Samuelson Law, Technology & Public Policy Clinic

July 2024

Federal Use of Digital Evidence in Investigations of Alleged Criminal Activity During Protests After George Floyd's Murder in Minneapolis–Saint Paul

A Samuelson Clinic Student White Paper

Margerite Blase '22
Gary Lee '23

Former Samuelson Clinic Students

Berkeley Law

SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC
UC Berkeley School of Law
353 Law Building
Berkeley, CA 94720
Phone 510-643-4800
www.law.berkeley.edu/SamuelsonClinic/

This publication is available online at https://www.law.berkeley.edu/case-project/george-floyd-warrants-white-paper/

Acknowledgments

We are grateful for the supervision of Professor Catherine Crump as we conducted our research and drafted this report. We are also grateful to former Samuelson Clinic supervising attorneys Megan Graham and Brianna Schofield and former Samuelson Clinic teaching fellow Gabrielle Daley for their suggestions and support.

We would also like to thank the Reporters Committee for Freedom of the Press for their efforts to secure the public's access to court records, including records reviewed in connection with this white paper, and to participants in the Samuelson Clinic and Advanced Samuelson Clinic seminars who workshopped drafts of this white paper.

Executive Summary

This white paper examines federal law enforcement agencies' use of digital evidence to investigate suspected criminal activity that took place during protests in Minneapolis–Saint Paul, Minnesota (the "**Twin Cities**") after George Floyd was murdered by Minneapolis police officers on May 25, 2020.

We reviewed hundreds of pages of unsealed federal warrant materials in the United States District Court for the District of Minnesota that were filed in the weeks following Mr. Floyd's death. These materials were filed by various federal law enforcement agencies. The warrants permitted searches and seizures of a range of physical and digital items.

Our goal in analyzing these materials is to better understand how federal law enforcement used digital evidence—i.e., information stored in digital form—in their investigations.[*] We hope that this white paper will assist journalists, policymakers, and the public in understanding the scope of existing surveillance technologies available to law enforcement at mass disturbances and the subsequent use of the data obtained from these sources. Given that the same types of surveillance technologies are available nationwide, it is likely that digital evidence will play a similarly central role when law enforcement investigates potential criminal conduct at future mass events.

We examined these records for two key reasons:

- ***First***, the public and other stakeholders are still learning how law enforcement agencies use digital evidence to further their investigations. The warrant materials we gathered offer vivid, concrete examples of how law enforcement use digital evidence, including the evidence that is generated by cell phones and social media posts. By examining the Minnesota records closely, we hope to inform a broader understanding of how digital evidence will be used in investigations.
- ***Second***, the information we learned sheds light on how digital evidence is likely to be used in investigating criminal activities during other mass disturbances. For example, as others have detailed, law enforcement also made extensive use of digital evidence during investigations of the January 6, 2021 insurrection and storming of the Capitol in Washington, D.C.

[*] Common examples of digital evidence include video footage from surveillance cameras or that is recorded on people's phones, and social media, cellphone, and vehicle records.

We found that most of the tools used by law enforcement are publicly known, but we learned more about *how* various forms of digital evidence are being used in investigations. The key takeaways from our research are:

- Warrant materials have an important role to play in explaining to the public what law enforcement and courts are doing;
- Digital evidence is commonly sought during investigations, and it is also regularly used to justify conducting other searches or seizures as investigations unfold;
- Warrant materials commonly offer descriptions of how agents weave together multiple types of digital evidence to advance their investigations; and
- This kind of analysis was made possible by the comparatively robust access available in the District of Minnesota—the same may not be possible in many state courts or other federal districts because courts' policies and procedures keep this information shielded from public view.

The white paper proceeds as follows. We first provide a brief overview of the murder of George Floyd and subsequent protests that took place in the Twin Cities during May and June 2020. Then we describe our methodology for identifying and reviewing warrants issued in connection with suspected criminal activity at the protests, and provide an overview of what we found. Finally, we discuss four categories of digital evidence law enforcement drew on: (1) surveillance camera footage, (2) social media information, (3) cell phone data, and (4) vehicle data. For each, we examine the specific types of information law enforcement agents obtained and the uses they made of them, illustrated with examples from the warrants.

Table of Contents

Murder of George Floyd and Subsequent Protests

On May 25, 2020, George Floyd was murdered by Minneapolis Police Department Officer Derek Chauvin.[1]

Police officers were responding to a call from a store clerk claiming that Mr. Floyd had attempted to make a purchase with a counterfeit bill.[2] A bystander's video showed that three officers pinned Mr. Floyd to the ground and a fourth officer kept other bystanders away.[3] Officer Chauvin kneeled with his knee on Mr. Floyd's neck for nine and a half minutes.[4] The video captured Mr. Floyd's pleas of breathing difficulties, fear of death, and cries of pain.[5] After six minutes, Mr. Floyd appeared unconscious and bystanders confronted officers about Mr. Floyd's condition, observing that Mr. Floyd was unresponsive.[6] Shortly after that, paramedics arrived and loaded Mr. Floyd into an ambulance.[7] Mr. Floyd was pronounced dead later that night.[8]

By May 26, 2020, local and national news outlets covered Mr. Floyd's death and people across the nation began to protest.[9] Several of the protests in the Twin Cities turned violent with vandalism and destruction including arson, looting, and smashing doors and windows.[10] For example, on May 27, individuals vandalized, looted, and set on fire a Target store and a Cub Foods store near the site where Mr. Floyd died.[11] And on May 28, individuals broke into and set fire to the Minneapolis Third Precinct police building.[12]

In response to the violence, the mayors of Minneapolis and St. Paul imposed curfews on May 29 and May 30, and Minnesota Governor Tim Walz also issued an executive order implementing the curfew in both cities.[13] Despite the curfew, individuals continued to protest and to vandalize, loot, and start fires in the Twin Cities.[14] More than 1,500 locations throughout the greater Twin Cities area were vandalized, looted, or damaged in the days following the murder of Mr. Floyd.[15]

Methodology and Overview of the Warrants We Reviewed

To learn more about the role of digital evidence in federal investigations of the alleged criminal activity and the protests more broadly, we reviewed more than 100 warrant applications filed in the federal District of Minnesota and examined how the court handled them. These warrant applications were filed between May 26, 2020 and September 14, 2020. When a warrant application is filed, a new case is opened[†] and all of the related documents (e.g., the warrant

[†] In the District of Minnesota, warrants are filed as "magistrate judge" cases with "Search Warrant" in the case name. Thus, when you look for search warrant cases in the court's records system, you can enter "Search Warrant" as a party name.

application, the supporting affidavit, the warrant, any motions and orders to seal, etc.) are filed in that case. Our analysis included a manual review of all the dockets, warrant applications, and related filings for this timeframe that were unsealed and publicly available in mid-November 2021.

In the District of Minnesota, if the Government wishes for a warrant application and the related filings to be sealed and kept from public view, it must file a motion to seal stating case-specific reasons justifying the sealing. In nearly all cases, an initial sealing order will last for up to 180 days. After that, most warrant applications and related materials are available to the public at one the Clerk's Offices in the District. Less frequently, the Government may seek to prolong the sealing by filing an additional motion demonstrating that continued sealing is necessary. Our review showed that virtually all warrants obtained in the months following the protests are now unsealed, but it is possible that more records have been made available to the public since our initial review.

After our initial review of the unsealed warrant materials, we conducted a deeper analysis of sixty-nine specific cases.‡ We did a deeper dive on the warrant materials in these cases because they focused on the protests that followed Mr. Floyd's murder and they either described digital evidence law enforcement had already obtained or they sought additional digital evidence.

There are some limitations to our methodology. First, there may be other warrant applications that are relevant to our analysis that were filed after September 14, 2020, or that were still sealed in November 2021. Second, we know that the federal court in Minnesota generally only unseals warrant applications, not other government requests for electronic surveillance (e.g., under the Pen Register Act[16]).[17] Materials sought under these statutes were not reviewed. And third, unless the evidence is discussed in the warrant applications, our dataset does not capture law enforcement access to digital evidence that does not require court involvement (e.g., video surveillance voluntarily turned over by private citizens or information that already exists in governmental databases).

Additionally, the case numbers for warrant cases will all include "mj" as a differentiator (e.g., 0:20-mj-475-DTS, which is discussed below).

‡ Most of these cases included only a single warrant, warrant application, and supporting materials. However, some involved more than one application (e.g., a renewal of the original request), motions to extend the time to execute the warrant, or similar filings.

We reviewed warrant applications that were related to more than a dozen different incidents of alleged criminal activity during the protests in the Twin Cities. Below, we discuss specific warrants related to the following events[§]:

- A fire at the Third Precinct, including at least a geofence warrant[18] [discussed here], two warrants for various types of cellphone location information for Suspect A[19] [discussed here], a warrant for various types of cellphone location information for Suspect B[20] [discussed here], the search of Suspect C's girlfriend's apartment[21] [discussed here and here], and a physical search of Suspect D's home and person [discussed here and here][22];
- Alleged vandalism at several post offices:
    - Lake Street Post Office, including both a Snapchat[23] [discussed here and here] and a geofence warrant[24] [discussed here];
    - Minnehaha Post Office, including a geofence warrant[25] [discussed here]; and
    - Powderhorn Post Office, including a geofence warrant[26] [discussed here];
- A fire at a Great Health and Nutrition store in St. Paul on May 28, including a warrant to search a phone[27] [discussed here, here, and here];
- A fire at the Minnesota Transitions Charter School ("**MTCS**") May 27, including a warrant to search a phone[28] [discussed here, here, and here];
- A fire at a Cub Foods in Minneapolis on May 28, including for various types of cellphone location information[29] [discussed here, here, and here];
- Apparently related alleged arsons at several stores in Minneapolis on May 29, including warrants for the suspect's Facebook account[30] [discussed here, here, and here], the suspect's brother's Facebook account[31] [discussed here, here, and here], and the suspect's brother's friend's Facebook account[32] [discussed here, here, and here];
- A fire at a Max It Pawn store in Minneapolis on May 28, which included warrants to search at least two cellphones[33] [discussed here] and to conduct cell site location searches for at least two phones[34] [discussed here, here, and here];

---

§ The materials discussed in this white paper are public records available in the Clerk's Office for the District of Minnesota. Where we have redacted certain personally identifying information for purposes of this white paper, our redactions are shown with brackets around a description of what has been redacted (e.g., "[Cell Phone Number]").

- A fire at Gordon Parks High School in St. Paul on May 28, including for various types of cellphone location information[35] [discussed here and here];
- A fire at a Walgreens in Minneapolis on May 30, including a geofence warrant[36] [discussed here] and a warrant for information about a cellphone account holder[37] [discussed here];
- A fire at an Enterprise Rent-A-Car in St. Paul on May 28, including a warrant to search a vehicle[38] [discussed here]; and
- An alleged conspiracy to illegally traffic explosives by members of the Boogaloo Bois, including at least three location tracking warrants for vehicles[39] [discussed here].

What We Found

In what follows, we describe our findings, starting with a high-level description of the elements of the warrant cases that we reviewed. Then, we identify four non-exhaustive categories of digital evidence that law enforcement agents used when investigating criminal activity: (1) surveillance camera footage, (2) data from social media platforms, (3) data related to cellphones, and (4) data related to vehicles. For each, we discuss what we learned about the specific types of data law enforcement obtained and what uses they made of that data. We use examples from the materials we reviewed to illustrate how the digital evidence at issue supported the government's investigations.

However, as an initial observation, we note that even though our analysis focuses on digital evidence in these four buckets, law enforcement agencies use all of these categories—and many others that are beyond the scope of our review because they were not apparent in our dataset—holistically to further their investigations.

A. Warrant Process

In each warrant case that we reviewed, we started with the docket sheet. The docket sheet contains a short description of each filing related to that particular case. In the District of Minnesota, docket sheets are now generally publicly available from the time the applications are filed.

Each case generally consisted of several filings. They all had an application for a search warrant, an affidavit supporting the request, and the signed warrant. The applications and warrants also generally had related attachments describing the person, place, or item to be searched or seized, as well as what specific information or evidence could be gathered. The affidavits were sworn to by a federal law enforcement officer and described the alleged crime, the status of the

investigation, and the factual basis for finding that probable cause existed to believe that the search would reveal evidence of a crime. In some instances, magistrate judges appended an addendum that spelled out limits on the searches.[40]

Many cases also had motions to seal the warrant application and separate orders sealing the materials, generally for no more than 180 days. In some cases, there were additional motions to extend the sealing or requests to extend the amount of time to conduct the search. And in some instances, law enforcement filed separate returns that detailed what was obtained during the search.

The District of Minnesota's relatively transparent docketing practices for warrant applications made it possible for us to review the sixty-nine warrants described above.

B. Surveillance Camera Footage

Footage from surveillance cameras was mentioned in many of the warrant applications we reviewed. The footage discussed in the affidavits was obtained from both the location where the alleged criminal activity occurred and nearby premises. We saw this type of footage used in three ways: (1) it was used as evidence in and of itself; (2) it was used to identify suspects and tie them to the alleged criminal activity under investigation; and (3) it was used as a key basis—if not the only basis—for establishing probable cause to seek additional forms of digital evidence.

1. Law Enforcement Uses Surveillance Camera Footage as Evidence

Law enforcement's use of surveillance camera footage as evidence can be seen in the example of an arson at a Great Health and Nutrition store in St. Paul on May 28, 2020.[41] As described in an affidavit accompanying a warrant application, on the evening of May 28, the owner of the Great Health and Nutrition store ("**JR**") received a call that people were inside his store, despite it being closed for the night.[42] JR had set up a remote Wi-Fi based surveillance system, iSmartViewPro, that allowed him to monitor audio and video inside the store without being on the premises.[43] While the system did not store historical footage, JR was able to record the events of May 28 that he was monitoring live.[44] JR told law enforcement that, through his iSmartViewPro, he observed individuals taking inventory, damaging property, and setting a fire.[45] JR later provided the video surveillance footage to the Bureau of Alcohol, Tobacco, Firearms and Explosives ("**ATF**").[46]

The warrant application also includes other details that assert criminality on the part of particular suspects.[47] For example, the affidavit describes in detail the

actions taken by people who were eventually charged, including statements that they spread liquid from clear bottles around the store and that they lit paper on fire before holding it to the liquid.[48]

2. Law Enforcement Uses Surveillance Camera Footage to Identify Suspects

In the same Great Health and Nutrition warrant application, ATF indicated that it had reviewed the surveillance camera footage to help identify suspects. For example, it described one person in the recording as a "white male wearing a green and black hoodie, dark colored pants and black tennis shoes . . . . He has dark brown hair, the top of which is pulled into a band."[49] ATF issued a press release describing the people they were looking for and provided local media with surveillance images with a "request for any tips or identifying information from the general public."[50] Once the images were provided to the public, ATF received multiple anonymous tips from the public identifying the suspect.[51]

In another example, law enforcement relied on surveillance camera footage to identify suspects in an arson at the Minnesota Transitions Charter School ("**MTCS**") that took place on May 27.[52] According to the warrant affidavit, law enforcement acquired copies of surveillance footage from inside the MTCS facility "through communications with administrative staff at MTCS."[53] The footage captured images of people at the scene, including a female with a large tattoo in the center of her back.[54] Subsequently obtained surveillance camera footage from a Dominoes showed a woman with the same tattoo, and also an image of her face.[55] ATF issued a press release asking for help identifying the suspect, and agents received an online tip identifying her.[56] Agents then corroborated the suspect's name by looking at her Facebook page, which had pictures of the same tattoo.[57]

3. Law Enforcement Uses Surveillance Camera Footage to Support Probable Cause for Subsequent Searches

Law enforcement also will use surveillance camera footage to justify other searches, as shown in both the Great Health and Nutrition and MTCS examples. The warrants we refer to above contained detailed descriptions of surveillance camera footage.[58] However, both warrant applications sought permission to search other sources, specifically the suspects' cellphones.[59] In each, law enforcement relied on descriptions of the surveillance camera footage to establish probable cause to conduct the subsequent searches.

4. Conclusions About Surveillance Camera Footage

In summary, the warrants that we reviewed showcase how powerful a tool surveillance videos can be for law enforcement as evidence of a person's allegedly

unlawful acts, to identify suspects, and to support articulations of probable cause to conduct subsequent searches.

C. Data from Social Media Companies

From our review of the Minnesota warrants, law enforcement also regularly relies on social media to further its investigations. Law enforcement uses social media in a variety of ways, including to identify suspects, gather evidence of criminal activity, and collect evidence to support warrants for additional types of digital evidence. We review each of these categories in turn.

1. Law Enforcement Uses Social Media to Identify Suspects

In many warrants that we reviewed, law enforcement used social media to obtain the name of or other information about people suspected of criminal activity. One such example occurred in an investigation of a fire at the Minneapolis Police Department's Third Precinct building.[60]

On the night of May 28, the Minneapolis Police Department's Third Precinct building was overrun and set on fire.[61] To assist in finding suspects, law enforcement collected and reviewed surveillance video from an external camera at the Third Precinct.[62] In the footage, an unidentified suspect had jumped over a fence, entered the building through a broken window, and assisted another individual in lighting a Molotov cocktail.[63]

On June 12, ATF received a tip through their electronic tip tracking system that showed five screen captures of that unidentified suspect—we have called this person "Suspect C" above and below.[64] Those screen captures were from an Instagram account of a woman who was not involved in the incident.[65] Law enforcement corroborated the tattoos and clothing of the suspect from the screen captures with the tattoos and clothing that Suspect C wore in surveillance video of the Third Precinct incident.[66] Because the woman's Instagram account was connected to her Facebook account,[67] law enforcement was able to review her Facebook profile. Her Facebook profile stated that she was in a romantic relationship with Suspect C[68] and disclosed Suspect C's name and Facebook profile.[69]

In other warrants that we reviewed, law enforcement described reviewing social media accounts during investigations to learn about additional suspects involved in incidents.[70] For example, Mr. Rupert, a suspect in the arson of several stores in Minneapolis on May 29 and who pleaded guilty, posted a live video to his Facebook account that depicted him and other suspects looting and setting fire to the stores.[71] The live video depicted Mr. Rupert passing out explosives,

encouraging others to throw explosives at law enforcement officers, damaging property, appearing to light a building on fire, and looting businesses.[72]

In addition to finding evidence about Mr. Rupert himself, Mr. Rupert's video showed two other suspects (later identified as his brother and a friend) who participated in the looting and arson.[73] Law enforcement subsequently sought warrants to search both his brother's and his friend's Facebook accounts.[74] According to one warrant affidavit, Mr. Rupert's brother is seen throughout the video participating in civil unrest.[75] The video captures his brother throwing a surveillance camera off the roof of McDonald's restaurant.[76] Another warrant affidavit indicates that Mr. Rupert's friend is also seen throughout the videos and that the friend commented on a post that Mr. Rupert made on May 28, in which the two were coordinating plans to travel to Minneapolis on May 29.[77]

2. Law Enforcement Uses Social Media to Gather Evidence of Suspected Criminal Activity

Law enforcement also used social media to gather evidence of criminal activity.[78] In arsons of several stores in Minneapolis discussed above, law enforcement gathered live stream evidence of Mr. Rupert allegedly passing out explosives, damaging property, lighting a building on fire, and looting businesses.[79] One affidavit says that in the video, Mr. Rupert's brother is seen throwing a surveillance camera off the roof of a McDonald's restaurant while the Rupert brothers' friend is nearby.[80]

Sometimes evidence of criminal acts on one person's Facebook account leads law enforcement to evidence of criminal acts on a second person's account. In the example involving fires at several stores in Minneapolis, law enforcement reviewed the three Facebook accounts and discovered many pieces of evidence. On the evening of May 28, Mr. Rupert posted that, "I'm going to Minneapolis tomorrow who coming only goons I'm renting hotel rooms."[81]. In reply to an earlier post from that night, his friend responded " . . . we out their tm or what?"[82] This exchange seemingly led law enforcement to examine the friend's Facebook page in more depth.[83] Law enforcement found that the friend had also posted live stream videos in Minneapolis from May 29 to May 30.[84] The affidavit says that videos depict Mr. Rupert's brother throwing a rock at the windows of a bus stop and breaking the window.[85] In another video, the friend texts his Facebook account "Rioting."[86] And yet another video shows Mr. Rupert and others throwing rocks at the windows of a White Castle restaurant.[87] In addition, shortly after Mr. Rupert was arrested on June 1, law enforcement observed that his brother had posted about explosives on the friend's account on June 3, stating "[Mr. Rupert] had fireworks that we bought from Missouri n [sic] everybody there was already throwing fireworks."[88]

In a separate example, in the warrant application for information from Suspect C's girlfriend's apartment, law enforcement detailed that law enforcement had reviewed the publicly available portions of the suspect's Facebook profile.[89] The affidavit noted that his Facebook profile cover photo was updated June 17, 2020, and showed him holding the Minneapolis Police Department seal above his head in front of a burning background.[90]

3. Law Enforcement Obtains Evidence from Social Media to Support Probable Cause for Additional Warrants

Sometimes law enforcement agents use evidence gathered from social media accounts as part of the basis for establishing probable cause to support additional warrant applications. In the example where several stores were burned that is discussed above, law enforcement used video evidence gathered from Mr. Rupert's social media account to support warrant applications requesting additional information from the Facebook accounts of his brother and his friend.[91]

Also, in the warrant to Facebook for information related to Mr. Rupert's account, law enforcement provided a detailed summary of the two-hour live video posted by Mr. Rupert on his Facebook account,[92] to establish probable cause to gather more information from Facebook related to the account.[93] Facebook was ordered to disclose eighteen categories of information, including account holder details, information about when the account was created and by whom, activity logs from May 25, 2020 until the warrant was executed, all profile information, photos, videos, and the contents of communications, among others.[94]

4. Conclusions About Social Media Evidence

The warrants involving social media paint a picture of how social media fits into the investigatory tools of law enforcement. Social media evidence was used in a variety of ways, such as to identify suspects, uncover alleged co-conspirators, gather evidence of criminal activity, and as probable cause to support additional warrants. The tools and features that social media companies have created to enhance socializing also serve as precise digital footprints of their users' activities.

D. Data Related to Cellphones

Another common step in law enforcement investigations is the collection of data from or pertaining to cellphones. Law enforcement uses this evidence in a variety of ways, which we describe below through examples from the warrants we reviewed. Specifically, we discuss how law enforcement: (1) uses data from mobile phone carriers to identify and locate specific suspects; (2) uses cellphone location data to identify multiple people at once; (3) uses devices known as cell

site simulators ("**CSS**") to locate cellphones; and (4) uses data that is stored on cellphones as evidence of alleged criminal activity.

1. Law Enforcement Uses Information from Mobile Carriers to Identify and Locate Specific Suspects

Law enforcement sometimes seeks a warrant to obtain data pertaining to the cellphone of a suspect. Law enforcement can seek both historical records—including location data and account holder information—and authorization to obtain data about future phone usage.[95]

a. Historical Records

In the warrants we reviewed, law enforcement sometimes sought to obtain historical data associated with a particular cellphone.[96]

For example, while investigating the May 28 fire at a Cub Foods in Minneapolis, law enforcement sought a warrant for historical records from a suspect's phone.[97]

After learning the suspect's phone number through a database, law enforcement secured a warrant for "historical records" held by the phone carrier that were associated with the number from May 25 through August 6, 2020.[98] The records sought included:

- Subscriber and billing information (e.g., name and address);
- Device identification information (e.g., make and model of the device);
- Records of voice, SMS, and data sessions, including dates, times, duration, cellular towers, and sectors used for each communication; and
- Internet activity reports.[99]

Because the records started on May 25 and the fire occurred on May 28, law enforcement explained that the data could "reveal [suspect's] location and contact with accomplices or witnesses in relation to the" crime.[100] Additionally, because the data would span multiple days, it could "enable the FBI to identify patterns of life for [suspect]" and "general areas where the individual frequents and their frequent contacts, both of which" would assist in locating the suspect.[101]

b. Prospective Data

Law enforcement can also obtain a warrant for real-time location data associated with a suspect during an investigation, also known as prospective cellphone location data. This can include non-content information similar to that which law

enforcement obtains on a historic basis.[102] It can also include collection of GPS and other location data, as well as information generated by the nationwide Enhanced 911 system.[103] The warrant in the Cub Foods investigation, sought this sort of prospective information for thirty days following the issuance of the warrant.[104]

2. Law Enforcement Uses Cellphone Location Data to Identify Multiple People at Once

We also found five examples of law enforcement agencies seeking "geofence warrants" that would allow them to identify all phones in a particular location at a particular time.[105]

In the days following George Floyd's murder, several post offices were vandalized, burglarized, and set on fire.[106] On May 29, for example, the Powderhorn Station Post Office in Minneapolis was burglarized twice.[107] According to a warrant affidavit, law enforcement obtained video surveillance that showed three individuals breaking through a window around 3:21 a.m. to gain access to the customer lobby and using their cellphones as flashlights as they searched through the premises.[108] After this incident, the station was closed for the day and was boarded up with plywood.[109] Around 11:37 p.m. that night, three individuals removed the plywood in the main entrance and entered through a broken window.[110] Video surveillance showed the individuals departing the customer lobby at 11:53 p.m.[111]

On June 4, law enforcement sought and obtained a geofence warrant for information held by Google to try to identify and locate the three people who were suspected of being involved in both break-ins.[112] The warrant sought information relating to GPS, WiFi, or Bluetooth location history data from devices at or around the latitudinal and longitudinal coordinates of the Powderhorn Post Office, as well as the identifying Google account information associated with the responsive data.[113]

3. Law Enforcement Uses Cell Site Simulators to Locate Suspects and Their Cellphones

In addition to the methods described above, law enforcement can obtain warrants to use CSS devices to locate a suspect's cellphone. A CSS is an electronic surveillance device that collects location data by imitating a cell tower, thereby causing nearby cellphones to connect to it.[114] Once the cellphone connects to the CSS, the CSS can determine a cellphone's location. In the examples we reviewed, law enforcement generally indicated that they were looking for a particular phone and they would delete the non-responsive data that is necessarily collected based on how a CSS works.[115]

In one example, as part of the investigation into the May 28 fire at Gordon Parks High School in St. Paul, ATF secured a warrant to, among other things, use "a CSS to precisely determine the location of" the suspect's cellphone.[116] The warrant affidavit stated that the CSS "may send a signal to the Target Mobile Phone and thereby prompt it to send signals that include the unique identifiers of the device."[117] Law enforcement can then monitor the signals sent by the phone and use the information to determine the phone's location, "even if it is located inside a home, apartment, or other building."[118]

In the warrants authoring the use of a CSS to locate a suspect, it appears that law enforcement intended to use the device in conjunction with prospective location data from the cellphone provider.[119] However, in some instances, the warrant specified that law enforcement would primarily rely on location information from the provider and use a CSS device only if necessary.[120] For example, in the investigation of a fire at a Max It Pawn store in Minneapolis on May 28, one warrant application stated that if ATF was able to locate the suspect's phone "without the use of a CSS, the device will not be utilized. Put another way, the ATF will use the least intrusive means necessary to locate the Target Mobile Phone and will employ a CSS only if other investigative techniques are not successful."[121]

While the warrants we reviewed suggested that law enforcement generally uses a CSS only when other methods have failed, we did find an example of law enforcement using a CSS. During the investigation of the fire at the Minneapolis Police Department's Third Precinct building, law enforcement sought a warrant to search the main suspect's home.[122] In the affidavit accompanying that application, law enforcement indicated they had previously obtained a warrant to use a CSS and had used the device to establish that the main suspect was at the home they were seeking to search.[123]

4. Law Enforcement Uses Data from Cellphones as Evidence of Criminal Activity

Based on our review, law enforcement also regularly obtains warrants to search the contents of a suspect's cellphone. In some cases, law enforcement already has possession of a phone they would like to search. In others, agents seek a warrant to search a phone they hope to acquire in the future, such as when they search a suspect's home or person and anticipate finding a cellphone there.[124] The warrants we reviewed indicated that physical cellphone searches generally seek access to records and communication stored on the cellphone.[125]

For example, during the investigation into the fire at the Max It Pawn store discussed above, law enforcement requested "all records" on two suspect's devices, including:

- Video recordings;

- Photographs;
- Records of internet activity; and
- Text messages.[126]

One of the suspects that had been identified through social media had provided his personal phone number during a traffic stop on May 24, four days prior to the Max It Pawn arson.[127] The warrant for a second suspect, who had been identified through surveillance images, stated that the "Rochester Minnesota Police Department advised [that the second suspect] provided as a personal cellphone contact the number of the Device on May 26, 2020, and on June 5, 2020."[128] Both warrants granted law enforcement access to the cellphones with the phone numbers the suspects had provided.[129] Both warrants also noted that the devices were believed to be in the possession of the suspects.[130]

5. Conclusions About Data Related to Cellphones

The warrants showcase how valuable cellphone data can be to law enforcement during an investigation. Even if law enforcement does not have access to a suspect's cellphone, they can obtain a variety of information about a suspect through their mobile carrier. Or, alternatively, if law enforcement does not know the identity of a specific suspect but does know the location and time of a criminal act, it can seek information regarding all cellphones in the vicinity. And law enforcement can use a CSS to locate and track a particular phone by forcing all nearby phones to connect to the device. Moreover, if law enforcement obtains a suspect's cellphone, they can secure a warrant to search the contents of the phone, which can include videos, photographs, internet use, forensic data, and more.

E. Data Related to Vehicles

Law enforcement also has a variety of tools at their disposal to learn more about suspects by examining vehicle-related information. This includes reviewing government-held data, such as looking up a suspect's driver's license and vehicle registration information. Law enforcement can also track vehicles' locations; in the warrants we reviewed, we saw examples of attaching GPS trackers to cars,[131] and utilizing automatic license plate reader ("**ALPR**") data[132]. Below, we first discuss the use of driver's license and vehicle registration databases, and then move onto vehicle tracking tools.

1. Law Enforcement Uses Vehicle Registration and Driver's License Information to Identify Suspects

Law enforcement uses a variety of databases pertaining to vehicles to help identify suspects.[133] In the warrants we reviewed, law enforcement looked up (1) vehicle registrations and (2) driver's license information.[134]

One investigation we reviewed illustrates how law enforcement can make use of both vehicle registration and driver's license information to advance its investigations. During the investigation of the fire at Great Health and Nutrition, after identifying the main suspect, law enforcement was still trying to identify additional suspects.

Based on information collected during the investigation, law enforcement obtained a warrant to search and seize certain evidence from the main suspect's residence.[135] Once agents arrived at the residence to execute a search warrant, they "observed an unoccupied vehicle parked across the street" from the suspect's house.[136] ATF personnel searched a Minnesota Department of Vehicle Services ("**DVS**") database for the vehicle's information, which showed that the car was registered to a particular woman.[137]

Law enforcement then compared DVS photographs of the car owner to images from the Great Health and Nutrition arson video and found that the owner closely resembled one of the women in the footage.[138] Specifically, the warrant affidavit notes that the owner is "wearing around her neck a dark-colored choker" and appeared to have "predominately blond hair on the ends, but with dark-colored hair at the base of her scalp" in her DVS photo, and the woman in the surveillance footage "also [wore] a dark-colored neck 'choker' and had predominately blond hair on the ends, but with dark-colored hair at the base of her scalp."[139]

While ATF was still conducting the search of the home, a group of people arrived, including the car owner.[140] During an interview with agents, the car owner confirmed that she was at the Great Health and Nutrition store and was arrested.[141]

2. Law Enforcement Uses Vehicle Tracking Tools to Identify Suspects' Locations

In addition to the databases described above, law enforcement also has tools to help them locate vehicles and, by proxy, their drivers. The warrants we received discuss two such tools: GPS tracking devices and ALPR data.

a. GPS Tracking Devices

Law enforcement obtained multiple warrants to track vehicles while investigating an organization called the "Boogaloo Bois" for an alleged conspiracy to commit explosives-related crimes.[142] According to the warrant affidavits, alleged members of the Boogaloo Bois were initially subjects of interest because they were discussing the commission of violent crimes and maintaining a "heavily armed presence on the streets of Minneapolis during the civil unrest following the murder of George Floyd."[143]

The FBI learned the identity of the two main suspects in the case through information they received from people they described as a "witness" and a "confidential human source."[144] During their investigation, law enforcement acquired myriad evidence against the suspects, including recordings and social media messages about their desire to commit acts of violence and obtain weapons.[145] Law enforcement also identified three vehicles registered to or used by the suspects.[146]

Based on evidence collected during the investigation, law enforcement obtained warrants authorizing the installation and monitoring of a tracking device on the three vehicles associated with the suspects for forty-five days.[147] Although law enforcement already knew the suspects' identities and general locations, officers continued to monitor the suspects and to "identify locations, subjects, and other targets."[148]

b. Automated License Plate Readers

Law enforcement can also use ALPR data to locate a vehicle or suspect, as was done in one of the warrants we reviewed.[149]

On May 29, the Lake Street Post Office was looted, burglarized, and set on fire.[150] Video surveillance from the cameras at the post office showed individuals attempting to break into the post office at 10:07 p.m.[151] According to a warrant affidavit, at approximately 10:11 p.m., someone succeeded in entering through a broken window.[152] After that, numerous individuals are seen entering and exiting the post office, some of whom took mail and parcels when they left.[153] The office was ultimately destroyed by fire, including all the mail that had not been taken.[154]

While reviewing the video footage from the post office, U.S. Postal Inspectors saw a vehicle parked in the back parking lot of the Post Office and were able to see the license plate number and the presence of two occupants.[155] Law enforcement contacted the registered owner and found that the owner had sold the vehicle in 2019.[156] After concluding that neither suspect was the registered owner of the vehicle, law enforcement agents then used ALPR data to uncover an address of

the where the license plate was observed.[157] On July 9, 2020, law enforcement physically observed the vehicle at a home, and spoke with a resident to identify the owner of the vehicle.[158]

3. Conclusions About Vehicle Surveillance

Access to vehicle information can be an important tool for law enforcement, both as a means of identifying suspects and acquiring more evidence on known suspects. If law enforcement agents know a suspect's name or the license plate number of their vehicle, the agents can utilize driver's license and vehicle registration databases to add to their store of knowledge. In addition, law enforcement can track suspects in real time using GPS tracking devices or use ALPR to locate suspects' previous locations.

Conclusion

The warrant materials we reviewed provide examples of how law enforcement agencies use digital evidence to advance their investigations into mass disturbances. The materials show that surveillance cameras, social media data, cellphone data, and vehicle data are prominent types of data that law enforcement agents gather through their investigations.

The protests and civil unrest that followed the murder of George Floyd in Minneapolis–Saint Paul were extensively documented by participants and bystanders, and the resulting digital evidence appears to have played a major role in law enforcement investigations. Today, smartphones allow every person to be their own videographer and to distribute their footage through online social media platforms. And this is just the tip of the iceberg because so many other types of digital evidence are available for law enforcement's review without a warrant.

Finally, this white paper highlights the value of docket transparency in the judicial system. Because of the Minnesota federal court's practice of unsealing warrants when there is no longer an investigative need for secrecy, we were able to access these warrants and gain a more granular understanding of how digital evidence was used in these cases. Given the power of these techniques, it is important that the public understand how the digital footprints we all leave behind may be used in investigations.

Endnotes

[1] Jon Collins, Riham Feshir, Brandt Williams & Matt Sepic, *Chauvin Guilty of Murder, Manslaughter in George Floyd's Killing*, Minn. Pub. Radio (Apr. 20, 2021, 7:04 AM), https://perma.cc/VQS2-FYVA.

[2] *Id*.

[3] *See* Kim Hyatt, *Ex-Minneapolis Cop Tou Thao Sentenced to Nearly 5 Years for Aiding George Floyd's Killing*, Star-Trib. (Aug. 7, 2023), https://perma.cc/V9G6-NPAA.

[4] Collins et al., *supra* note 1.

[5] Cathy Wurzer, Aleesa Kuznetsov & Matt Sepic, *Final Ex-Cop Sentenced in Floyd's Murder, Closing a Chapter in the Case*, Minn. Pub. Radio (Aug. 7, 2023, 12:55 PM), https://perma.cc/7AZQ-UJCU.

[6] *Video Shows Initial Arrest of George Floyd, Who Later Died in Police Custody*, Star-Trib. (May 27, 2020), https://perma.cc/A2YE-QBUV.

[7] Libor Jany, *Minneapolis Police, Protesters Clash Almost 24 Hours After George Floyd's Death in Custody*, Star-Trib. (May 27, 2020), https://perma.cc/L8DF-W4LD.

[8] *Id*.

[9] *See, e.g.*, *"Please, Please, Please, I Can't Breathe*," Star-Trib. (May 29, 2020, 4:43 PM), https://perma.cc/AN5U-5VCT; Yamiche Alcindor & Amna Nawaz, *What We Know About George Floyd's Death in Minneapolis Police Custody*, PBS (May 26, 2020, 6:21 PM), https://perma.cc/9ZZL-TUTB.

[10] Josh Penrod & C.J. Sinner, *Buildings Damaged in Minneapolis, St. Paul After Riots*, Star-Trib. (July 13, 2020, 2:45 PM), https://perma.cc/ESB4-G9PG.

[11] Dylan Thomas, *Cost to Repair Lake Street Target, Cub Foods Stores Damaged in Riots Exceeds $4 Million*, Minneapolis/St. Paul Bus. J. (Oct. 21, 2020, 2:47 PM), https://www.bizjournals.com/twincities/news/2020/10/21/lake-street-target-cub-foods-repairs-4-million.html.

[12] Angela Caputo, Will Craft & Curtis Gilbert, *"The Precinct Is on Fire": What Happened at Minneapolis' 3rd Precinct—and What It Means*, APM Reports (June 30, 2020), https://perma.cc/JZE3-76B2.

[13] Minn. Exec. Order No. 20-65 (May 29, 2020), https://perma.cc/4MWV-G5UR; Minneapolis Emergency Reg. No. 2020-2-1 (Amended) (May 29, 2020), https://perma.cc/2F2Z-3AG2; St. Paul Emergency Exec. Order 2020-11 (May 29, 2020), https://perma.cc/DZ8F-XF55.

[14] Anna Boone, *One Week that Shook the World: George Floyd's Death Ignited Protests Beyond Minneapolis*, Star-Trib. (June 3, 2020), https://perma.cc/99QL-W7NN.

[15] Penrod & Sinner, *supra* note 10.

[16] 18 U.S.C. § 3123.

[17] The Samuelson Clinic is co-counsel in a case on behalf of the Reporters Committee for Freedom of the Press that asks the District of Minnesota to unseal several types of governmental requests to engage in electronic surveillance, including under the Pen Register and Stored Communications Acts, on both a retrospective and prospective basis. *See* Am. Appl., *In re Appl. of Reporters Comm. for Freedom of Press to Unseal Certain Warrant Materials*, Case No. 0:20-mc-82-PJS-TNL (D. Minn. Jan. 28, 2022), ECF No. 35.

[18] Appl. for Search Warrant, *In re Search of Info. that Is Stored at Premises Controlled by Google LLC*, Case No. 0:20-mj-475-DTS (D. Minn. July 9, 2020), ECF No. 3 [hereinafter Third Precinct Geofence Warrant].

[19] Appl. for Search Warrant, *In re Search of the Cellular Telephone Assigned Call Number [number]*, Case No. 0:20-mj-367 HB (D. Minn. June 8, 2020), ECF No. 3 [hereinafter Third Precinct Suspect A Phone Location Warrant 1]; Appl. for Search Warrant, *In re Authorization to Obtain Historical Records Containing Cell Site Info., Pen Register/Trap and Trace Devices with Cell Site Info., and GPS Ping Data, and to Use a Cell Site Simulator to Locate Target Phone with Number [number]*, Case No. 0:20-mj-396-HB (D. Minn. June 12, 2020), ECF No. 3 [hereinafter Third Precinct Suspect A Phone Location Warrant 2].

[20] Appl. for Search Warrant, *In re Authorization to Obtain Historical Records Containing Cell Site Info., Pen Register/Trap and Trace Devices with Cell Site Info., and GPS Ping Data Concerning the Target Mobile Phone Described in Attachment A*, Case No. 0:20-mj-392-HB (D. Minn. June 12, 2020), ECF No. 3 [hereinafter Third Precinct Suspect B Phone Location Warrant].

[21] Appl. for Search Warrant, *In re Search of the Premises [Address]*, Case No. 0:20-mj-448-KMM (D. Minn. June 18, 2020), ECF No. 3 [hereinafter Third Precinct Girlfriend Warrant].

[22] Appl. for Search Warrant, *In re Search of [Address]; and the Person of [Name]*, Case No. 0:20-mj-504-KMM (D. Minn. July 9, 2020), ECF No. 3 [hereinafter Third Precinct Physical Search Warrant].

[23] Appl. for Search Warrant, *In re Search of Info. Associated with Snapchat Username "[Username]" with a Display Name of [Display Name], and the Associated Telephone Number of [Number], that Is Stored at Premises Controlled by Snap, Inc.*, Case No. 0:20-mj-587-JTH (D. Minn. Aug. 4, 2020), ECF No. 3 [hereinafter Lake Street Post Office Snapchat Warrant].

[24] Appl. for Search Warrant, *In re Search of Info. Described in Attachment A that Is Stored at Premises Controlled by Google LLC*, Case No. 0:20-mj-483-HB (D. Minn. July 9, 2020), ECF No. 3 [hereinafter Lake Street Post Office Geofence Warrant].

[25] Appl. for Search Warrant, *In re Search of Info. that Is Stored at Premises Controlled by Google LLC*, Case No. 0:20-mj-494-KMM (D. Minn. Jul. 13, 2020), ECF No. 3 [hereinafter Minnehaha Post Office Geofence Warrant].

[26] Appl. for Search Warrant, *In re Search of Info. that Is Stored at Premises Controlled by Google, 1600 Amphitheatre Parkway, Mountain View, California 94043*, Case No. 0:20-mj-350-BRT (D. Minn. June 4, 2020), ECF No. 3 [hereinafter Powderhorn Post Office Geofence Warrant].

[27] Appl. for Search Warrant, *In re Search of Apple iPhone Cell Phone ("Subject Phone 1"), as Further Described in Attachment A*, Case No. 0:20-mj-376-HB (D. Minn. June 10, 2020), ECF No. 3 [hereinafter Great Health Phone Warrant].

[28] Redacted Appl. for Search Warrant, *In re Search of an Apple iPhone Model [Model] Currently in the Custody of ATF*, Case No. 0:20-mj-421-KMM (D. Minn. Dec. 15, 2020), ECF No. 7 [hereinafter Charter School Phone Warrant].

[29] Appl. for Search Warrant, *In re Appl. of U.S. for Authorization to Obtain Historical Records Containing Cell Site Info., Pen Register/Trap and Trace Devices with Cell Site Info., and GPS Ping Data Concerning the Target Mobile Phone Described in Attachment A; and In re Use of a Call Site Simulator to Locate the Target Mobile Phone Described in Attachment A*, Case No. 0:20-mj-605-JTH (D. Minn. Aug. 6, 2020), ECF No. 3 [hereinafter Cub Foods Warrant].

[30] Appl. for Search Warrant, *In re Search of Info. Associated with the Facebook User IDs: Account Number [Number], Username: [Username], and Account Number [Number], Username: [Username] that Are Stored at Premises Owned, Maintained, Controlled, or Operated by Facebook, Inc.*, Case No. 0:20-mj-351-BRT (D. Minn. June 5, 2020), ECF No. 1 [hereinafter Rupert Facebook Warrant].

[31] Appl. for Search Warrant, *In re Search of Info. Stored in Servers that Are Associated with Facebook User Account Number [Number], URL: https://www.facebook.com/[unique identifier], with Display Name: [Name] that Is Stored at Premises Controlled by Facebook*, Case No. 0:20-mj-440-KMM (D. Minn. June 17, 2020), ECF No. 3 [hereinafter Rupert Brother Facebook Warrant].

[32] Appl. for Search Warrant, *In re Search of Info. Stored in the Servers that Are Associated with Facebook User Account Number [Number], URL: https://www.facebook.com/[unique identifier], with Display Name: [Name], Username: [Username] that Is Stored at Premises Controlled by Facebook*, Case No. 0:20-mj-457-KMM (D. Minn. June 19, 2020), ECF No. 3 [hereinafter Rupert Friend Facebook Warrant].

[33] Appl. for Search Warrant, *In re Appl. of the Cellular Phone Using Number [number], Currently Believed to Be in the Possession of [Name]*, Case No. 0:20-mj-381-HB (D. Minn. June 11, 2020), ECF No. 3 [hereinafter Max It Pawn Phone Warrant 1]; Appl. for Search Warrant, *In re Appl. of the Cellular Phone Using Number [number], Currently Believed to Be in the Possession of [Name]*, Case No. 0:20-mj-383-HB (D. Minn. June 11, 2020), ECF No. 3 [hereinafter Max It Pawn Phone Warrant 2].

[34] Appl. for Search Warrant, *In re Authorization to Obtain Historical Records Containing Cell Site Info., Pen Register/Trap and Trace Devices with Cell Site Info., and GPS Ping Data Concerning the Target Mobile Phone Described in Attachment A; and In re Use of a Cell Site Simulator to Locate the Target Phone Described in Attachment A*, Case No. 0:20-mj-382-HB (D. Minn. June 11, 2020), ECF No. 3 [hereinafter Max It Pawn Cell Site Simulator Warrant 1]; Appl. for Search Warrant, *In re Authorization to Obtain Historical Records Containing Cell Site Info., Pen Register/Trap and Trace Devices with Cell Site Info., and GPS Ping Data Concerning the Target Mobile Phone Described in Attachment A; and In re Use of a Cell Site Simulator to Locate the Target Phone Described in Attachment A*, Case No. 0:20-mj-380-HB (D. Minn. June 11, 2020), ECF No. 3 [hereinafter Max It Pawn Cell Site Simulator Warrant 2].

[35] Appl. for Search Warrant, *In re Authorization to Obtain Historical Records Containing Cell Site Info., Pen Register/Trap and Trace Devices with Cell Site Info., and GPS Ping Data Concerning the Target Mobile Phone Associated with Number [number]*, Case No. 0:20-mj-479-DTS (D. Minn. June 26, 2020), ECF No. 3 [hereafter Gordon Parks High School Warrant].

[36] Appl. for Search Warrant, *In re Search of Info. that Is Stored at Premises Controlled by Google*, Case No. 0:20-mj-586-JTH (D. Minn. Aug. 05, 2020), ECF No. 3 [hereinafter Walgreens Geofence Warrant].

[37] Appl. for Search Warrant, *In re Search of Info. Associated with the Cellular Device Assigned Call Number [Number] that Is Stored at Premises Controlled by Sprint*, Case No. 20-mj-446-KMM (D. Minn. June 18, 2020), ECF No. 3 [hereinafter Walgreens Phone Account Warrant].

[38] Appl. for Search Warrant, *In re Search of Vehicle, Namely, [Make, Model] Bearing Minnesota License Plate [License Plate Number], Vehicle Identification Number [Number]*, Case No. 0:20-mj-442-KMM (D. Minn. June 18, 2020), ECF No. 3 [hereinafter Enterprise Vehicle Warrant].

[39] Appl. for Search Warrant, *In re Installation and Monitoring of a Tracking Device on a [Vehicle Description]*, Case No. 0:20-mj-463-DTS (D. Minn. June 22, 2020), ECF No. 3 [hereinafter Boogaloo Bois Vehicle Warrant 1]; Appl. for Search Warrant, *In re Installation and Monitoring of a Tracking Device on a [Vehicle Description]*, Case No. 0:20-mj-464-DTS (D. Minn. June 22, 2020), ECF No. 3 [hereinafter Boogaloo Bois Vehicle Warrant 2]; Appl. for Search Warrant, *In re Installation and Monitoring of a Tracking Device on a [Vehicle Description]*, Case No. 0:20-mj-543-KMM (D. Minn. July 24, 2020), ECF No. 3 [hereinafter Boogaloo Bois Vehicle Warrant 3].

[40] *See, e.g.*, Gordon Parks High School Warrant, *supra* note 35, at 17 (stating that law enforcement was required to use search methodologies that would avoid searching files, documents, and other data that was not identified in the warrant, among other restrictions).

[41] *See* Nick Woltman, *Brooklyn Park Man, 20, Pleads Guilty to Arson of St. Paul Nutrition Store*, TwinCities Pioneer Press (July 21, 2021), https://perma.cc/66HK-SUT4.

[42] Great Health Phone Warrant, *supra* note 27, ¶ 18.

[43] *Id*. at ¶ 19.

[44] *Id*.

[45] *Id*.

[46] *Id*. at ¶ 20.

[47] *See, e.g.*, *id*. at ¶ 24 (stating that "[a]t approximately the 1:01 time mark, one of the female co-conspirators says, 'who's got a lighter?' and "at approximately the 2:36 time mark, a female co-conspirator announces, 'he lit the fire!'").

[48] *Id*. at ¶ 24.

[49] *Id*. at ¶ 20(a).

[50] *Id*. at ¶ 27.

[51] *Id*.; Woltman, *supra* note 41.

[52] Charter School Phone Warrant, *supra* note 28, ¶¶ 12–16.

[53] *Id*. at ¶ 11.

[54] *Id*. at ¶ 15.

[55] *Id*. at ¶ 16.

[56] *Id*. at ¶¶ 17–18.

[57] *Id*. at ¶ 18.

[58] Great Health Phone Warrant, *supra* note 27, ¶¶ 18–26; Charter School Phone Warrant, *supra* note 28, ¶¶ 11–16.

[59] Great Health Phone Warrant, *supra* note 27, at 1; Charter School Phone Warrant, *supra* note 28, at 1.

[60] Third Precinct Girlfriend Warrant, *supra* note 21, ¶¶ 21–29.

[61] *See* Caputo et al., *supra* note 12.

[62] Third Precinct Girlfriend Warrant, *supra* note 21, ¶ 11–20.

[63] *Id*. at ¶¶ 13–16.

[64] *Id*. at ¶ 21; *see also* See Something, Say Something: Oversight of the Parkland Shooting and Legis. Proposals to Improve School Safety: Hearing Before S. Comm. on the Judiciary, 115th Cong. (2018) (statement of Thomas E. Brandon, Acting Dir., ATF, pp. 3–4) (explaining ATF's electronic tip tracking system).

[65] Third Precinct Girlfriend Warrant, *supra* note 21, ¶¶ 21–29.

[66] *Id*. at ¶¶ 22–26.

[67] *Id*. at ¶ 27.

[68] *Id*.

[69] *Id*. at ¶¶ 27–28.

[70] *See e.g.*, Rupert Brother Facebook Warrant, *supra* note 31, ¶¶ 8–9, 16–17; Rupert Friend Facebook Warrant, *supra* note 32, ¶¶ 8–9, 16–18; Max It Pawn Cell Site Simulator Warrant 1, *supra* note 34, ¶¶ 22–23 (describing using public Snapchat and Facebook posts to identify a second suspect based on his connections with a previously identified suspect).

[71] Rupert Facebook Warrant, *supra* note 30, ¶¶ 6–12.

[72] *Id*. at ¶¶ 8–12.

[73] Rupert Brother Facebook Warrant, *supra* note 31 ¶¶ 8–9, 16–17; Rupert Friend Facebook Warrant, *supra* note 32 ¶¶ 8–9, 16–18.

[74] *See* Rupert Brother Facebook Warrant, *supra* note 31; Rupert Friend Facebook Warrant, *supra* note 32.

[75] Rupert Brother Facebook Warrant, *supra* note 31, ¶¶ 16–17.

[76] *Id*. at ¶ 16.

[77] Rupert Friend Facebook Warrant, *supra* note 32, ¶¶ 9, 16–18.

[78] *See* Rupert Facebook Warrant, *supra* note 30, at 4–6; Rupert Brother Facebook Warrant, *supra* note 31, at 5–7; Rupert Friend Facebook Warrant, *supra* note 32, at 5–9.

[79] Rupert Facebook Warrant, *supra* note 30, ¶¶ 8–12.

[80] Rupert Brother Facebook Warrant, *supra* note 31, ¶ 16.

[81] Rupert Facebook Warrant, *supra* note 30, ¶ 7.

[82] Rupert Friend Facebook Warrant, *supra* note 32, ¶ 9.

[83] *See id*.

[84] *Id*. at ¶ 17.

[85] *Id*.; *see also* Rupert Brother Facebook Warrant, *supra* note 31, ¶ 17.

[86] Rupert Friend Facebook Warrant, *supra* note 32, ¶ 17.

[87] *Id*.

[88] *Id*. at ¶ 22.

[89] Third Precinct Girlfriend Warrant, *supra* note 21, ¶¶ 28–29.

[90] *Id*. at ¶ 28.

[91] *See* Rupert Facebook Warrant, *supra* note 30, ¶¶ 7–15; Rupert Brother Facebook Warrant, *supra* note 31, ¶¶ 8–9, 16–17; Rupert Friend Facebook Warrant, *supra* note 32, ¶¶ 8–9, 16–18.

[92] Rupert Facebook Warrant, *supra* note 30, ¶¶ 9–12.

[93] *See id*. at 16–18.

[94] *Id*.

[95] *See, e.g.*, Gordon Parks High School Warrant, *supra* note 35, at 14–16.

[96] *See, e.g.*, *id*.; Cub Foods Warrant, *supra* note 24, at 27–30; Max It Pawn Cell Site Simulator Warrant 2, *supra* note 34, at 27–30.

[97] Cub Foods Warrant, *supra* note 24, at 27–30.

[98] *Id*. at 27.

[99] *Id*.

[100] *Id*. at ¶ 27.

[101] *Id*.

[102] *See, e.g.*, *id*. at ¶ 27–28 (permitting collection of data on when voice, SMS, and data were transmitted and which cellphone towers were used).

[103] *See, e.g.*, *id*. at ¶ 27; *see also* Fed. Comm'ns Comm., *Enhanced 911 — Wireless Services*, https://perma.cc/W42B-NFZF (last visited Feb. 12, 2024) (describing the Enhanced 911 system and data it generates).

[104] Cub Foods Warrant, *supra* note 24, ¶ 27–28.

[105] Walgreens Geofence Warrant, *supra* note 36; Powderhorn Post Office Geofence Warrant, *supra* note 26; Lake Street Post Office Geofence Warrant, *supra* note 24; Minnehaha Post Office Geofence Warrant, *supra* note 25; Third Precinct Geofence Warrant, *supra* note 18.

[106] *See 2 Minneapolis Post Offices Deemed Total Losses After Fires*, Fox 9 (June 1, 2020, 11:07 PM), https://perma.cc/965N-P8UT; Henry Pan, *What Comes Next for South Minneapolis' Recently Destroyed Post Offices?*, MinnPost (June 10, 2020), https://perma.cc/Z6F5-7KXK.

[107] *See* Powderhorn Post Office Geofence Warrant, *supra* note 26, ¶¶ 15–25.

[108] *Id*. at ¶¶ 15–16.

[109] *Id*. at ¶ 21.

[110] *Id*. at ¶ 23.

[111] *Id*. at ¶ 23.

[112] *Id*. at ¶ 26.

[113] *Id*. at 16–19.

[114] Elec. Frontier Found, *Street-Level Surveillance: Cell-Site Simulators/IMSI Catchers* (Aug. 28, 2017), https://perma.cc/7TAS-JXH2.

[115] *See, e.g.*, Gordon Parks High School Warrant, *supra* note 35, ¶ 25.

[116] *Id*. at ¶¶ 4–5.

[117] *Id*. at ¶ 24.

[118] *Id*.

[119] *See, e.g.*, Third Precinct Suspect A Phone Location Warrant 2, *supra* note 19, ¶ 5 ("The purpose of applying for a warrant authorizing the use of a CSS is to precisely determine the location of the Target Mobile Phone. This warrant also seeks to obtain the most recent historical call detail records . . . to locate, identify, and possibly arrest the user . . . .").

[120] *See, e.g.*, Third Precinct Suspect A Phone Location Warrant 1, *supra* note 19, ¶ 23; Max It Pawn Cell Site Simulator Warrant 2, *supra* note 34, ¶ 26; Cub Foods Warrant, *supra* note 24, ¶ 28.

[121] Max It Pawn Cell Site Simulator Warrant 2, *supra* note 34, ¶ 26.

[122] *See* Third Precinct Physical Search Warrant, *supra* note 22.

[123] *Id*. at ¶¶ 41–42.

[124] *See, e.g.*, *id*. at 4 (listing cellphone, computers, and other devices "containing electronically stored communications" as items that can be searched and seized during a physical search).

[125] *See, e.g.*, Max It Pawn Phone Warrant 1, *supra* note 33, at 21; Charter School Phone Warrant, *supra* note 28, ¶¶ 22–31.

[126] Max It Pawn Phone Warrant 1, *supra* note 33, at 21; Max It Pawn Phone Warrant 2, *supra* note 33, at 23.

[127] Max It Pawn Phone Warrant 1, *supra* note 33, ¶ 23.

[128] Max It Pawn Phone Warrant 2, *supra* note 33, ¶ 18.

[129] Max It Pawn Phone Warrant 1, *supra* note 33, at 20; Max It Pawn Phone Warrant 2, *supra* note 33, at 22.

[130] *Id*.

[131] *See, e.g.*, Boogaloo Bois Vehicle Warrant 1, *supra* note 39, ¶ 3; Boogaloo Bois Vehicle Warrant 2, *supra* note 39, ¶ 3; Boogaloo Bois Vehicle Warrant 3, *supra* note 39, ¶ 3.

[132] Lake Street Post Office Snapchat Warrant, *supra* note 23, ¶¶ 24, 29.

[133] *See, e.g.*, Great Health Phone Warrant, *supra* note 27, ¶¶ 31–32; Walgreens Phone Account Warrant, *supra* note 37, ¶ 13 (law enforcement utilized "government vehicle records" to learn that a vehicle parked outside a Walgreens before it was set on fire was owned by Enterprise and had been rented by a woman whose brother ended up being the main suspect in the case).

[134] *See, e.g.*, Enterprise Vehicle Warrant, *supra* note 38, ¶¶ 30, 35; Third Precinct Girlfriend Warrant, *supra* note 21, ¶¶ 32, 35.

[135] Great Health Phone Warrant, *supra* note 27, ¶ 31.

[136] *Id*.

[137] *Id*.

[138] *Id*. at ¶ 32.

[139] *Id*.

[140] *Id*. at ¶ 34.

[141] *Id*. at ¶¶ 39–40.

[142] *See* Boogaloo Bois Vehicle Warrant 1, *supra* note 39, at 1; Boogaloo Bois Vehicle Warrant 2, *supra* note 39, at 1; Boogaloo Bois Vehicle Warrant 3, *supra* note 39, at 1.

[143] Boogaloo Bois Vehicle Warrant 1, *supra* note 39, ¶ 5; Boogaloo Bois Vehicle Warrant 2, *supra* note 39, ¶ 5; Boogaloo Bois Vehicle Warrant 3, *supra* note 39, ¶ 5.

[144] Boogaloo Bois Vehicle Warrant 1, *supra* note 39, ¶¶ 6, 9; Boogaloo Bois Vehicle Warrant 2, *supra* note 39, ¶¶ 6, 9.

[145] *See, e.g.*, Boogaloo Bois Vehicle Warrant 1, *supra* note 39, ¶¶ 7–16.

[146] *Id*. at ¶¶ 17–18; Boogaloo Bois Vehicle Warrant 3, *supra* note 39, ¶ 18.

[147] Boogaloo Bois Vehicle Warrant 1, *supra* note 39, ¶ 24; Boogaloo Bois Vehicle Warrant 2, *supra* note 39, ¶ 24; Boogaloo Bois Vehicle Warrant 3, *supra* note 39, ¶ 24.

[148] Boogaloo Bois Vehicle Warrant 1, *supra* note 39, ¶ 21; Boogaloo Bois Vehicle Warrant 2, *supra* note 39, ¶ 21; Boogaloo Bois Vehicle Warrant 3, *supra* note 39, ¶ 21.

[149] Lake Street Post Office Snapchat Warrant, *supra* note 23, ¶¶ 24, 29.

[150] *See* Pan, *supra* note 106.

[151] Lake Street Post Office Snapchat Warrant, *supra* note 23, ¶ 21.

[152] *Id*.

[153] *Id*.

[154] *Id*.

[155] *Id*. at ¶ 22.

[156] *Id*. at ¶ 23.

[157] *Id*. at ¶¶ 24, 29.

[158] *Id*. at ¶ 30.