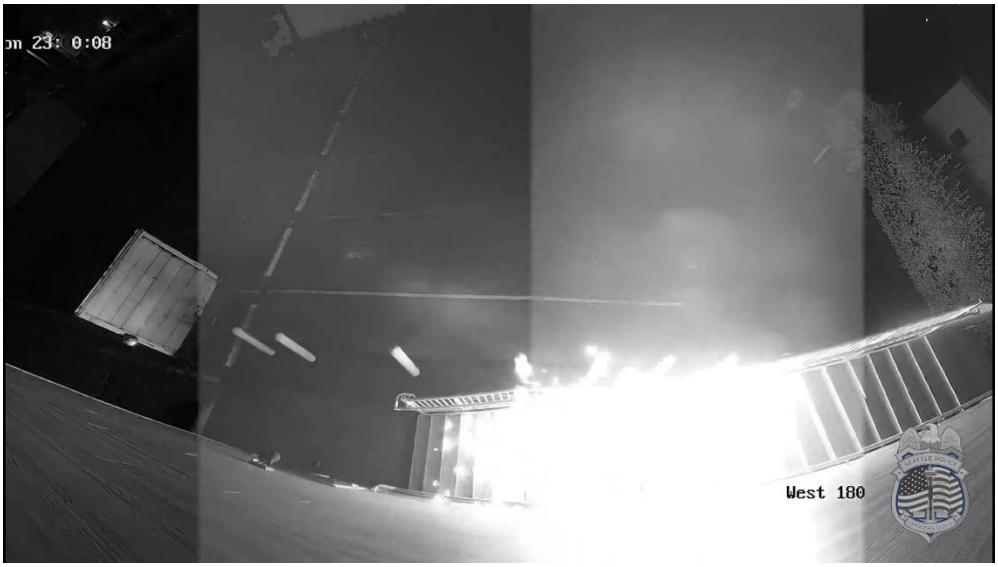
One of the devices impacted the west side of the building where the flames spread rapidly, almost instantaneously, along the impact location. The spread was consistent with the rapid escape of a flammable liquid from a broken container. One of the subjects threw

---

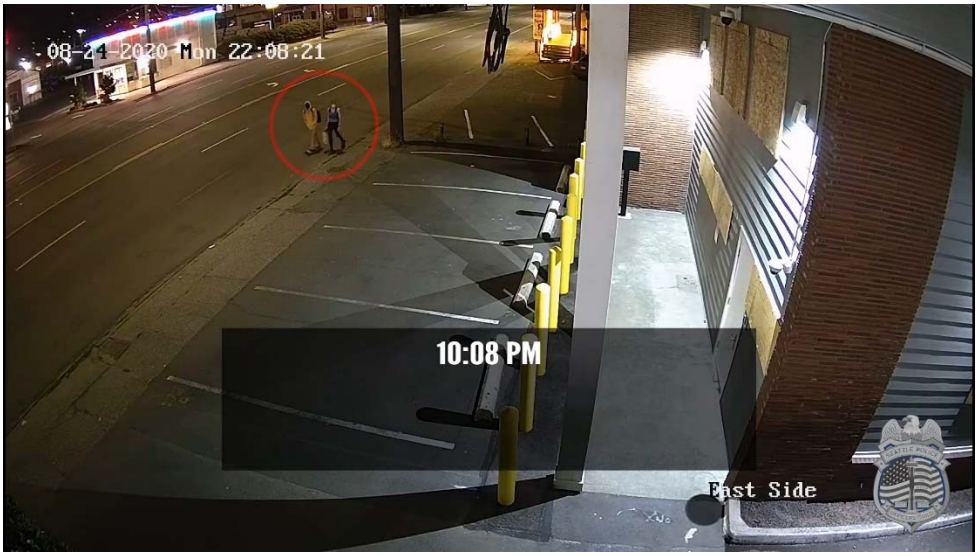
commonly known as a Molotov cocktail creates a destructive device."); *United States v. Wilson*, 546 F.2d 1175, 1177 (5th Cir.) (same); *United States v. Tankersley*, 492 F.2d 962, 966 (7th Cir.1974) (affirming conviction for possession of a "destructive device" which consisted of "a bottle, a firecracker and tape, and paint remover: the components of a Molotov cocktail")).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

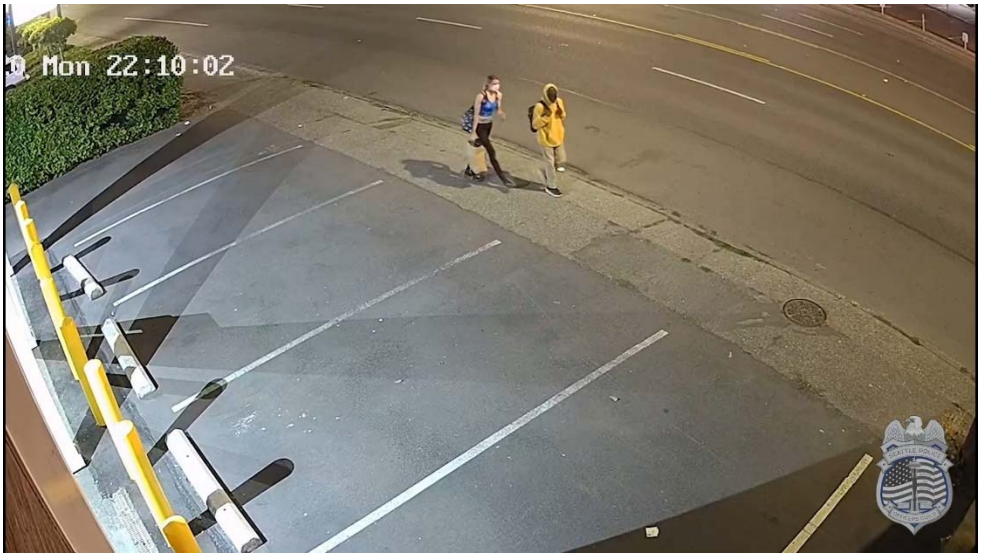
two of the incendiary devices but missed the building both times, with the devices landing adjacent to the building in its northern driveway and shattering on the asphalt.



The surveillance camera footage shows the two subjects walking in front of the building beginning at 10:08 p.m., approximately 52 minutes prior to the deployment of the incendiary devices. The subjects arrived from the south and walked northbound past the front of the building before doubling back and walking past the building again in a southbound direction of travel.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



Investigators collected additional surveillance footage from nearby businesses in an effort to determine the path that the two subjects travelled prior to the deployment of the incendiary devices. After reviewing all the collected footage, investigators were able to determine that between 10:07 p.m. and 11:04 p.m., the subjects walked on foot throughout the one square block area bordered by Third and Fourth Avenue South, between S. Forest Street and S. Hanford Street. During this time, only a few other individuals were in this area; these persons were transiting through the area by vehicle or bicycle. There were no demonstrations or protests occurring in this area during this time. The area is primarily a commercial and industrial neighborhood with no residential dwellings. Although Fourth Avenue is a major arterial, given the hour of the night, most of the nearby businesses were closed and the traffic on the street was minimal.

Based on the review of various surveillance video cameras, investigators determined that between 10:07 p.m. and 10:40 p.m., the two suspects made two full loops around the block containing the SPOG building – one in a clockwise direction and then one in a counter-clockwise direction. Between 10:44 p.m. and 10:57 p.m., the suspects walked back and forth twice between Third Avenue South and the rear of the SPOG building. This area contains no pedestrian walkways or sidewalks, and is primarily used for parking and as a loading area by an adjacent food processing facility. At 10:59 p.m., the suspects walked

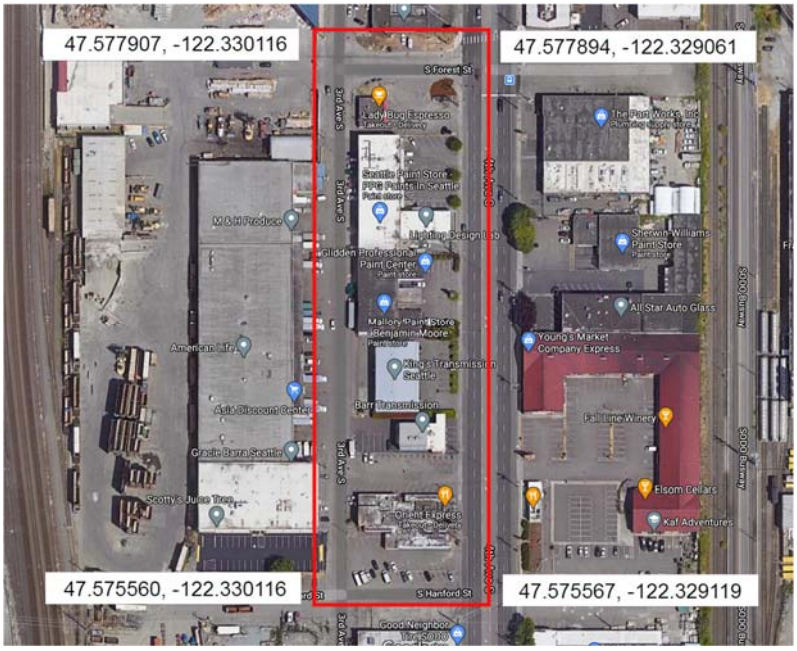
UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

back to the rear of the SPOG building and at 11:00 p.m. they detonated the incendiary devices at the rear of the building, as further described above. They immediately thereafter walked north along Third Avenue South and departed the area by 11:04 p.m.

The specific target location (depicted on the above map) for which we are seeking Google data is as follows:

> Geographical box with the following four Google Earth latitude and longitude coordinates near the address of 2949 4th Avenue S. #A, Seattle, WA 98134, for the time period of 10:00 p.m. to 11:15 p.m. PDT, on August 24 2020 (see below):
>
> (1) 47.577907, -122.330116
> (2) 47.577894, -122.329061
> (3) 47.575560, -122.330116
> (4) 47.575567, -122.329119

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



Based on my training and experience and knowledge of other investigations that I and other FBI agents have conducted, I know that it is common for individuals to carry electronic devices, including cellular telephones, and to use those devices and the services and applications they contain, including internet search engines, Global Positioning Systems (GPS) and mobile applications. I am further aware that individuals will use such electronic devices to plan, coordinate, communicate, implement, and document the commission of crimes, and that it is common for persons to use such devices and services to map and navigate prior to, and during, the commission of crimes. I am also aware that it is common for service providers to store detailed user history, including search and navigation history, in their databases that is otherwise not stored on the devices collecting the data.

Based on the foregoing, I submit that there is probable cause to search information that is currently in the possession of Google and that relates to the devices that reported being within the Target Location described in Attachment A during the time period described in Attachment A for evidence of the crimes under investigation. The information to be searched includes (1) identifiers of each device; (2) the location reported by each

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

device to Google and the associated timestamp; and (3) basic subscriber information for the Google account(s) associated with each device.

The proposed warrant sets forth a multi-step process whereby the government will obtain the information described above. Specifically, as described in Attachment B.I:

a. Using Location History data, Google will identify those devices that it calculated were or could have been (based on the associated margin of error for the estimated latitude/longitude point) within the Target Location described in Attachment A during the time period described in Attachment A. For each device, Google will provide a unique device ID assigned by Google and its location coordinates along with the associated timestamp(s), margin(s) of error for the coordinates (*i.e,.* "maps display radius"), and source(s) from which the location data was derived (*e.g.*, GPS, wi-fi, bluetooth), if available. Google will not, in this step, provide the Google account identifiers (*e.g.*, example@gmail.com) associated with the devices or basic subscriber information for those accounts to the government.

b. The government will identify to Google the devices appearing on the list produced in step 1 for which it seeks the Google account identifier and basic subscriber information. The government may, at its discretion, identify a subset of the devices.

c. Google will then disclose to the government the Google account identifier associated with the devices identified by the government, along with basic subscriber information for those accounts.

This process furthers efficiency and privacy by allowing for the possibility that the government, upon reviewing contextual information for all devices identified by Google, may be able to determine that one or more devices associated with a Google account (and the associated basic subscriber information) are likely to be of heightened evidentiary value and warrant further investigation before the records of other accounts in use in the area are disclosed to the government.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The proposed warrant would not authorize the disclosure or seizure of any tangible property or the content of any wire or electronic communication, as defined in 18 U.S.C. § 2510(8).

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CONCLUSION

Based on the forgoing, I request that the Court issue the proposed warrant, pursuant to pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c). I further request that the Court direct Google to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control.

Pursuant to 18 U.S.C. § 2703(g), the government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records and data, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

I declare under penalty of perjury that the statements above are true and correct to the best of my knowledge and belief.

DATED this 7th day of October, 2020.

MICHAEL STULTS
Special Agent, FBI

The above-named agent provided a sworn statement to the truth of the foregoing affidavit by telephone on 7th day of October 2020

BRIAN A. TSHUCHIDA
Chief United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970